Digital Evidence Management and Analysis in the Cloud

Special Report

Prepared by:
Alison Brooks, Ph.D.
IDC Canada Consulting
33 Yonge St #420, Toronto, ON M5E

PWGSC Contract Number: W7714-166152/001/SV
TA: Gerry Doucette, DRDC Centre for Security Science, 613-943-2463

Contract Report
DRDC-RDDC-2016-C198
April 2016

IMPORTANT INFORMATIVE STATEMENTS

The Digital Evidence Management and Analysis in the Cloud study, CSSP-2015-CP-2106, was supported by the Canadian Safety and Security Program, which is led by Defence Research and Development Canada's Centre for Security Science, in partnership with Public Safety Canada. The project was led by the Vancouver Police Department and contracted to IDC Canada. The study drew mainly on key informant interviews conducted with representatives from six leading organizations that have deployed, or anticipate deploying, cloud-based evidence management solutions. The study provides planning guidance to governments and law enforcement service providers related to the viability of creating national or regional based cloud and analytics evidentiary data management systems.

The Canadian Safety and Security Program is a federally-funded program to strengthen Canada's ability to anticipate, prevent/mitigate, prepare for, respond to, and recover from natural disasters, serious accidents, crime and terrorism through the convergence of science and technology with policy, operations and intelligence.

Special Report

Digital Evidence Management and Analysis in the Cloud

Alison Brooks, Ph.D.

INTRODUCTION

In January and February 2016, IDC conducted executive interviews with six organizations that have leveraged cloud deployment models to manage digital evidence in a multi-agency setting. The findings from these international deployments should inform the development of local, regional, and national business cases for those organizations considering investment in cloud and/or analytically driven evidence-based decision-making environments.

IDC and its partner organizations in this project created an initial list of more than 20 organizations. Each organization was contacted to glean insights into their use of multi-agency cloud and analytic solutions. While a significant number of them have not yet deployed cloud solutions, the following six were able to share their experiences and insight about digital asset management:

- The Automated Regional Justice Information System (ARJIS)
- The San Diego Police Department
- The Federal Bureau of Investigation
- Orange County
- London Metropolitan Police
- The Dutch National Police

In addition to these six case studies, IDC conducted an executive interview with the Royal Canadian Mounted Police (RCMP) to further understand its cloud strategy moving forward.

This study was funded by a Centre for Security Studies Program (CSSP) research contract in 2015 and 2016. The project team for CSSP #2015–CP–2106 would like to acknowledge and formally thank the individuals at these organizations, and the organizations themselves, for agreeing to participate in the research and for taking the time to share their insights with the broader public safety community.

This report provides a case study of each organization's cloud deployment according to five core research areas:

- Stakeholders and governance
- Technology scope and parameters
- Implementation and maintenance
- Security provisions
- Key business outcomes

While recent discussions around digital evidence management have focused on challenges created by body-worn video (BWV) technology, for the scope of this research we defined digital evidence more broadly as any digital asset being managed by law enforcement and the courts.

CLOUD SERVICES

IDC defines cloud services more formally through a checklist of key attributes that an offering must manifest to end users of the service. To qualify as a "cloud service," as defined by IDC, an offering must support all of the following six attributes:

- Shared, standard service: built for multitenancy, among or within enterprises
- Solution packaged: a "turnkey" offering, pre-integrates required resources
- Self-service: provisioning and management, typically via a web portal and APIs
- Elastic resource scaling: dynamic, rapid, and fine-grained
- Elastic, use-based pricing: supported by service metering
- Published service interface (API): web services, other common Internet APIs

These attributes apply to all cloud services — in all public and private cloud service deployment models — although the specifics of how each attribute applies may vary slightly among these deployment models. The sections that follow provide a more detailed explanation of what we mean for each of these attributes.

At the highest level, the two types of deployment models for cloud services are public and private (see Figure 1):

- Public cloud services are shared among unrelated enterprises and/or consumers, open to a largely unrestricted universe of potential users, and designed for a market, not a single enterprise.
- Private cloud services are shared within a single enterprise or an extended enterprise, with restrictions on access and level of resource dedication, and defined/controlled by the enterprise, beyond the control available in public cloud offerings.

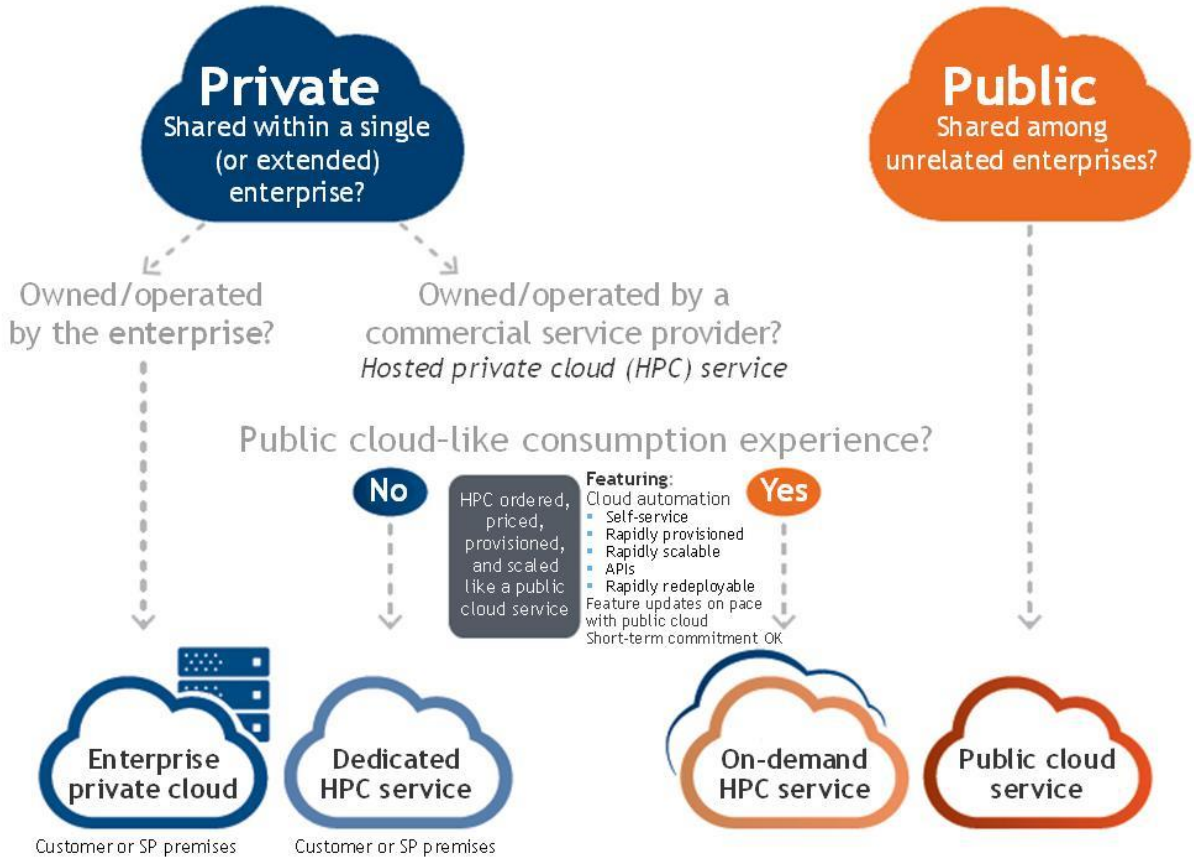
In the public cloud world, we define one major model called, not surprisingly, public cloud service. Underneath this big umbrella, there are a growing variety of options available relating to public/private/VPN network connection, geolocation of data, options for dedicated data storage devices, and so forth. IDC considers all these "subspecies" within the public cloud world.

In the private cloud services world, there are two major options:

- **Enterprise private cloud.** This is owned and operated by an enterprise for its own internal use.
- **Hosted private cloud.** In this private cloud scenario, third-party commercial cloud service providers offer customers access to private cloud services that the service providers have built, own, and operate. Within the HPC world, IDC has identified two very different HPC deployment models: dedicated HPC, fully dedicated to a single customer for an extended period of time, and on-demand HPC, where resources from a shared pool are dynamically provisioned for dedicated use by clients.

FIGURE 1

Public and Private Deployment Models for Cloud Services



Source: IDC, 2016

ROYAL CANADIAN MOUNTED POLICE

With 700 geographical detachments across Canada, digital evidence management is a sizeable challenge for the Royal Canadian Mounted Police (RCMP). On any given day the RCMP manages up to 15 different types of critical audio and video data sources, including body-worn and in-car video, cell block video feeds, CCTV feeds of Parliament Hill, tactical video, interview video, drone video, crime scene video, videos from border services, 911 calls, radio communication, and interview audio. Combined this amounts to thousands of hours of audio and video generated every day. Turning to cloud deployment solutions to manage its existing audio and video data – and to manage *all* of its digital assets in the longer term – is of significant interest to the RCMP since it would allow the organization to cost-effectively create a single master repository for all of its digital assets.

Changing Approach to Cloud

The RCMP's approach to cloud technologies has changed dramatically in the past six months. Historically, the organization had only considered private cloud offerings owing to data residency concerns related to public cloud hosting solutions. However, the 2015 launch of a number of Canadian public cloud solutions opened the door to the consideration of public cloud. The RCMP's shifting position on cloud has also been nudged by the vendor community, which is increasingly

offering only cloud-based solutions. The migration to cloud is being shepherded by the disappearance of on-premise solutions.

While the RCMP is far from having an official position on digital evidence management in the cloud, it is leaning toward public cloud for all of its information and digital assets classified up to Protected B (everything short of "extremely sensitive" or "top secret" information). It would like to take a software-as-a-service approach to digital evidence management, relying on the hosting organization to put in place the necessary safeguards, based on existing standards like the Federal Risk and Authorization Program (FedRAMP) in the U.S. FedRAMP is a risk management program that provides a standardized approach for assessing and monitoring the security of cloud products and services. The RCMP plans to contract directly with a digital evidence management solution provider as opposed to going to a system integrator to build a custom solution.

RCMP Cloud Readiness Assessment

The RCMP completed a cloud readiness assessment in March to flesh out its digital evidence management strategy and will use this to guide the creation of the National Digital Asset System (NDAS). The assessment will help the RCMP prepare to support cloud services by addressing a number of key questions including security, benefits, and risks of private and public cloud, and funding implications. With regards to funding, while large IT projects have historically been funded by capital expenditures, cloud costs are considered operating expenditures and carry with them a different set of funding implications.

Moving forward, the RCMP will draw on three policy documents developed as part of the assessment to manage three distinct areas of its digital asset management: collection (retention policies, storage), evidence management, and usage.

From this assessment, the RCMP will create a preliminary list of system requirements for NDAS which includes but is not limited to the following:

- Mobile access
- Mobile metadata tagging
- Continuity of evidence
- Traceability
- Court disclosure (including integration with RMS)
- Date-driven automatic purging of evidence
- The capacity to search outside of the RMS
- Respect for the RCMP's low bandwidth realities
- Upload continuity in cases of network interruption
- Audio and video clipping
- Video redaction
- Medium-high redundancy
- BCP/DR that is geographically separated enough to withstand a natural disaster

The RCMP plans to include in-car and body-worn video in NDAS initially, expanding over time to incorporate all of its other digital assets. Part of its strategy, therefore, is to build an architecture that accommodates *all* digital evidence. In the long term it envisions a tagged and searchable video service akin to an RCMP YouTube channel. At the moment, the RCMP does not believe it needs to, or can afford to, back up every single video file from every detachment. It intends to take a rules-based approach to what is uploaded to NDAS.

The RCMP has a number of challenges related to its vast geographical distribution, including bandwidth and T1 network constraints. Due to the high costs of network bandwidth in many areas serviced by the RCMP, the force plans to establish an external ISP Internet connection for the uploading and viewing of video.

Security

The digital evidence management solution vendor and its associated hosting vendor will need to meet the business and security requirements specified in a forthcoming RFP (another outcome of the cloud-readiness assessment), which will align with the NDAS strategy. The Treasury Board Secretariat is currently undertaking an initiative to create a Canadian equivalent to the U.S.'s FedRAMP security standard (CanRAMP). Though development is not expected in the near term, the RCMP plans to leverage this standard once it is available.

Challenges Specific to the RCMP

- How does it work with Shared Services Canada (SSC); will SSC provide the infrastructure as a service?
- How are CSE and the Treasury Board Secretariat involved?
- Supplier readiness
- RCMP readiness

THE AUTOMATED REGIONAL JUSTICE INFORMATION SYSTEM

Overview

The Automated Regional Justice Information System (ARJIS) manages all police incidents and court disclosures for San Diego and the Imperial County of California. Set up in the late 1970s, ARJIS was the brainchild of San Diego Chief of Police Bill Kolender, known for being decades ahead of his time in terms of both information sharing and community policing. What began in the 1970s has become a 40-year legacy of collaborative police work.

Stakeholders and Governance

The stakeholder and governance structure within which ARJIS sits – while elaborate, multilayered, and somewhat complicated – strikes a particular balance which is integral to its ability to deliver on complicated public safety technology-related issues.

At its highest level, the San Diego Association of Governments (SANDAG) is a *regional* "Council of Governments" decision-making entity that spans 18 local city and county governments across San Diego and Imperial County. SANDAG is governed by a board of directors comprising the mayor or council member from those cities and counties; the board is mainly focused on budgetary and policy decisions. Representation also incorporates a broad ecosystem of critical infrastructure and public safety partners. Supplementing those voting members are advisory representatives from Imperial County, the U.S. Department of Defense, Caltrans, San Diego Unified Port District, the Metropolitan Transit System, the North County Transit District, the San Diego County Water Authority, the Southern California Tribal Chairmen's Association, and border services with Mexico.

The Public Safety Committee (PSC) is the primary governing body for public safety related issues. The PSC is fairly unusual in that it's composed of both elected officials and public safety executives, giving it the right mix of operational, electoral, policy, and geographic representation. The Public Safety Committee advises the SANDAG board of directors on major policy-level matters related to public safety and is supported by ARJIS and the Criminal Justice Research Division.

ARJIS itself was created as a joint powers agency to share information among justice agencies throughout San Diego and Imperial County in California. The Chief Sheriffs' Management Committee functions as the central body making recommendations to the PSC. The CSMC in turn, is supported by the ARJIS Business Committee, the ARJIS Technical Committee, and a Data Quality Committee. Currently the ARJIS system spans 5,000 users and 81 local, state, and federal criminal justice and critical infrastructure agencies. The system is member-funded and therefore completely sustainable, with new technology acquisitions funded through Homeland Security and other grants.

ARJIS is the first and only *regional* member of the National Law Enforcement Telecom system (NLETs), the system that links together U.S. law enforcement, justice, and public safety agencies to share critical information. Participation is typically reserved for state representation, but the enormous size of the state of California means that it often struggles with agility, flexibility, and speed. In view of this, both the State of California and NLETs supported ARJIS becoming a regional member. As a result of that association, ARJIS has been able to undertake a number of test-bed projects like the Driver's License Photo Exchange project.

Technology Scope and Parameters

ARJISnet is a private cloud deployment hosting all of its 81 supported agencies' major operations and investigative systems. ARJIS' physical datacentre is hosted at the NLETs datacentre in Phoenix, and its cloud deployment provides triple redundancy.

ARJIS provides all infrastructure to its member organizations, including networking and mobile platform, as well as data validation for all user organizations. It also provides members with a broad suite of business and operational tools, built in-house and/or incorporated from one of its members. These include officer notification, tactical search, i2, Coplogic, Palantir, and in-house GPS apps. The sheer volume of organizations using ARJIS means that it has had to create 47 different interfaces to all its members' core systems, ensuring that the data arrives in one single database in real time. Leveraging IBM Cognos, ARJIS also manages its members' mandatory FBI Unified Crime Reporting requirements, a significant data collection and classification effort.

Implementation and Maintenance

ARJIS' foray into the cloud began in 2010 when it initiated its migration off the mainframe system, a process that took two years to complete given the number of agencies involved. The total cost of moving to the ARJISnet private cloud was US$14 million. ARJIS has a US$4.5 million annual budget, and 20 to 25 FTEs, roughly five of whom are in management roles. Interestingly, the annual budget is funded by a legal settlement from a failed vendor implementation.

Security Provisions

An example of the security standards leveraged in ARJIS and in the SDPD can be found here: https://www.microsoft.com/en-us/TrustCenter/Compliance/CJIS.

Key Challenges

ARJIS noted a number of challenges to its current operations, specifically:

- The dissonance between the civil liberties groups with regard to body-worn video, transparency, and faith in the policing community.
- The overwhelming volume of public records requests.
- The process of managing privacy issues proactively creates far more work and cost than originally forecast.

- Inaccurate and outdated documentation for some of its members slowed the aggregate migration to cloud.
- Given the current negative attitude to policing, the need to get the elected officials on board with regard to privacy and policy issues being addressed.

Business Outcomes

- ARJIS is able to provide seamless, immediate, efficient interjurisdictional information sharing across all of its member organizations.
- Qualitative insights suggest efficiencies in the time to arrests; ARJIS is currently working with the RAND Corporation to quantify these insights.

ARJIS Recommendations

- Governance, complicated and dull though it might seem, is the key to success in the region; broader representation almost always ensures a successful project or portfolio.
- Build performance metrics into vendor solutions for digital evidence, network security, etc.
- Focus on mobile as it is the next frontier.
- Take a regional focus, which is likely more manageable than state or national.
- Get business case requirements and buy-in from everyone, including the officers on the street; include the officers in technology-related projects.
- Learn how to present technology information to a number of different types of stakeholders – boards of directors, IT, police chiefs, etc. The high visibility of some technology issues leads to the involvement of more and different stakeholders than is typical.
- Private cloud is considered to be something that helps to address some of the burgeoning concerns with privacy; there is more at risk in the current political environment if an organization were to use public cloud and suffer a data or privacy breach.

THE SAN DIEGO POLICE DEPARTMENT

Overview, Stakeholders, and Governance

San Diego's body-worn video implementation, involving the San Diego Police Department (SDPD) and the lower and higher courts in the region, was the first (and still the largest) of its kind in North America. The project initially arose out of some conduct issues in the force, but the focus quickly shifted toward creating a culture of transparency and restoring civic faith in policing services, an issue with which U.S. law enforcement across the country struggled immensely in 2015.

Technology Scope and Parameters

The SDPD began researching body-worn video solutions in 2011, piloting and testing options in 2013, ultimately implementing the first wave of 300 devices in 2014. By the end of 2016 it will have deployed a total of 1,450 devices across its base of 1,850 officers.

In 2013 the SDPD selected Axon's Evidence.com body-worn video software-as-a-service solution; the cloud hosting provider supporting Evidence.com is Amazon Web Services, though both Amazon and Microsoft can be used to host Evidence.com. San Diego county and the city of San Diego proper also have their own Evidence.com cloud solutions, allowing the three organizations to share video footage from one cloud to another. A universal control number is attached to each evidence file and is opened on the organization's own cloud system. Video transfer between the SDPD and lower and higher courts is facilitated by MOUs.

The solution requirements were set out initially in 2014. At that time the SDPD was looking for a solution that could, at minimum, match the length of its officers' shifts. Accordingly, requirements included:

- 10 hours of run time
- 12 hours of buffering (while in the buffering mode, the camera will continuously record only video in 30-second loops)
- 30-second pre-buffer (the system provides 30 seconds of video recording prior to the record button being pushed)
- Mobile metadata attachment
- Docking capacity: dock, charge, upload, and wipe immediately
- Audit trail and traceability
- Non-alterable video transfer
- Cloud-based solution

The SDPD did not want its officers to be able to alter the video, so it made a policy decision to use the solution without the redaction and editing functionality; the SDPD collects and sends everything to the courts in raw form to be managed. There is an impressive level of traceability embedded in the solution. If someone tries to put a video online, the solution can determine who is responsible and can display an audit trail. Similar audit trails are created when video files are uploaded into a case, or sent to a prosecutor.

While this implementation has a lot of interesting information to share regarding public cloud, the SDPD doesn't need complex analytics given that the videos are managed by the court. The SDPD would like to be able to collect some basic stats such as the number of videos taken during a given event, or the percentage of calls involving mental health issues, traffic stops, domestic violence, etc.

Implementation and Maintenance

The initial cost of the implementation was US$4 million for all of the devices, docking, cloud licenses, and associated hardware for five years. Given that the docking stations needed to have their own Internet connection, the SDPD spent an additional US$40,000 in network upgrades for the department. In 2015 the SDPD signed a five-year contract extension with Evidence.com for US$1.8 million, bringing the total investment with Taser, over six years, to US$5.8 million. As part of that contract, the SDPD has a maximum of 234TB storage at its disposal over the same period; in early 2016 it had used 50TB of that total allowance.

Moving forward, the SDPD plans to expand the management of its other digital assets into the Evidence.com system when its CAD system is replaced in 2017. This will require storing all of its major operational and investigative systems to Evidence.com, but should yield some very interesting investigative and analytical capabilities.

Security

The SDPD follows FBI Criminal Justice Information Security (CJIS) Standard, a 200-page policy document that can be found here: https://www.fbi.gov/about-us/cjis/cjis-security-policy-resource-center.

Key Challenges

- Body-worn video is slow and difficult to implement.
- At the time of the initial implementation, storage requirements were unknown.

- Usage issues: officers need to turn the recorders on when certain policy triggers have been met.
- Demands for video release: the SDPD didn't foresee all of the public and media demands to view all videos.
- The ACLU is positioning that officers can only view the video after writing up an incident.
- Logistical and bandwidth issues relaying video efficiently with prosecution and courts: for traffic violations, hotspots have been set up in traffic court to provide direct video feeds.
- When they first started, the courts weren't involved, making the process of sharing video extremely onerous.

Business Outcomes

The SDPD deployment was able to provide some interesting statistics related to the effect body-worn video was having on day-to-day operations, and on its goals of increasing transparency in policing.

- Complaints about police conduct decreased 45%, and racial discrimination complaints have almost disappeared.
- The technology provides a different unbiased perspective on critical incidents, but organizations need to contextualize this information as it is important to stress that what is on the video is not what the officer is seeing.
- SDPD feels that officers who previously did not see the value of the technology have changed their positioning on the matter.
- SDPD feels that the system in the aggregate is helping to build trust in the community. The technology makes officers and civilians alike aware of their actions and comportment; this has made good officers better.

Recommendations

- Focus on training and policy iteration. The SDPD updates its BWV policies every six months.
- Avoid the video gatekeeper bottleneck: SDPD officers and investigators manage all videos, avoiding having to allocate 10–20 full-time resources to do so.
- The SDPD would like the vendor community to provide a 2-minute pre-buffer with audio.

THE FEDERAL BUREAU OF INVESTIGATION

Introduction

Like the RCMP, the Federal Bureau of Investigation (FBI) remains in the evaluation stage of its cloud deployment strategy. What follows are its current thoughts on technology scope, parameters, security, and challenges specific to the FBI. In contrast to some of the other case studies in this research, the FBI's interest in moving to cloud began as a cost savings and quality of service initiative. Federal government efficiency mandates, datacentre rationalization, and a desire to leverage a more scalable infrastructure were key drivers to adoption. The FBI will invariably create a hybrid cloud solution, with costs/benefits, data sensitivity, and performance concerns guiding the decisions about what would be placed in a public cloud, and what will be retained in-house.

Stakeholders and Governance

The scope of the cloud implementation being considered is limited to the FBI, specifically the Department of Justice, although FBI systems are accessed by many partner law enforcement organizations around the United States.

Cloud governance will align with many federal laws, as well as internal policies, especially in terms of monitoring, access, and encryption for chain of custody, as well as overall security and integrity. While there is currently no single governing entity or structure, those who utilize cloud services in their implementation are required to comply with appropriate security and data management policies. The FBI is moving to a model whereby an Application Hosting (i.e., "Cloud") team sets the standards and policies surrounding cloud initiatives.

Technology Scope and Parameters

The FBI/CJIS is developing an internal, unclassified cloud solution for the entire Department of Justice. It is being designed with the intent of becoming a hybrid solution for DOJ customers, with its more sensitive data being kept in-house. The hybrid solution will be accomplished via one of two implementation methods: 1) using commercial cloud services (C2S) with the C2S footprint as an extension to their in-house solution, or 2) making C2S available to applications directly, with no tie to the in-house evidence management solution. The FBI is implementing commercial cloud-hosted applications selectively, with the majority of utilization at this time reserved for development and testing.

Evidence management solutions will be based on common and commercial options such as Dell, Microsoft, Cisco, VMWare, and OpenStack. Wary of the current turmoil in the cloud market – buyouts, mergers, and acquisitions – the FBI is looking for a stable industry leader with a reputation for security.

Key business requirements are primarily cost-driven. The FBI will use C2S services when it is most beneficial to the government, and use the in-house solution when mission criticality, sensitivity of the data, and/or other key factors outweigh the additional costs. "Some systems, applications, and data cannot have a price put on it were it to be compromised in any fashion," the FBI said.

The in-house solution will be located at a minimum of two locations, one in Clarksburg, WV, and one in Pocatello, Idaho. The Bureau is considering a third location in the Washington, D.C. metro area. Any C2S vendor will be required to demonstrate capacity and capability to support a minimum of two locations. Redundancy requirements could also be met by the use of multipoint cloud services, such as AWS activity zones and regions.

The FBI will demand a minimum of three or four "9s" (99.9% or 99.99%) for compute availability including during scheduled maintenance, and five "9s" (99.999%) availability for disk storage. The FBI will leverage stringent service-level agreement parameters.

Implementation and Maintenance

Implementation is not anticipated to take a significant amount of time since the federal government is creating many contract vehicles and agreements with approved requirements and capacity already in place. Verification of the security issues below will likely be the longest process. The FBI anticipates rolling C2S out in stages.

The FBI is developing granular cost models for each agency at the application level. The granularity of the model will include software, employee salaries, and real-estate costs for leased environments, attributable to each application. For example, it will know how much electricity should be allocated to run the hardware, and how much to run the cooling devices for each application. Each application and/or system will pay according to the model. The sunk costs setting up the environment are being paid from a base budget and there are no plans to recoup past costs.

Security

The FBI CJIS Division created the CJIS Security Policy (CSP) for all users of unclassified, law-enforcement-sensitive data. Regardless of whether an entity uses an in-house cloud or outsources its compute/storage to a C2S, the same security, protection, safeguarding, data integrity, and processes must remain in place. The CSP was clearly written when cloud was immature, but much of it will be applicable to C2S.

Having said that, the FBI remains concerned about a number of items, as provided and documented in its internal cloud report. Concerns include:

- Who from the C2S vendor has access to the storage and compute where the data resides?
- Does the data and compute remain within the continental United States?
- Are there rogue connections to the compute and storage not associated with the government's compute and storage connection that serve no purpose that benefits the government?
- How will law enforcement data be protected from access, disclosure, etc., during updates and firmware changes?

In addition to the concerns noted above, consideration will be given to performing encryption in transit and at rest, assuring that data is unusable if compromised, data is not exposed incorrectly, and the integrity of the data is paramount in any cloud solution, particularly in a C2S solution. Policy and contract requirements will ensure that nothing can be compromised, manipulated, or exposed.

Key Challenges

Currently, the adoption of commercial cloud services is managed by each of the teams responsible for a specific application set. This has led to a variety of implementation approaches and makes future management more complicated.

Recommendations

Reflecting on those applications already moved into the cloud, the FBI feels there is a lot of unnecessary worry and concern about cloud; this stems from the traditional mindset of wanting to physically control the location of one's hardware and data. Recommendations include:

- Ensure a good communication plan, because you'll find yourself saying, "I did not think of that" many times during the process.
- Expect everything, and expect strange requirements.
- Do not expect to complete within a certain time frame.
- Set realistic goals.
- Crawl, walk, run, with some breakage during the process.

For more information on the FBI's Cloud Risk Analysis and CSP documents, see the link below. Note that these are not the final versions, and not the complete set of guidance and policy to be produced.

https://www.fbi.gov/about-us/cjis/CJIS%20Cloud%20Computing%20Report_20121214.pdf

ORANGE COUNTY

Introduction

The Orange County data sharing initiative arose out of a small project in the 1990s that sought to curtail annual overtime costs of US$4 million being paid out to officers waiting in court to testify for the DA; the lack of visibility into officers' schedules across jurisdictions and for different cases led to these cost overruns. Therefore, the initial push to share information across agencies and with the courts arose out of a cost-cutting initiative.

Stakeholders and Governance

The implementation spans all of Orange County, including 23 full-service cities (meaning cities with independent police agencies and fire, paramedic, and water services), a further 12 cities covered by the Orange County sheriff's department (board representation by the Orange County sheriff's department), the Orange County District Attorney's Office, the Probation Department, the Court system, and the Public Defender. Also participating are a number of larger college police departments including California State, Fullerton, and University of California, Irvine. The total citizen population covered under the arrangement is approximately 3.5 million, over an area of around 200 square miles.

Similar to ARJIS, Orange County's cloud deployment is set up as a Joint Powers Authority with 17 voting members; formally initiated in 2005, implementation took until 2009 to fully complete. There is a financial commitment from each of the agencies based on population, with a couple of minor exceptions such as the Orange County sheriff's department, which represents 650,000 people, and the DA, which represents the whole county; they are charged a fee to participate that is not commensurate with population. Some of the organizations have historically taken on a bigger commitment to accommodate the group's success — the City of Santa Ana managed the IT for free initially, another city managed the finances, and the Attorney General worked on the legal side for free initially. These organizations are now being compensated for these efforts in the budget.

Technology Scope and Parameters

Orange County operates a private cloud data sharing initiative hosted out of the City of Santa Ana's IT organization. All member agencies have access to the data and, while managed out of the IT shop of a member agency in rotation, all of the equipment is owned by the conglomerate. Data sharing between agencies is protected by the pre-existing law-enforcement-grade network, a T1 network between all the agencies, the sheriff's department, and the City of Santa Ana. Storage is managed in the City of Santa Ana's datacentre. Data is backed up to two separate, independent third-party sites.

The system manages a wide variety of information — each agency's CAD, RMS, etc., and then specific systems a given agency might have, such as license plate readers, juvenile probation, citations, mugshots, jail management systems, etc. Orange County is considering introducing more biometric data, DNA evidence for example, for which there is a slightly different set of data management procedures.

Orange County is leveraging a number of analytics solutions on top of its cloud deployment including IBM's i2/COPLINK/Face Match, and Tyler Technologies for citations. To cite one example of the value it is able to derive through analytics, recently a crime analyst was able to match a photo using COPLINK Face Match and identify a suspect very quickly.

Implementation and Maintenance

Beginning in 2005, the integration of approximately 30 different CAD and RMS systems was done by the predecessor to COPLINK — a company called Knowledge Computing. The system allows member agencies to block out sensitive information should they choose. Some of the issues encountered then recur when member organizations migrate to new RMS and CAD systems. As noted in other case studies in this document, on-premise solutions are becoming increasingly rare. With IBM currently contracted as its systems integrator, ongoing integration is perceived as being quite expensive and it is finding funding upcoming integrations a challenge. This is complicated by the relative age of the solutions and that none of the core systems are based on any consistent standards. The annual budget to support the data sharing initiative is US$3.54 million.

Challenges

One of the challenges early on was that the majority of agencies that had digital access to their data were the larger agencies, and they were concerned that what they were signing up to pay for was access to their own data. Over time, however, more agencies were able to contribute and the benefit was shared more evenly across the member organizations.

Another challenge that continues in some part today is that the solution that is selected is best for the whole group of agencies as opposed to what might be best for one particular agency.

Orange County has recently been talking with IBM and Microsoft about adopting one of their government cloud solutions. While Amazon and Microsoft have both been CJIS certified through the State of California's Department of Justice, the board and the chiefs in the county are hesitant to move further into cloud or into a vendor's government cloud because of security concerns.

Originally, the issue of mutual indemnification prevented a number of organizations from joining the consortium. Recently, however, they have made some key amendments to the structure of the JPA, and involved risk assessment professionals who have been able to illustrate that the risks of not participating outweigh the risks that one's data could be compromised. Additionally, they have purchased insurance to protect against instances of data misuse.

Benefits

Overall, each of the member organizations is able to access more digital information, with less effort, more quickly.

Having access to a large pool of data has made people take the time to enter information they wouldn't have previously. For example, the system can search partial license plate entries, so officers enter them today whereas previously it would have been perceived as a waste of time; both the volume and quality of information entered into the RMS and the CAD are far better overall as a result.

Lessons Learned

- **Pay attention to governance.** The broad base of membership was noted as a critical success factor; the governance arrangements were constructed thoughtfully from the outset — all of the organizations, regardless of size, jurisdiction or mission, feel well-represented.
- **Align to CJIS.** Adopting CJIS allows organizations to share information more broadly than their immediate multi-agency setting should there be interest or need. For example, Orange County receives a large number of requests from Las Vegas PD as there are a lot of people travelling back and forth each week. They are currently in discussion about how to ease the information sharing across those state boundaries by leveraging the CJIS standard, and the ability to operate without mutual indemnification.

- **Learn from partial rollouts.** Orange County stressed that waiting until all of the organizations are 100% on board was unrealistic – rarely is everyone on the same page at the time. Orange County recommended getting 70% or 80% of the organizations onboard and rolling out. This gives organizations the opportunity to implement, enhance the product, and attract more organizations to an iterated product.
- **Have realistic and consistent expectations.** Sometimes there are false standards that are erected for digital systems and solutions that do not exist in the traditional, paper equivalents. In the example cited by Orange County, it was experiencing some initial resistance to automating bookings because staff weren't sure what to do with an error. On paper they would simply erase and re-enter – the same as hitting backspace and re-entering.

LONDON METROPOLITAN POLICE

Introduction

Similar to the Dutch National Police (as highlighted later in the report), the London Metropolitan Police (the Met), because of its existing infrastructure investments and some trepidation over public cloud solutions, is implementing a private cloud digital evidence management system starting first with its body-worn video, then moving on to incorporate other digital assets. Cost efficiencies and public confidence improvements were key drivers in the migration to private cloud.

Stakeholders and Governance

While we sought to profile organizations operating digital evidence management solutions across multiple agencies, the size of the Met, and the installed base of its existing CCTV video feeds, meant that the case study was of considerable interest to the project team. The Met shares its body-worn video with the Crown Prosecution Service via the CJEX network. At the moment it is not planning to incorporate video feeds from other, external organizations such as private security firms or privately owned videos.

Technology Scope and Parameters

In the fall of 2014 the Met began an 18-month body-worn video pilot, deploying 1,500 cameras with patrols across 10 London boroughs. The pilot successfully demonstrated the value of BWV and the Met formalized its plans to expand the initiative. It received interest from seven digital evidence management solution vendors, from which it shortlisted three vendors. Procurement was limited to a list of prequalified vendors so the Met could implement more quickly. Ultimately the Met signed a three-year contract with Taser and its Evidence.com solution, with private cloud hosting from integrator CSC. The Met will begin implementation in May 2016, rolling out to more than 22,000 BWV units by the end of 2016. Funds to support the initiative are being generated from the sale of underutilized police buildings.

CSC was selected as part of a €250 million contract to outsource a large portion of the Met's IT service delivery, including the private cloud for the BWV initiative. IT service delivery in the U.K. has been broken out across separate vendors in the following discrete "towers," two of which were awarded to CSC:

- Infrastructure and end-user services (CSC)
- IT hosting (CSC), including IaaS, PaaS, and SaaS
- Application management (Accenture)
- Networks (TBD)
- System integration management (Atos)

Implementation and Maintenance

Strategically, the Met was somewhat limited by the purchasing framework for the pilot; it had to buy a BWV solution as opposed to a broader suite of digital evidence management because it could leverage a prequalified list of BWV suppliers and implement far quicker. However, it is aware that BWV is just one of the many types of digital assets needed to be managed and integrated into a digital evidence management system. In addition to the traditional digital assets like digital interview recordings and custody audio and video recordings, the Met maintains a footwear database of shoe imprints and has the highest CCTV installed base of any metropolitan city in the world. The Met plans to integrate these digital assets into a comprehensive system in the near future.

Longer term the Met will revisit the possibility of migrating to public cloud. It is also moving forward with plans to integrate its core policing platform (CAD, RMS, etc.). This is currently in the requirements phase, and will likely take two years to launch, as there are approximately 30 separate systems to embed in a new integrated platform. One problem here is trying to determine whether it could use one single application or whether it would need to stitch together a number of products. The intention is to migrate core policing systems — case files, custody, MIPS, intelligence (everything short of counter-terrorism) — into one system.

Security

While the Met considered public cloud solutions and hosting, the public cloud providers did not meet the U.K. government protective marking schema (security clearances) which required a public hosting vendor to be rated "2" or above; the public cloud vendors it assessed achieved ratings of "0." For BWV there are a number of ISO and operational standards around the solution, as well as a raft of standards for private cloud.

Challenges

- **Storage costs.** Storage management issues are a challenge for BWV projects, and the lack of certainty around public cloud storage costs in effect was one of the reasons the Met chose to select a private cloud solution. Tied to this were fears around the exponential growth in storage needs as BWV rollouts are implemented. Officers currently videotape an average of 15–60 minutes per day. Were that to double, or potentially grow to 5 hours a day, then the public costs would become prohibitive. An additional challenge noted by the Met was that public cloud providers don't typically charge organizations to integrate data, but charge considerable amounts for extraction. Lastly, public cloud solutions raise significant data residency concerns.
- **Network load.** Uploading the content was also somewhat problematic in that there was a sizeable network load at the end of the officers' shifts.
- **Integration.** There are sizeable integration challenges with the Met's 3,000 CCTV cameras, and the images it can collect from the 17,000 other council and local government cameras to which it has access. Many of those cameras are analog and need to be converted to digital.
- **Training.** The other challenge it is addressing is training 22,000 officers on proper recording, use, and upload procedures.

Benefits

BWV was seen as an excellent way of increasing transparency and protecting the public and the officers themselves. The London BWV pilot — the largest on record — highlighted some tangible benefits, including a 33% reduction in allegations against officers in the trial. Additionally, there has been a significant increase in guilty pleas because of the availability of video evidence.

The benefits noted of moving to the cloud were textbook: speed, agility, deployment times, etc.

Lessons Learned

The Met cautioned organizations to pay attention to, and prepare for, the network impact involved in uploading the content. Additionally, although much of the pilot was done in standard format video, there is great interest in moving to HD, and the Met would encourage others to investigate different formats, functionality, and operating costs in that regard.

THE DUTCH NATIONAL POLICE

Introduction

The Netherlands consolidated 26 police forces into one — the Dutch National Police (DNP) — in 2012. The DNP has deployed an open source digital evidence management system predicated on its Big Data initiative.

Stakeholders and Governance

The IT organization supporting the DNP also manages the needs of 35 government agencies including all other security, cybercrime, and intelligence organizations in the country. This currently encompasses 20,000 users, but is being scaled up to 60,000 users by the end of 2016. The IT organizational structure is flat. Small, highly skilled teams rapidly deploy leading-edge technology. Nearly all of the technology used is open source. There are a number of key features and strategic pillars guiding its approach to IT service delivery. They are open by default, focused on agility, and try to embed "fast innovation" into their processes by mimicking the innovation culture and processes at Google and Facebook. Additionally, they are trying to build applications and services that can be shared across all member organizations, and deliver remote access to all systems. Lastly, everything the organization deploys is multi-redundant by design. The organization perceives everything to be data.

Technology Scope and Parameters

The DNP's cloud solution is large and privately hosted within the DNP datacentre. The centre currently houses 250 physical servers, which is expected to grow to 600 by the end of 2016, and manages 12 petabytes of new data monthly. The decision to leverage a private cloud solution was as a result of recent infrastructure investments, as well as concern over the legal issues around procuring public cloud solutions from U.S.-based providers.

The open source technology used for the cloud solution is OpenStack, with Ceph providing the cloud storage layer. The DNP has been a heavy Hadoop user since 2012 so the leap to open source cloud provision was somewhat natural. Scalability was the key business driver; the DNP wanted to scale out horizontally, but at the time it could not anticipate exactly what data it would want to leverage in the future.

All of the DNP's software licenses are open source, so it must give back everything it builds or develops to open source repositories. The most common open source software the DNP leverages to manage its infrastructure, cloud, and analytics are listed below.

TABLE 1

Open Source Software Currently in Use

OpenStack (open source provider)	Kafka http://kafka.apache.org
Ceph as cloud storage layer	Redis http://redis.io/
Linux (Ubuntu) http://www.ubuntu.com/	Java/Python/C/bash, etc. programming languages/scripting
OpenStack http://www.openstack.org/	Jenkins https://jenkins-ci.org/
Ceph http://ceph.com/	Puppet https://puppetlabs.com/puppet/puppet-open-source
Sensu https://sensuapp.org/	Ansible http://www.ansible.com/
Flapjack http://flapjack.io/	Rundeck http://rundeck.org/
Docker https://www.docker.com/	AngularJS https://angularjs.org/
Hadoop https://hadoop.apache.org/	Bootstrap http://getbootstrap.com/
Spark http://spark.apache.org/	Redmine http://www.redmine.org/
Storm http://storm.apache.org/	MediaWiki https://www.mediawiki.org/wiki/MediaWiki
Cassandra http://cassandra.apache.org/	WordPress https://wordpress.org/
MongoDB https://www.mongodb.com	Logstash https://www.elastic.co/products/logstash
MySQL (MariaDB) https://mariadb.org/	Graylog https://www.graylog.org/
Galera http://galeracluster.com/	Grafana http://grafana.org/
PostgreSQL http://www.postgresql.org/	InfluxDB https://influxdb.com/
Elasticsearch https://www.elastic.co/	Gitlab https://https://about.gitlab.com/

Source: IDC, 2016

Implementation and Maintenance

Both their cloud and Big Data initiatives started in 2013/2014, emerging from smaller pilot projects to test basic requirements. Within a year, the IT organization had grown to 10 FTEs, who were able to set up the final technology implementation in four months. Attaining this speed of deployment required significant preparation, professionals with the right skills, and the right tools. The cost of the implementation was €2.5 million.

Security

The DNP believes that securing cloud deployments can be more difficult than for non-cloud deployments. As a result, the DNP felt that it needed to create its own security baseline.

Key Challenges

- Having achieved a higher level of maturity than other countries in both cloud and Big Data deployments, there are few other nations to turn to for advice, help, or inspiration. "One of the problems we face is that we're at a totally different level of maturity than other countries around us or globally," the DNP said.
- Open source repository rules are a challenge for traditionally minded government.
- Establishing high-speed connectivity to manage the content is difficult and expensive.
- Change management can be a major challenge, simultaneously exciting in terms of the potential innovations at hand, but also daunting in that the organization will be operating in uncharted territories.
- The DNP's cloud implementation has opened up an entirely new set of potential ways to work, conduct investigations, and manage data.
- Existing legal statutes written in an era prior to Big Data can cause friction.

Business Outcomes

- The DNP is able to connect the dots faster; for example it can now run real-time risk analysis on Twitter data/feeds in 10 milliseconds to determine if a given threat is a concern.
- More sources of information about a given entity brings clarity; understanding a given MO across a number of jurisdictions can help to pinpoint who might be a suspect.
- The DNP is able to move toward a model of predictive policing: combine the data, predict results from just the metadata.

Recommendations

- Although it sounds like a technological cliché, the DNP wanted to stress that organizations should have faith in the agile environment.
- Leap, and the net will appear: "Trust it without being able to understand or control what is going on."
- Focus on future possibilities; there are benefits you don't even understand right now.

KEY FINDINGS

Use of cloud for multi-agency evidence management is relatively nascent as evidenced by the small number of organizations having deployed a solution.

For leading organizations deploying cloud solutions, there is a mix of private and public cloud based solutions with some employing hybrid solutions (a combination of on-premise and cloud solutions). The appropriate deployment model will depend on available infrastructure, skill sets, cost considerations, future datacentre plans, availability of public cloud solutions, and security requirements.

RECOMMENDATIONS

The following key recommendations are based on the case studies undertaken for this report:

- **Governance.** The vast majority of the case studies stressed that organizations beginning on multi-agency data sharing arrangements should pay special attention to governance. Comparatively, technology is the easy part.
- **Multi-agency focus from the onset.** Tied closely to the economic challenges currently facing law enforcement, we recommend that organizations fundamentally change the

operational ecosystem so that various units within a given organization, and among multiple agencies, pool resources and create centralized cloud repositories.

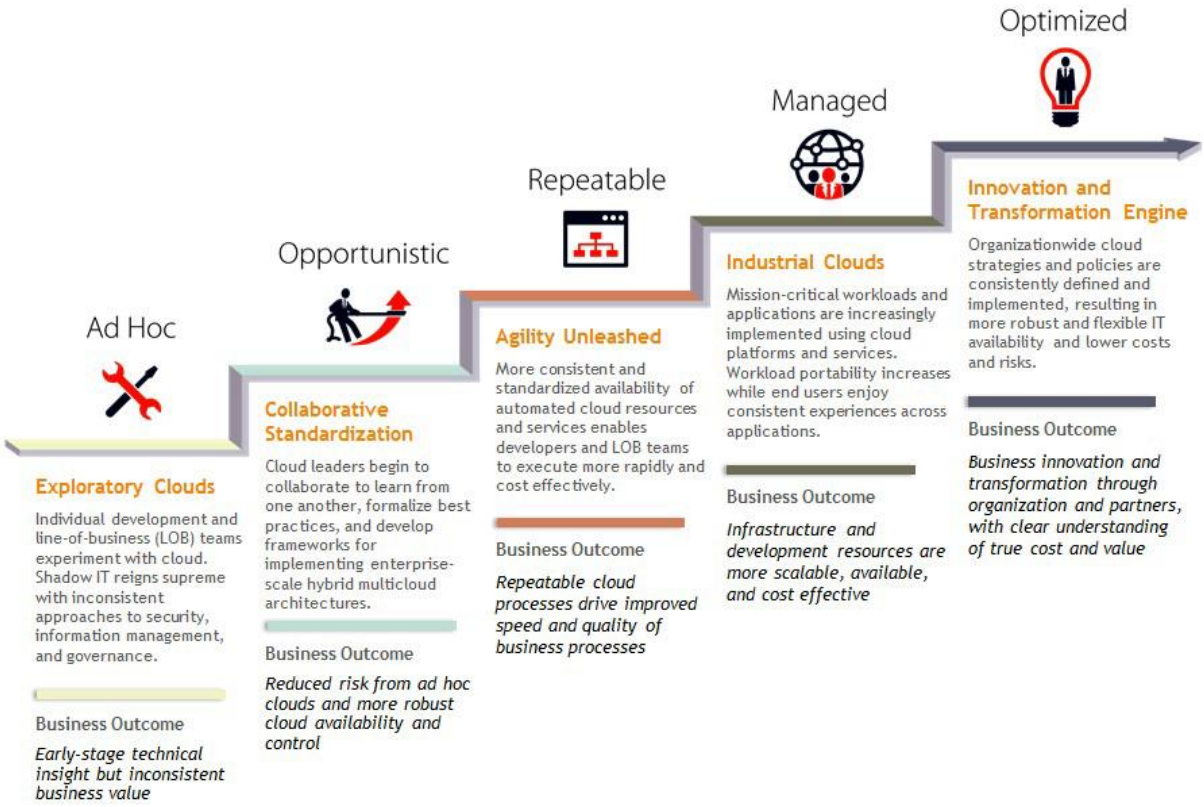
- **Data quality.** Data quality and validation is critical to leverage insights across multiple agencies, and organizations typically underestimate the amount of effort required to harmonize and integrate information from multiple systems and agencies. Information exchange models such as NIEM will become invaluable in ensuring that data sharing can occur as fluidly as possible.
- **Seek out scalability and integration ease.** Irrespective of the cloud deployment model being implemented, users stressed the need to build or purchase a scalable architecture that can accommodate and manage all digital assets.
- **Mobile.** For many of the organizations in the study, mobile is the next frontier for effective police service delivery. Participants urged organizations to mobile-enable core business solutions as officers need to be able to both enter and receive real-time data to enhance situational awareness.
- **Start small and scale.** Start with a pilot or limit the initial scope of digital evidence to be included. This ensures a reasonable deployment time. Successful implementations can be used to validate future expansions.
- **Align to endorsed standards for cloud security.** While there is currently no agreed standard in Canada, a consensus seems to be forming that security for public cloud solutions should meet a standard such as the FBI CJIS Security Standard or the U.S. FedRAMP. Moreover, the consensus in the law enforcement community is increasingly that compliance should be the responsibility of the cloud solution provider and its datacentre partners.
- **Quantify business outcomes.** Quantifying business outcomes was a priority for a small minority of the organizations profiled, but each believed that its cloud initiative was valuable. IDC recommends that organizations define key KPIs prior to implementing a cloud solution to substantiate further business investments.

NEXT STEPS

Internationally, the movement to multi-agency cloud deployments has begun and is demonstrating its ability to enhance public safety and improve efficiency. To realize these benefits, Canada will need to align the findings in this report with the Canadian Community Safety Information Management Strategy (CCSIMS). CCSIMS sets out Canada's information management strategy, goals and priorities, paying particular attention to governance, planning, technology, training and exercises. Together this will facilitate the development of a Canadian law enforcement information management strategy that offers a single vision on how to move forward collectively with respect to digital asset management, and provides guidance on endorsed data sharing and security standards in the cloud. The government, law enforcement agencies, and other data sharing entities are encouraged to examine existing standards and adapt parallel national standards as quickly as possible.

FIGURE 2

IDC's MaturityScape Cloud Stage Overview



Note: Excerpted from *IDC MaturityScape: Cloud* (IDC #259534, October 2015)

Source: IDC, 2016

STAGES OF IDC'S CLOUD MATURITYSCAPE

IDC's Cloud MaturityScape traces cloud computing across five stages, from the ad hoc stage to the optimized stage. The following sections describe the stages and highlight the fundamental outcomes at each stage.

IDC carries out extensive maturity modeling across these stages, some of which is driven by IDC's *CloudView Survey*. As one measure of maturity among many, the percentage of IT respondents (director and above, including more than 400 CIOs and CTOs) who said that when either replacing capability they now have or sourcing net-new technology, they would approach their selection process using a "cloud last," "cloud first," or "cloud also" mindset, was considered and is mentioned at each stage.

Ad Hoc

Description

Line-of-business units, in particular, begin to increase their awareness of cloud technology options, key considerations, and cloud's contribution to IT efficiency. There is limited awareness, or use, of third-party professional service providers to help build or implement cloud services. There is very limited experimentation with private clouds, with organizations looking first and foremost to extend

application categories that have already been virtualized. With private cloud implementation, the enterprise has started to integrate "automation" and "self-service" into virtualized IT infrastructure, but "standardization" is limited. Complications stemming from the need to scale, the need to build integrations to data sources, and the increasing need to make complex configurations begin to drive more reconnection with IT leaders to get developer and other resources. But business goals are simple — find, retain, and serve customers — and internal IT service supply in this stage is unable to meet these needs in an agile way.

As a sourcing measure, IT leaders are reluctant and unlikely to consider cloud for new solutions, and according to maturity modeling based on IDC's *CloudView Survey*, the measure of "cloud first" sourcing is about 19% in ad hoc companies, with about 43% "cloud also" and 38% "cloud last."

Business Outcome

In the gap between backlogged IT service supply and the requirement to build new technology capability (mobile, social, and systems of transaction and engagement) services to chase new business, many sales and marketing organizations turn to SaaS because of the immediacy of the IT or business need and the ability to procure capacity with minimal monthly or one-time investments that require little or no formal approval. There is limited enterprisewide awareness of these activities even between non-IT business units. SaaS use is operational and driven by valid, though "pro tem," needs, promoting a growing "shadow IT" run by administrators in lines of business, particularly marketing and sales but also human resources.

The business leaders' focus is very much on customer acquisition/attrition and revenue impact/profit margins, and "business" goals are mostly abstracted from the IT organization they have at hand. Driven by metrics such as customer retention, average spend per transaction, or the time a customer spends on a web site store, LOB managers are most interested in how effective the business services delivered by IT are in meeting these goals, and they tend to look outside the organization first, within their budget limits. At smaller firms, this "outsourcing" comes with the express approval of CEOs and CFOs who are pushing for growth and expansion. At midsize firms, both ITDMs and BDMs have little experience of working in concert.

Opportunistic

Description

IT organizations experiment with more standardized offerings, and develop short-term access to SaaS offerings on an as-needed basis, and on sourcing "pro-tem" IT solutions that speed up, or instrument, existing IT tasks. Line-of-business organizations promote buy-in to cloud computing across the organization and the C-suite begins to acknowledge the need for an enterprisewide approach. IT leaders — particularly developers and solutions architects — begin testing their ability to transition jobs and workloads from existing traditional, in-house or outsourced IT deployments, and the efficacy of building net-new applications and services. As a sourcing measure, IT leaders begin to consider cloud for new solutions or isolated computing environments with minimal impact on existing business processes, lower implementation costs, and/or faster delivery for commodity resources. IT organizations lacking skills internally begin to consult with third-party professional services to help develop cloud assessments, strategies, and future implementation road maps (i.e., which workloads to migrate to which cloud environments).

The measure of "cloud first" sourcing is about 31% in opportunistic companies, with about 35% "cloud also" and about 34% "cloud last." Also, IT is starting to regularize the activity of gathering business requirements from key stakeholders in targeted departments/functions (e.g., sales, marketing, HR, and finance) to help select appropriate cloud solutions and identify which features are needed today and how those features might apply to a wider base of users in the future.

Although cloud usage may be sporadic across the business, security requirements should be thorough by this point, particularly for IaaS and PaaS usage.

Business Outcome

The business begins to promote buy-in to cloud computing and an enterprisewide approach, experimenting with short-term improvements in access to IT resources via the cloud. The beginning of the enterprisewide approach to cloud leads to an increase in corporate IT governance. Business and IT teams collaborate to identify key risk management concerns on a project-specific basis. IT efforts to build new services for the business (particularly with web front ends for customer campaigns, data services, and dashboards for business analysts) help create the basis for a more agile and service-oriented delivery to the business. In some cases, both parts of the business begin to see the first signs of cost savings, which, at many firms, will result in new experiments and innovation. In addition, the beginning of the enterprisewide approach to cloud leads to the beginnings of the expansion of the business risk management/governance role to external computing and multisource data management.

Repeatable

Description

Organizations enable more agile access to IT resources through aggressive standardization, maintained service catalog, cloud best practices, and governance. Business and IT users begin to rely on self-service portals to access cloud services based on cost and quality of service, and automate approvals and workflows to rapidly provision and activate services. Users have access to a wider range of resources with more predictability and transparency into the cost of those resources, and the ability to more easily forecast their IT resource requirements. Organizations are building internal competencies and skills to support the delivery of cloud computing, either as standalone offerings or in conjunction with legacy IT operations. Where they don't have the skills available internally, organizations are identifying which third-party IT service providers are best suited for each stage of the services life cycle (plan/design, build, run, and support).

These organizations are formalizing "business outreach" functions, putting dedicated IT staffers on the task of liaising with key business line leaders to source new initiatives, review business requirements and KPIs, help weigh costs and value, and shepherd winning projects to the right IT resources for planning. In tandem, IT also formalizes the process to continually review business in targeted departments/functions (e.g., sales, marketing, HR, and finance) using SaaS services and to bring IT discipline to reviewing cloud solutions in use, looking at performance, logs, and trouble tickets, with an eye to playing a broker role. Part of this role includes identifying which features are needed today and how those features might apply to a wider base of users in the future. Although cloud usage may be sporadic across the business, security requirements should be thorough by this point, particularly for cloud middleware and infrastructure services. According to IDC's *CloudView Survey*, the measure of "cloud first" sourcing is about 39% in repeatable companies, with about 40% "cloud also" and 21% "cloud last."

Business Outcome

Repeatable cloud processes drive improvements in both the speed and quality of business processes, and the business team's direct app requirements to the IT team (application-specific KPIs, best practices, and even SLAs) to leverage repeatable best practices across business units. A select pool of end users begin to have access to IT-built self-service functionality for selected SaaS services and cloud resources. IT has enabled business users to have more agile access to IT resources through standardization and implementation of best practices, and users are more readily relying on self-service portals.

Managed

Description

Managed-stage organizations have developed a consistent, enterprisewide approach to cloud based on industry best practices, speeding iterative improvement cycles to increase cloud adoption and business value. Organizations are orchestrating cloud delivery across an integrated set of IT and professional service resources, and collaborating internally and externally to support their future technology needs. Users can procure additional services, add new users, and increase or decrease compute capacity as needed through self-service portals, expanding the organization's ability to operate not just more efficiently but also more strategically. Organizations can quantitatively justify why a cloud service is running on-premise, in a private cloud, or in a public cloud setting. Metrics are based on cost, uptime, user satisfaction, usefulness/availability of features, and adherence to compliance requirements/standards, among other criteria.

Clearly, the appeal of cloud infrastructure is a reduced datacentre footprint, reduced utility cost, and reduced IT staffers to operate IT subsystems. The demand for IT operations staff is lower in managed and optimized organizations because they are using provider (public cloud or hosted private cloud) storage and compute services being maintained by external teams. Part of the goal of repeatable, managed, and optimized growth is greater efficiency, and this outsourcing is part of this effort. But very few organizations we work with decide to reduce headcount from their core operations staff: aside from developers and DBAs, a host of existing roles take on great importance and new ones emerge.

Network operations, application performance, web and infrastructure security, automation, web performance, and similar roles focused on positive customer (internal and external) experience grow in importance. Newer roles like data managers, vendor managers, and agility teams (outreach teams to reconcile technology projects originating in the LOB) become more important in this stage.

The measure of "cloud first" sourcing is about 47% in managed companies, with about 34% "cloud also" and 19% "cloud last." According to IDC's *CloudView Survey*, managed-stage companies use some form of public cloud 89% of the time, and 91% of managed-stage companies have implemented at least one enterprise private cloud service.

Business Outcome

The business is expanding its consistent, best practice, enterprisewide approach to cloud, speeding iterative cycles to increase cloud adoption and value.

By moving from fixed long-term costs to flexible, variable consumption-based opex expenses, organizations achieve a more flexible operational model. Leveraging cloud deployments speeds up provisioning, which enables faster testing cycles for IT solutions and a more agile business. For SaaS solutions, organizations are more flexible with budgeting and actual spending. Capacity that bursts into public clouds at peak loads increases their agility.

BDMs begin to articulate business KPIs for their customer-facing services (web sites, commerce sites, business networks, integration to social media, and marketing campaigns) using terms that are shared by IT leaders: high-availability, fault-tolerant, and performant applications; quick-loading web content; seamless transactions; and modern, satisfying CX. As the supply of IT capability (SaaS applications; integrated PaaS platforms to build, test, and iterate web products and content rapidly; data analytics and visualization services, etc.) in the provider-based cloud increases, and more of the managing of underutilized applications, customizations, and reports falls away, the IT service supply becomes far more agile and responsive to the business needs of now and the near future, not yesterday and the past few years. Greater synchronization of effort and direction

between ITDMs and LOB leaders about the effective use of technology (what's possible) to guide strategy (what's profitable) grows more mutually beneficial to business goals.

Optimized

Description

Optimized organizations are driving business innovation through seamless access to IT and professional service resources from internal and external service providers and by making informed decisions based on the true cost and value of those services. They are using cloud to lower the costs and speed up the delivery process. The business impact is most noticeable for new initiatives as well as for high business value or highly innovative projects such as industry clouds, where some level of customization of IT resources is critical and risk sharing creates an environment that fosters innovation. These organizations have the ability to leverage their IT capabilities as a component of new products and services. IT is an equal partner in achieving long-term business goals, and IT is responsible for ensuring the successful delivery of IT capabilities throughout the life cycle of those technologies.

Optimized organizations have identified all sources of IT-related spend throughout the entire business and have worked with business units to test assumptions about which external applications, projects, contracts, and services are viable and important to business growth, using a "business lens" calibrated with IT controls. A goal of optimized IT organizations is to be the trusted broker for >75% of all IT-related spend for the company, including IT outsourcing, business process management, systems integration, and SaaS services.

As broker, the IT organization is an internal accelerator for business access to services, whether IT created or IT sourced, and to provide policy-based access to best-in-class IT resources for all its users. Optimized IT organizations are far more appropriately capacitized than their counterparts (generally 70% of application services and packaged software seats are utilized, far above the benchmark 30%–35%), and that percentage is expected to increase every year. The most optimized large IT organizations IDC has encountered effectively source, manage, and internally provision around 95% of the entire scope of IT capability consumed by their companies, delivering best-in-class IT services from both internal and external IT developers as part of a combined service list with costing and chargeback capabilities.

3rd Platform technologies such as 3D printing, the Internet of Things, cognitive systems, robotics, and drones enabled by the cloud accelerate digital transformation and enable innovation, allowing IT leaders in optimized organizations to launch initiatives around new value propositions created from partnerships with other companies, sometimes in completely different industries.

The measure of "cloud first" sourcing is about 61% in optimized companies, with about 31% "cloud also" and 8% "cloud last." According to IDC's *CloudView Survey*, optimized-stage companies use some form of public cloud 64% of the time, and 95% of optimized-stage companies have implemented at least one enterprise private cloud service.

Business Outcome

Business organizations in the optimized stage are themselves optimized as IT consumers use technology appropriately to guide their strategy and innovation. Optimized business organizations have done the math to use real IT service costs as part of their cost-benefit analysis in building new campaigns and business models rather than viewing IT as a cost center. Users benefit from optimized IT organizations driving business innovation through seamless access to IT capability, based on the value to business, using transparent metrics and measures. Using automated costing and feedback, these organizations are making informed decisions based on true cost and value with internal and external partners operating at speed of business as standard operating

procedure. The mechanisms for procurement, contracting/subscription, vendor management, and SLA monitoring are automated and abstracted from users. Optimized IT organizations have a standardized process in place for dedicated "agility" teams to work with key internal "consumers" to evaluate possible projects and products based on their true costs over time, driving positive business outcomes.

Optimized organizations are well primed to adopt industry cloud services, as both a consumer and/or a provider of these services. Many optimized organizations have in the past few years made a major change, redirection, or addition in their revenue-generating business models, and of the 2,200 SaaS ISV organizations IDC tracks, nearly 10% are "sector" companies that had no "aaS" business revenue before 2014. For these companies, the change in business model enabled by digitization and subscription delivery has given them a new direction and access to new revenue. The optimized IT organization and senior IT leadership do not only optimally serve their internal audience, but they have effectively merged with the key revenue-generating functions (R&D, sales, and marketing) to create and drive innovation and profit through new digital offerings.

DIMENSIONS OF IDC'S CLOUD MATURITYSCAPE

Table 2 describes the major dimensions (vision, people, process, and technology) of IDC's Cloud MaturityScape, along with the relevant subdimensions that make up each of the dimensions.

TABLE 2

Major Dimensions (Vision, People, Process, and Technology) of IDC's Cloud MaturityScape

Dimensions/Sub-Dimensions	Stage Names				
	Ad hoc	**Opportunistic**	**Repeatable**	**Managed**	**Optimized**
Vision					
Strategy	Project-driven clouds are treated as pilots or experimental projects and used for learning purposes.	App developers and IT teams collaborate to define best practices and reuse opportunities.	Standardized cloud service catalogs and automated self-service access are available to selected groups.	There is a consistent, enterprise-wide approach to cloud based on industry best practices and specific business needs.	An enterprise-wide cloud-first strategy is implemented; technology guides strategy in the pursuit of business excellence.
Leadership	Organizations are led by individual BDM and ITDM champions with little-to-no coordination across projects.	LOB organizations lean on SaaS; C-suite begins to acknowledge the need for an enterprise-wide approach.	Business teams direct app requirement to IT team to leverage repeatable best practices across business units.	Business and IT leaders use standardized services, tools, and shared best practices.	Business and IT leaders follow well-documented standards and continuously iterate over improvements.
Risk management	Cloud workloads are non-sensitive and require little security oversight.	Business and IT collaborate to identify key risk management concerns on a project-specific basis.	Consistent, automated data protection and access control are applied across cloud services.	Maturing cloud CISO and CCO functions view the whole spectrum of IT procurement and begin to play oversight role.	Security, business continuity, disaster recovery, and compliance programs are architected with cloud-first priorities.
Technology					
IT infrastructure	Most projects use SaaS services sourced independently by individual BDMs or departments.	Public and private cloud infrastructure is used on a project-by-project basis with limited coordination.	Infrastructure choices are standardized, sourced by IT, and driven by policy.	Workload portability and consistent software-controlled infrastructure use enable improved agility.	Hybrid public and private cloud architectures consistently match cloud cost, performance, and security to workload requirements.
Security	Security is often managed by individuals or departments with inconsistent compliance to corporate rules.	Security monitoring is selectively extended to cloud services but is not as well integrated as with legacy systems.	IT operations and end-user security monitoring are expanded and standardized as cloud services use grows.	Consistent, automated security monitoring, control, and reporting are the norm.	Advanced analytics proactively identifies risks and maintains compliance across hybrid cloud resources.
IT automation	Ad hoc self-service solutions provided by specific cloud services are deployed without broader integrations.	Standardized VM and middleware templates are developed and shared to drive more consistent cloud provisioning.	Automation extends beyond provisioning to support workload portability and dynamic resource scaling.	Templates and service catalogs expand to support fully automated service brokering across public and private clouds.	Real-time analytics linked to automated workflow and provisioning engines optimize resource use and app performance.
People					
Skills and training	Individual developers and IT infrastructure ops staff are "learning on the job."	Internal cloud teams begin to develop skills and best practices with help from third parties.	Best practices are well defined and supported by training for end user, dev, and IT roles.	Targeted hiring shifts to emphasize cloud-specific skills and roles.	Cloud skills are expected of all employees across all roles.
Self-service empowerment	The organization has a traditional ITIL-based approach to service request, problem, incident, and configuration management.	Selected end users and dev teams get self-service functionality for selected cloud services and resources.	A unified self-service portal is introduced to streamline self-service provisioning and control for selected services.	Users can procure additional services, add new users, and increase or decrease compute capacity as needed through self-service portals.	The default IT supply mode is LOB accessing services based on cost and reputation, not on location.
Process					
Controls/governance	IT and business teams pursue individual agendas with inconsistent alignment; consumption-aware chargeback is rarely implemented.	IT and business teams partner to selectively evaluate public cloud services and define private cloud templates.	IT and business teams partner to expand shared efforts. Consumption-aware showback is considered by some.	Highly collaborative business and IT decision making is in place, including consumption-aware showback or chargeback.	The collaborative LOB/IT governance process is institutionalized and provides ongoing cloud management leadership.
Data/information management	There is random placement of data in file sharing and other services regardless of company/regulatory policy.	IT and LOB start defining what data can be placed in public clouds or should stay on-premises.	Cloud data management policies and protections are well defined in selected business units or geographies.	Cloud data management policies and protections are well defined across all business units and geographies.	Automated data management solutions are used to proactively maintain and enforce cloud data management policies.
Cloud service provider (CSP) contract management	CSP evaluations and contracts are managed by individual groups with no IT coordination/leadership.	Individual groups run evaluations; CSP contracts are extended internally based on LOB-only KPIs.	The enterprise aligns around a minimal set of CSP evaluation criteria and centralizes larger contracts.	Organizations begin to quantitatively evaluate services based on cost, uptime, user satisfaction, usefulness/availability of features, and so forth.	CSP evaluations and contracts are based on measurable metrics and policies defined by a collaborative LOB/IT process.

Source: IDC, 2015

Source: IDC, 2016

About IDC

International Data Corporation (IDC) is the premier global provider of market intelligence, advisory services, and events for the information technology, telecommunications and consumer technology markets. IDC helps IT professionals, business executives, and the investment community make fact-based decisions on technology purchases and business strategy. More than 1,100 IDC analysts provide global, regional, and local expertise on technology and industry opportunities and trends in over 110 countries worldwide. For 50 years, IDC has provided strategic insights to help our clients achieve their key business objectives. IDC is a subsidiary of IDG, the world's leading technology media, research, and events company.

IDC Canada

33 Yonge St., Suite 420
Toronto, Ontario Canada, M5E 1G4
Twitter: @IDC
idc-community.com
www.idc.com

Copyright Notice