Future-proofing IT for Smart City services

1 Executive Summary

Smart City Services bring many benefits

Smart City applications such as street light control, smart parking and road traffic management are starting to be widely deployed around the world, bringing benefits to city operations, better quality of life and reduced costs and energy use. Currently these services tend to be deployed as stand-alone applications, but the full benefits of a Smart city will only be realised if these applications are able to share data, enabling cross-department processes, engaging citizens, and making city operations transparent to all stakeholders. In addition, many cities are growing rapidly and need to be sure that these applications can be extended and expanded as required. This means a strategy is required for future-proofing the IT used to implement Smart City services, to ensure that the city is not restricted by the limitations of an initial pilot deployment.

Hybrid Cloud offers the most cost-effective infrastructure

Cloud implementations deliver the flexibility, scalability, and cost-effectiveness needed to implement Smart City applications connecting many thousands of end-points. Many cities are starting to outsource more elements of their IT infrastructure to cloud service providers in order to relieve their IT staff of the routine day-to-day technical tasks and allow them to concentrate on the tasks that require detailed knowledge of the city. As cities implement their Smart City applications, they will find that making use of cloud infrastructure for new applications, while maintaining existing in-house infrastructure, at least in the short term, is the only practical solution. Expanding an on-premise infrastructure to support the requirements of these new applications would be a lengthy and expensive project carrying a significant risk of failure. Nevertheless new Smart City services will need to work with legacy on-premise systems and across multiple verticals if they are to deliver the full benefits that a Smart City implementation can bring. Robust APIs are the key to ensuring that services implemented in the cloud can work together in the future.

Cloud solutions are likely to be the most secure

Physical location is no longer a major factor in ensuring the security of today's networked IT systems. The most secure infrastructure is one for which all the latest security techniques are applied as soon as they become available. This is best achieved by professional data center managers for whom security is a full-time job. And it can be most effectively realized in the cloud where there is the capacity to test backup routines rigorously and to apply big data analytics to filter out the false alarms which often overwhelm in-house IT teams.

Contents

2 Introduction to Smart City Services

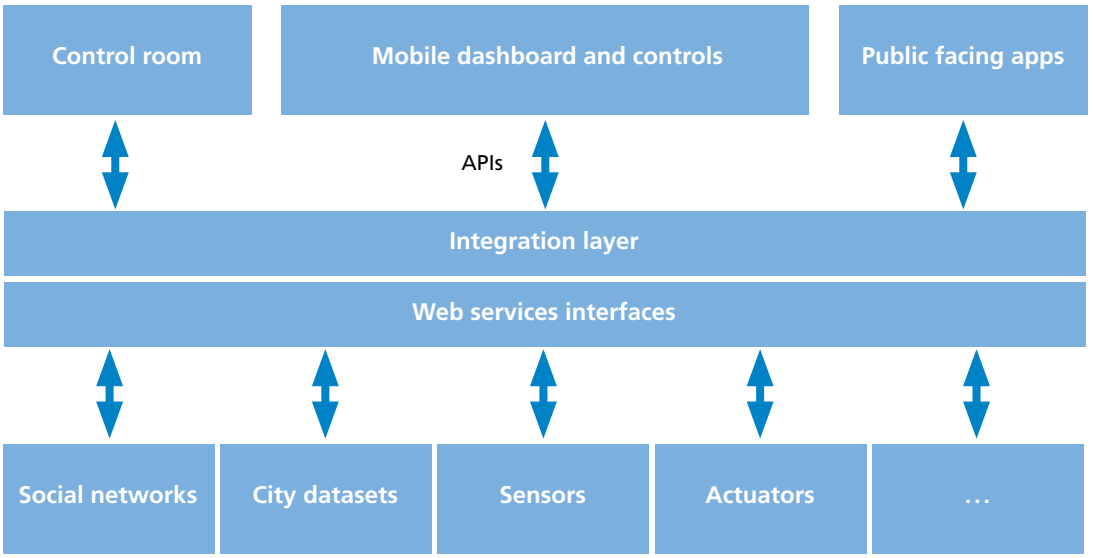
Smart Cities are high on the political agenda around the world. From China and Singapore to Barcelona and Boston, across Asia, Europe and the Americas, cities large and small are implementing schemes for connecting various aspects of everyday life. As part of this trend to adopt Smart City strategies we have seen successful deployments of applications such as connected parking and connected street lighting for which the business case is easy to make. We have also seen increasingly integrated systems connecting different aspects of the Smart City. In Helsinki, for instance, public transport and traffic lights have been connected to allow for more efficient public transport. While in Spain, Valencia has handed Telefonica a contract for comprehensive Smart City management based on the European FIWARE standard.

This White Paper provides guidance to city managers on a future-proof approach to implementing new Smart City applications that will bring the maximum benefits from the new technology by allowing different applications to work together and to scale as the city grows.

Currently, the majority of Smart City applications are deployed as retro-fit point solutions aimed at solving a single, clearly defined problem. While this may have sufficed in the past, urbanisation brings with it increasingly complex issues relating to service provision; a more integrated approach to IT infrastructure can help make these easier to manage. Over time Machina Research believes this vertical approach of running separate applications will give way to a more horizontal one. At its simplest, this would comprise an integration layer that brings together the data from the separate applications to be viewed in a single dashboard. Linking the Smart City services will improve the way in which the city operates, as data can be shared in real time between different departments, allowing for cross-department processes, engaging citizens, and making city operations transparent to both employees and citizens.

The graphic in figure 3.1 below illustrates how different elements of Smart City services can work together, either within one vertical or across several.

Figure 3-1: Leveraging cloud for city service delivery [Source: Machina Research, 2016]



To create a Smart City, sensors are deployed for many purposes, some to support specific applications such as traffic management or smart parking– for example sensing a car in a parking space, and others to provide data on variables such as air quality or light levels used by many applications. City staff have dashboards that provide the information and control appropriate to their responsibilities– and a city control room can access many different datasets to share date between departments and link data from other sources such as social media. With a thin integration layer, data is stored and managed in the separate applications so as to generate the information needed to manage that function; and the central systems provide combined visuals for multi-function dashboards along with the means to send commands to the different applications. Selected data can also be made accessible to the public.

Some cities are electing to procure more integrated systems in which the sensors, applications and social networks are linked through APIs and web service interfaces to a horizontal platform. In this scenario, the platform will manage the storage of the raw data and apply analytics across multiple applications to deliver deeper insight to city managers as well as dashboards and commands for users of individual applications. The key to this type of architecture is the interfaces between the different applications and the integration layer, which will require robust Application Programming Interfaces (APIs) so that they can work together seamlessly and securely. The City of Barcelona is currently engaged in a procurement process for a platform of this type. In 2013 it took the first steps with a cloud solution to deliver better insight into government effectiveness. The city built a hybrid cloud based on Microsoft products to store and analyze large volumes of structured and unstructured data from its systems and new public sources such as social media, software log files, and GPS data. This generated business intelligence (BI) and data services that could be accessed using any Internet-connected device.

Implementing a central platform will require a bigger initial investment but it can accelerate and simplify the deployment of future Smart City applications, since network connectivity, data management, analytics and dashboard creation functions are already in place and can be shared with new applications, potentially reducing ongoing costs.

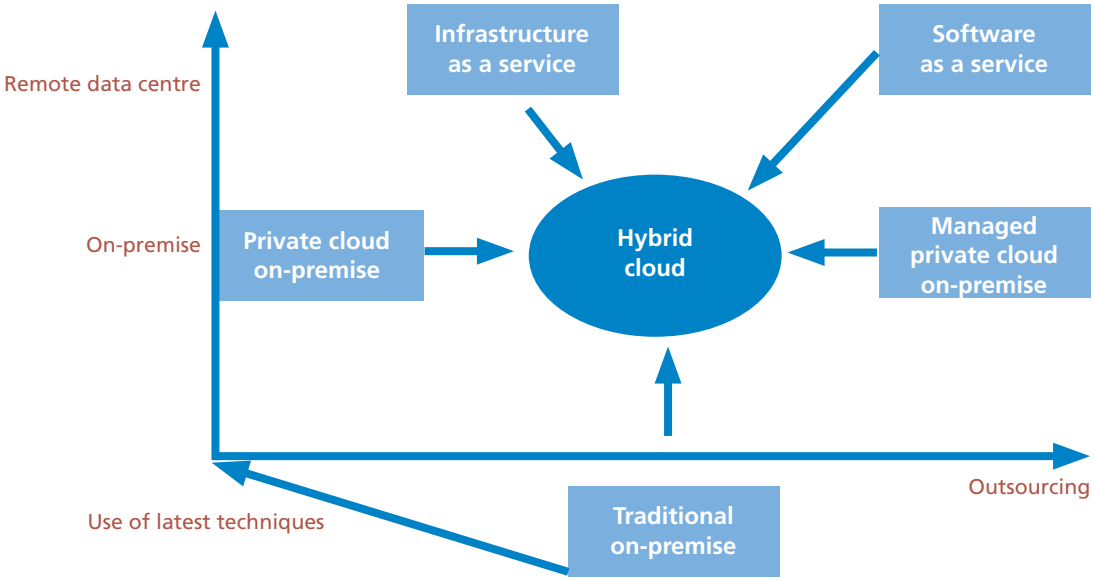
On the other hand, some established applications are supplied with all the data management and control functionality already implemented as Software as a Service by the vendor (see section 4.3) and this will be the fastest route to deployment of an individual application. For example, a number of cities have installed street lighting systems managed by the Philips CityTouch platform or systems from other vendors. In the case of the ports of Tenerife, this has delivered energy savings of up to 80% by using more efficient luminaires, remote control and the cloud-based management system.

Another widely used SaaS service is for Big Belly Solar smart waste bins. These are being deployed in cities around the world to reduce litter and mess in city centers and are linked to a central cloud server that sends alerts to city staff when the bins need emptying and provides access to reports and maintenance information.

3 Different IT approaches for Smart City Services

In order to future-proof Smart City services and to ensure that the city's requirements are met, the IT strategy needs to be evaluated along three dimensions: location (whether on-premise or in a remote data center), outsourcing and ability to use latest IT techniques, as illustrated in Figure 4-1 below.

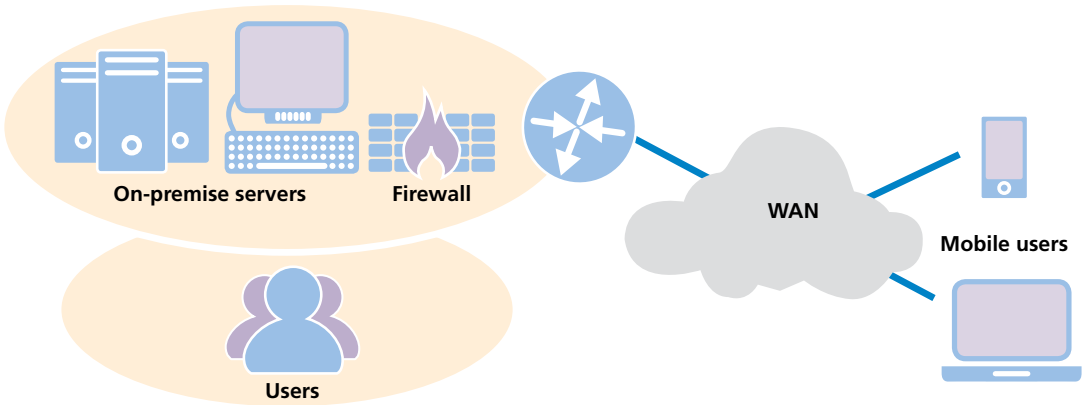
Figure 4-1: Dimensions of city IT strategy [Source: Machina Research, 2016]



On-premise infrastructure

There was a time when most IT systems were installed by the users in their own premises in the architecture illustrated in Figure 4-2 below. The different infrastructure options available are described briefly below.

Figure 4-2: On-premise server infrastructure [Source: Machina Research, 2016]



In this case, the user's IT staff is responsible for installation and providing connectivity, as well as keeping operating systems up-to-date with the latest patches, keeping all of the software, databases, middleware and operating system versions in sync, ensuring there is a robust back-up routine with both on-site and off-site backups, implementing the latest security measures and responding to security alerts. Any upgrade to the system requires project planning, server procurement, software installation, and often downtime while the servers are switched.

Private Cloud On-Premise

In a cloud architecture servers are not dedicated to a particular task but form a pool of resources delivering a service to users in an efficient and scalable way. They typically make use of techniques such as virtualisation – in which a number of separate logical servers, or Virtual Machines, are running on one physical server. This approach greatly increases the flexibility and speed of response of the infrastructure. In private clouds the pool of resources (the cloud) is only accessible by a single organisation, it can be implemented in-house if the organisation has the requisite IT skills.

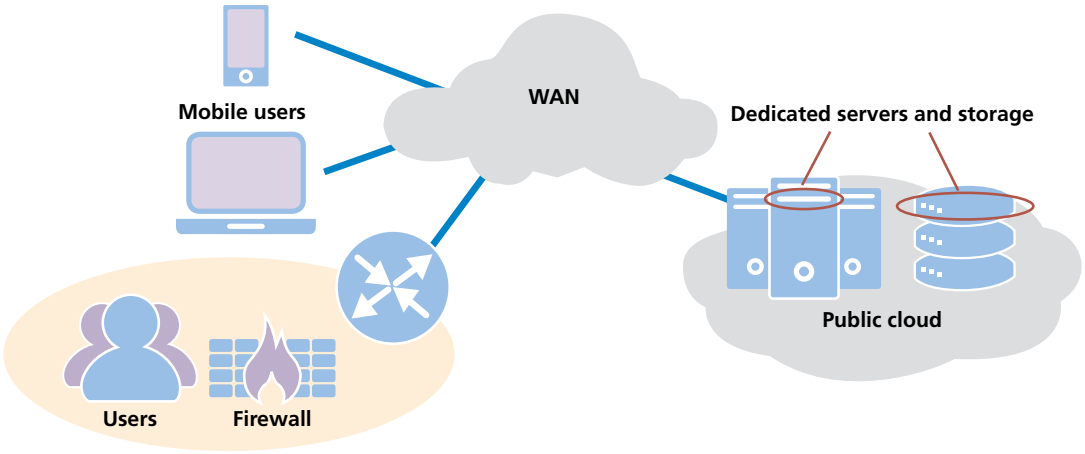
Managed Private Cloud On-Premise

This approach delivers the benefits of cloud without requiring IT staff with the new skills, since the service provider manages the cloud infrastructure on the client's premises.

Infrastructure as a Service

A public cloud solution may make use of dedicated servers to provide Infrastructure as a Service (IaaS) within a cloud data center, in which case the management of the infrastructure has been outsourced but the city's IT staff may still maintain the applications.

Figure 4-3: Infrastructure as a Service [Source: Machina Research, 2016]



The French city of Drancy has installed a CCTV system to reduce crime in which the data is stored on a private cloud platform with the video feeds transported by two dedicated 10 Gbit/s fibre links directly to the datacentre for distribution and storage. The decision to outsource has paid off handsomely for Drancy because the resolution of the video feeds has increased, and new government policy has increased the number of days that data must be stored from 10 days to 30 days. If the council were managing the datacentre itself, it would have meant extra work for the team and increased expenditure on equipment. Now the solution is very scalable, and all the IT department needs to do is to place one phone call to the provider to increase their capacity.

Software as a Service

A public cloud infrastructure may be used to provide applications running on multi-tenant servers as Software as a Service (SaaS). In this case, the whole task of supporting the application has been out-sourced to the cloud service provider and all that the in-house IT staff need to worry about is supporting the Internet connection and the end-user devices. Many cities are adopting this approach for their Smart City services, as it brings the scalability, security and reliability needed. For example, the City of Nice has implemented a smart parking solution that uses Urbiotica sensors linked to their U-Spot cloud platform. This cloud-based approach minimises the energy required by the U-Spots and helps them achieve their 10-year, battery-powered lifespan.

Software as a Service is likely to be the most cost effective means of implementing any single application. This is because the customer pays only for what they use, usually on a monthly basis (see Section 5). All the routine issues in running a data center, securing the building, the networks and the servers, providing connectivity and ensuring the right applications are installed on the right servers become the responsibility of the service provider.

Cloud brings a great many benefits in availability, scalability, flexibility and disaster recovery.

- Computing power can be added quickly when they are needed and released (and no longer paid for) when requirements change
- Software, databases, middleware and operating systems are kept up to date with the latest version
- All features are available to authorised users at all times and they can access the applications from any browser, including mobile devices, at any time of the day or night
- Resources can easily be duplicated as and when required to ensure high availability and can be in different physical locations to increase resilience
- Backups can be stored in multiple service provider sites, reducing the risk of services going off-line if there is a disaster such as a flood

The service provider will give clear SLAs for all of these aspects.

Moving to a cloud infrastructure frees the organisation from the need to foresee their server needs years in advance and ensures that security is in the hands of experts. It also allows it to keep pace with the speed of innovation in the cloud ecosystem, applying the latest techniques in spheres such as analytics, databases etc.

In a full public cloud solution, all of the organisation's IT concerns are the responsibility of the cloud service provider, who will employ highly professional staff who are dealing with the issues of server management and security day in day out, and for whom the quality of their responses and the speed of their upgrades is critical to retaining their certifications and staying in business.

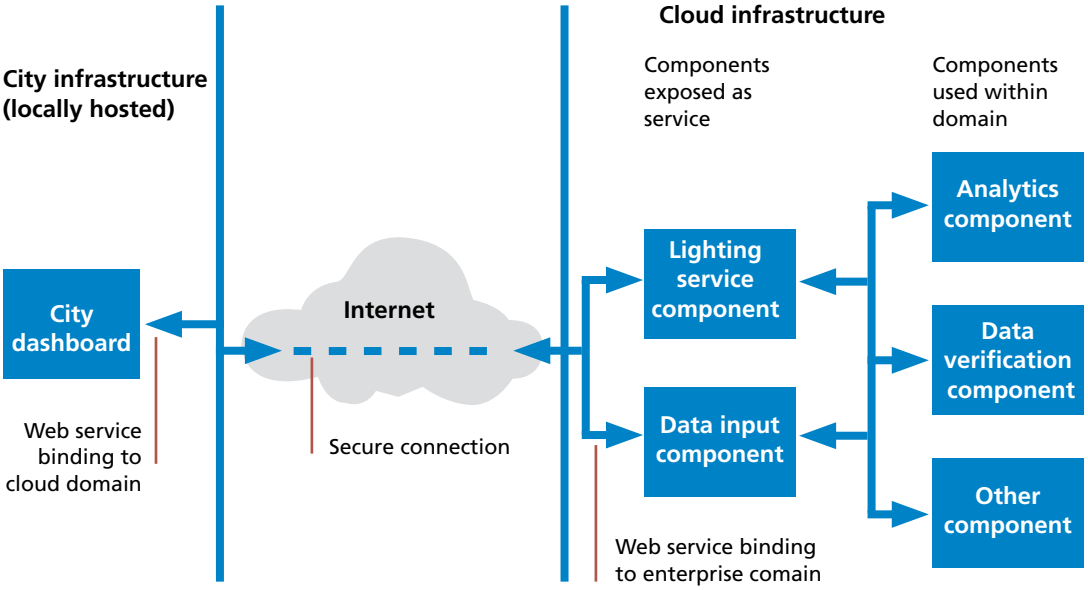
Hybrid Cloud Infrastructure

In reality, existing organisations are unlikely to be able to select one type of infrastructure. To integrate the Smart City Services and obtain the maximum benefits from their deployment, a hybrid cloud will be the most likely solution for most cities. It provides a way of combining the flexibility of cloud with legacy on-premise infrastructure, allowing the city to integrate existing applications while expanding their Smart City infrastructure in a flexible and scalable way.

A survey in the US in 2015 (carried out by vendor RightScale but not limited to their customers) found that 82 percent of enterprises have a hybrid cloud strategy, up from 74 percent in 2014; 88 percent of organizations are using public cloud while 63 percent are using private cloud.

For many cities a horizontal Smart City platform is likely to integrate both legacy services implemented on their premises and applications running in the cloud. Figure 4-5 illustrates how this can work for applications, using lighting as an example:

Figure 4-4: Integrating software as a service into a city dashboard [Source: Machina Research, 2016]



In this architecture the Smart City services are accessed through a dashboard that provides the city's staff with access to a range of different services that may allow them to see data from the many city applications and may also allow them to control these applications, depending on the implementation. In this instance, the street light management is provided as SaaS and linked by Web services to the city dashboard. Access from the city data center is via a secure connection. Only the elements of the lighting service that need to be accessed from the internet are exposed, there are many components that are invisible to the Internet within the cloud datacentre, reducing the risk of hacker attack.

4 Developing an IT Strategy for Smart City Services

As with any major deployment, the first step is to think carefully about what the city is trying to achieve by deploying a smart service.

- What applications need to be supported now?
- What applications might need to be supported in the future?
- What is the projected lifetime of these applications?
- How are they expected to grow over time?
- Might they need to work together in the future?
- Do they need to be integrated with the current city IT systems?
- Will there need to be public access?
- Will there need to be credit card transactions?

It is important that any Smart City infrastructure be sufficiently flexible to accommodate future needs and scalable to cope with hundreds of thousands, if not millions, of connected devices and to manage data from a wide range of sources. Access for the public may be needed, as well as for city staff. The backup and disaster recovery strategy must deliver 24x7x365 availability. It must be capable of exchanging data with existing and future city systems. Costs must b e kept as low as possible as public funds are always stretched to the limit. To achieve all of this is likely to require a strategy that includes at least some elements of cloud infrastructure because flexibility, scalability and disaster recovery are the things that cloud does best.

Cost Effectiveness

On-premise systems require purchase of servers and licences up front whereas cloud solutions can be paid for as required. This is particularly important for Smart City infrastructure which is likely to grow steadily over time as new services and more areas of the city are added to the system.

Using a cloud service provider, the city can pay for the IT that it uses and expand or contract it as required without financial penalty. Capital expenditure (CAPEX) is replaced by operations expenditure (OPEX) – which may or may not be an advantage depending on the accounting rules under which the city operates.

The total cost of ownership (TCO) of a city's on-premise investment includes the cost of licences, hardware, network, backup and development systems, and the cost of replacing these on a regular basis as they become obsolete. It also includes the cost of human capital, such as project management, as well as database, server, firewall, security, backup and help desk resource.

Replacing all of this with a monthly payment to a service provider both makes costs more predictable and reduces the initial outlay required to introduce new Smart City services. It also frees up the IT staff to focus on more strategic IT issues.

Scalability and Availability

Implementing Smart City infrastructure requires a scalable infrastructure. A pilot application with 500 end points might work well from a laptop. But when it has to be scaled to support hundreds of thousands of endpoints, then a properly designed application infrastructure is required. Many city applications are implemented under 25 year contracts, and they need to be supported by IT systems that can continue to adapt throughout that period. Mega cities are growing extremely fast and their requirements for physical infrastructure such as lighting and traffic management are growing along with the population so the IT infrastructure has to be able to match that.

Disaster Recovery and Resilience

Ideally, a critical system will have a hot back-up server running in a different physical location to take over the load immediately if the main server fails, and there should be back-ups stored in two other geographically distant locations in addition to any that are kept on site for easy access. The backup strategy must be tested, which means keeping additional servers running to do this. Cloud providers can often create a 'sandbox' on their systems in which backups can be tested without any disruption to operational systems.

In-house skills required

Managing the IT infrastructure for a Smart City Service is a challenging task requiring highly skilled staff. It is not a good idea to add this to the workload of network support staff whose main task is looking after the end users clamouring for immediate attention. It requires staff with up-to-date skills in server management who are able to make installing the latest updates and implementing the latest security techniques their top priority. In order to make the most efficient use of the city infrastructure, they should also be able to deploy the latest cloud techniques and software. The in-house IT staff have detailed expertise in understanding the city's IT needs and will be better deployed in areas where that understanding is important, rather than routine maintenance.

For example, Newcastle City Council in the UK found that its IT system was becoming overly complex with a massive server farm, reliability issues, third-party software and lots of points of failure. The city's IT manager chose to go to a cloud provider and remove a lot of the day-to-day technical tasks that were consuming a lot of time. The city switched from Windows XP and Office 2003 to cloud-powered alternatives such as Office 365, SharePoint and OneDrive. The transition was fast, within 14 days of starting the project, 500 council workers had been moved onto Office 365 and a new email system supported by Microsoft Exchange Online. Security and identification verification was shifted to multi-factor authentication powered by Microsoft's Azure cloud platform. This freed Newcastle's IT staff to make better use of their time by concentrating on more of the high-end intellectual tasks.

5 Securing a Smart City Service

The first stage of any security implementation has to be a risk assessment. What exactly are the threats that the infrastructure needs to be secured against? The city needs to separate, understand and value the critical assets of each department or business unit so that they can identify the potential threats and the overall risk to the city before applying effective countermeasures. Some applications may require the storage of personal or sensitive data. For other parts of the Smart City Service the concern may not be storage of personal data but the possibility that an intruder might take control of the city's systems.

Data Privacy

There are some Smart City services which will require extra attention to privacy

- Is the service holding personal data? If so it must comply with local laws about storing personal data, including any rules about the location of data centers, such as the EU Directive on data Protection.
- Will it need to handle payments? For example credit card details for parking payments. If so, it will have to comply with the Payment Card Industry's Data Security Standard (PCI DSS).
- Is it used by law enforcement or security services? Then it may have to comply with local regulations, for example the FBI's Criminal Justice Information System (CJIS) rules.

However, there are many Smart City infrastructure management applications, such as public transport, street lighting or road traffic management that do not fall into any of these categories, and for these data privacy is not such an issue.

Authentication

It is widely agreed that usernames and passwords are not sufficient for user authentication for any application that needs to be secure. As defined by the European Central Bank, strong security is any combination of at least two mutually-independent factors of authentication, which must also have one non-reusable element that is not easily reproduced or stolen from the Internet. For systems that control city infrastructure, it is advisable to use at least two-factor authentication but in a way that is user friendly. Factors may be:

- Something the user knows, such as a password or PIN number
- Something the user possesses: typically a hardware device such as a security token or a mobile phone used in conjunction with a software token.
- Something inherent to the user such as a fingerprint.
- User location and current time are sometimes considered the fourth factor and fifth factor for authentication and can be confirmed by smartphone GPS
- Another possible factor is the MAC address of the login point – limiting access to pre-registered devices.

For Smart City applications that are managing things or connecting sensors, reliable machine authentication is crucial to allow secure communication. It is important to realize that each access point is a potential intrusion point. Each networked device needs strong machine authentication and also, despite their normally limited activity, these devices must be configured for limited permissions access as well, to limit what can be done even if they are breached.

Encryption

Encryption is an important tool in securing any infrastructure. Access from end-user devices should be over secure encrypted transmission paths. It is also advisable to encrypt stored data when this will not slow down performance too seriously, for example in backups.

Intrusion Detection

Securing network boundaries is an outdated approach, although it is still important to install the very latest firewalls, an intrusion detection system is also important. An intrusion detection system (IDS) differs from a firewall in that a firewall looks outwardly for intrusions in order to prevent them from happening, An IDS evaluates a suspected intrusion once it has taken place and watches for attacks that originate from within a system. The Smart City Service should be secured with both network and host intrusion detection systems that detect abnormal behavior and either send alerts to the administrator or takes action such as disconnecting a suspect user as appropriate.

Predictive Security

Predictive analytics can be used help protect the Smart City Service from threats, regardless of source. One of the big problems with the alerts generated by the IDS or similar tools is the number of false alarms. Predictive analytics will eliminate the majority of false-positives or non-urgent events and help the IT staff to take action when there are real threats. The use of machine learning to identify assets and the application of threat intelligence to identify attack patterns can be combined to move to a more predictive and ultimately proactive strategy.

6 Six Questions to Answer when Deciding on a Smart City IT Strategy

A well-designed Smart City infrastructure can enhance services and business opportunities, improve safety, and boost collaboration between the city, its citizens, and businesses and continue to do so for decades to come. To achieve this, make sure the following questions have been answered satisfactorily.

1 Is it scalable?
The need for a scalable infrastructure to support a fast growing city and an expanding range of applications makes cloud the obvious choice. SaaS provides the fastest way to introduce a new application, and makes it easy to start small and scale the application as the requirements grow. There is no need to foresee precisely what will be required and no need to buy all the servers and software licenses upfront. The infrastructure can be expanded as the city's needs expand.

2 Is suitable connectivity available?
If the city is in a region where connectivity is slow or unreliable, then on-premise systems have to be the primary implementation, but for most large cities in developed countries this is not an issue. There are some applications which may be better hosted locally, for example CCTV generates large amounts of video that could place a strain on the communications infrastructure.

3 Are the right IT staff available?
Maintaining an in-house infrastructure requires highly skilled staff able to keep up with all the latest developments in the field. It is not surprising that a recent survey in the UK by the Cloud Industry Forum (CIF) shows the overall cloud adoption rate in the UK now stands at 84 percent, with almost four in five (78 percent) of cloud users having adopted two or more cloud services.

4 Is it sufficiently secure?
The key to a secure system is not the location of the servers, but that it is managed following the latest security practices and software is kept up to date. The complexity of modern security systems mean that, for most organisations, using a cloud provider brings an improvement in security. Choosing a best in class provider that has all the relevant certifications and is able to guarantee the security of the cloud is going to be preferable to that of owned IT infrastructure for many Cities. Cloud backups are often the best way of easily storing back-ups in remote locations. The states of Texas and California are both using Microsoft's Office365 service which is delivered from Microsoft's cloud infrastructure, and Microsoft has obtained the stringent FBI CJIS certification to make this possible.

5 Is it accessible?
Many of the benefits of creating a Smart City infrastructure stem from making the applications accessible to a variety of users, whether different city staff or the public, so appropriate user management tools must be in place. A cloud service will be able to spin up servers on demand if there is a sudden demand from the public, for example after an extreme weather event.

6 Can all the elements be integrated successfully?
The need to integrate legacy infrastructure with new services is likely to require a hybrid cloud solution to ensure that the necessary IT infrastructure can evolve and expand. Each element must have the APIs needed to work with all the others.

PHILIPS

This white paper has been commissioned by Philips Lighting.

About Philips Lighting

Philips Lighting, a Royal Philips (NYSE: PHG, AEX: PHIA) company, is the global leader in lighting products, systems and services. Our understanding of how lighting positively affects people coupled with our deep technological know-how enable us to deliver digital lighting innovations that unlock new business value, deliver rich user experiences and help to improve lives. Serving professional and consumer markets, we sell more energy efficient LED lighting than any other company. We lead the industry in connected lighting systems and services, leveraging the Internet of Things to take light beyond illumination and transform homes, buildings and urban spaces. In 2015, we had sales of EUR 7.4 billion and employed 33,000 people worldwide. News from Philips Lighting is located at www.philips.com/newscenter

About Philips CityTouch

Philips CityTouch is an end-to-end street lighting management system that integrates connected devices, intuitive software-as-a-service applications, and specialized services to transform a city's lighting operations. It provides a seamless solution connecting every individual street light directly to the lighting management system. If the luminaires are connected over public mobile networks, it can be a plug & play installation without the need of any commissioning, locating or manual data upload or any local network or additional hardware. However the system is flexible and can make use of a local wireless or powerline network if that is preferred.

Existing third party city systems or dashboards can be connected with CityTouch through APIs, so the system can be integrated with asset management systems now and with Smart City Platforms in the future. Customers can customize existing data fields, add new data categories and adapt user profiles.

The system uses a mature cloud platform with more than 99,9% uptime connecting hundreds of thousands of lighting assets worldwide. It delivers high performance and fast response times, whether managing 10 or 10 million assets. The SaaS implementation is future-proof through continuous innovation adapting important technology trends.

The system is designed for fail-safe operation. In the unlikely event of a total failure of the CityTouch infrastructure or an attack, the lights in the street will continue to function according to pre-loaded schedules.

About Machina Research

Machina Research is the world's leading provider of market intelligence and strategic insight on the rapidly emerging Machine-to-Machine (M2M), Internet of Things and Big Data opportunities. We provide market intelligence and strategic insight to help our clients maximize opportunities from these rapidly emerging markets. If your company is a mobile network operator, device vendor, infrastructure vendor, service provider or potential end user in the M2M, IoT, or Big Data space, we can help. We work in two ways:

- Our **Advisory Service** consists of a set of Research Streams covering all aspects of M2M and IoT. Subscriptions to these multi-client services comprise Reports, Research Notes, Forecasts, Strategy Briefings and Analyst Enquiry.
- Our **Custom Research and Consulting** team is available to meet your specific research requirements. This might include business case analysis, go-to-market strategies, sales support or marketing/white papers.

Machina Research's Advisory Service provides comprehensive support for any organisation interested in the Internet of Things (IoT) or Machine-to-Machine (M2M) market opportunity. The Advisory Service consists of thirteen Research Streams (as illustrated in the graphic below), each focused on a different aspect of IoT or M2M. They each provide a mixture of quantitative and qualitative research targeted at that specific sector and supported by leading industry analysts.

Machina Research's analysts also have a wealth of experience in client-specific consultancy and custom research. Typical work for clients may involve custom market sizing, competitor benchmarking, advice on market entry strategy, sales support, marketing/promotional activity, and white papers.

For more information, refer to our website at https://machinaresearch.com, or email us at enquiries@machinaresearch.com.

Advisory Service Research Streams [Source: Machina Research, 2014]