Smart cities appeal and 15 things that should not go wrong

Sept 12, 2017

Authors

Mohamad Amin Hasbini, *Senior Security Researcher, Kaspersky Lab*

James Mckinlay, *Director, Praetorian Consulting International Limited*

Martin Tom-Petersen, *Client director and partner, Smart City Catalyst*

Aseem Jakhar, *Co-Founder - Payatu, hardwear.io, nullcon, null*

Amgad Magdy, *INVLAB Founder, IS Consultant*

David Jordan, *CISO, Arlington County Government, Virginia, USA*

Contributor

Alan Seow, *Cyber Security Practitioner*

SECURING
SMART
CITIES

INTRODUCTION

Urbanization of populations is a continuous phenomenon, cities are transforming digitally into smarter ones, enabling better governance, enhancing the living of humans and facilitating better resources utilization efficiency. In reality, various systems such as cameras and traffic signals, street lights, sewers sensors, gas and electric meters make up the digital infrastructure of smart cities. Residents will pay their bills and get access to a range of municipal services by connecting to the infrastructure of the smart city. Since smart cities are expected to make up top urban centers, they are expected to contribute to a large percentage of the global GDP. With all the developments taking place, cities around the world could spend as much as $41 trillion on smart tech over the next 20 years.

Smart cities integrate technologies and innovations such as Big Data, mobile technologies, robotics, artificial intelligence and the Internet of Things (IoT) to change how humans interact, work and prosper. This means that tremendous communication will be taking place across smart city systems, leading to huge data transfers and large data storage facilities run by municipalities. As much as the physical and virtual infrastructure interconnectivity in smart cities render them functional, they also add to their vulnerabilities, creating significant cybersecurity risks.

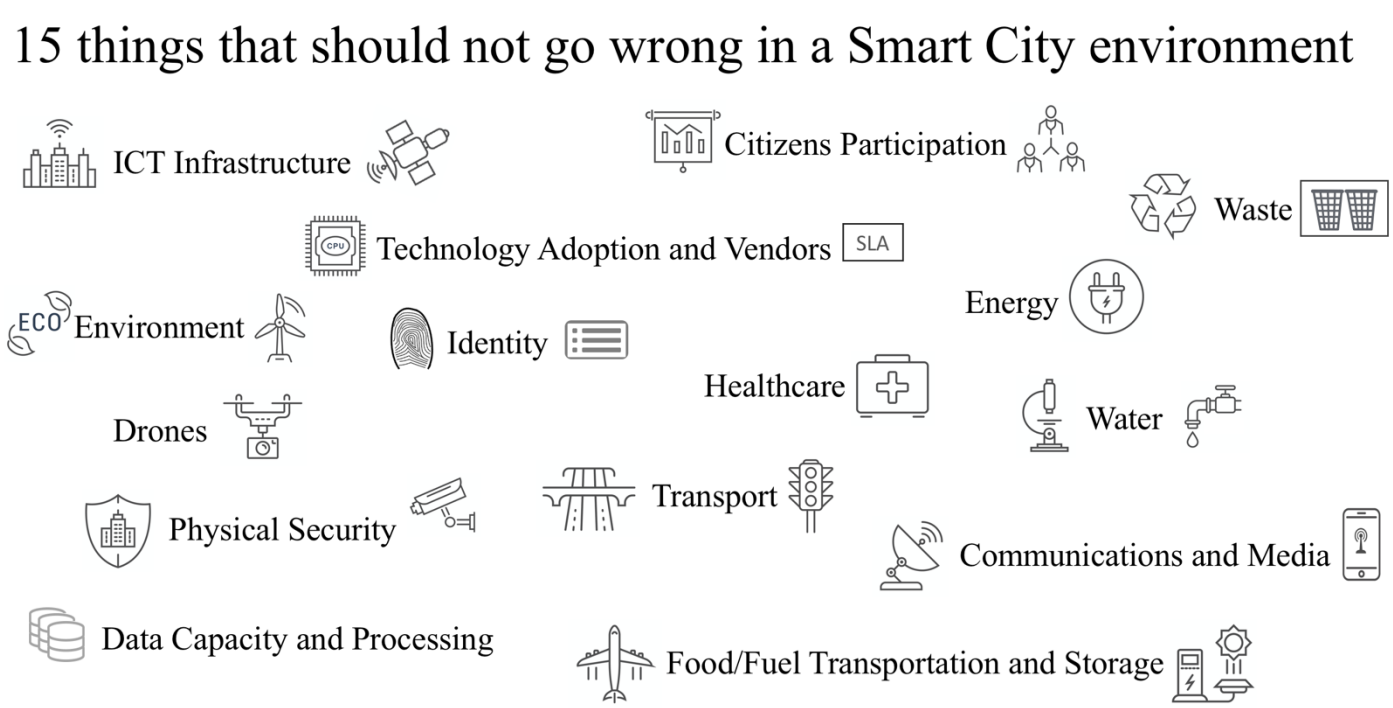
The cities are vulnerable to threats such as signal jamming, remote systems or data manipulation, Denial of Service (DoS), malware attacks and the recent rampant ransomware and wiping attacks. There is a need therefore for comprehensive smart city plans to minimize cybersecurity risks and protect critical infrastructure in smart cities as to defend stakeholders, ranging from residents to private and public service providers or institutions.

Typical IoT devices are also expected to be in constant communication with the devices of residents such as smartphones, wearables and even implants. Smart cities' virtual doors will need virtual keys and locks controlled through remote communications. In real sense, these virtual doors to smart cities are never fully locked, creating loopholes cyber attackers will sure attempt to exploit. This then means smart cities are not safe until proven, hence measures must be put in place, spanning physical security and national security, to continuously ensure, guarantee and verify certain processes and operations never go wrong. This paper discusses some of the critical things that should never go wrong in smart cities.

SECURING SMART CITIES

Things That Should Not Go Wrong in a Smart City Environment

This section details some of the most important functions in a smart city environment, the goal is to point out on a high level, the most pressing risks that necessitate the earliest attention. Each subsection will discuss what could go wrong and possible solutions that may help. Discussions will attempt to focus on the most relevant issues for each smart city function, some other general recommendations could still be valid to address mentioned issues but are not listed to avoid repetition or because they represent common safety practice (e.g. operational security, personnel security, service level agreements, systems hardening, physical security).



1. ICT Infrastructure Management

What could go wrong

There are a number of things that could go wrong in the smart city Information and Communication Technologies (ICT) infrastructure, it being the core and focus of operations, in the following we detail briefly the main cyber related issues, excluding natural disasters:

Data Availability Management - Cyber attackers can compromise ICT systems through denial of service attacks, spoofing, ransom or wiper attacks with an aim of making services or data unavailable. Without access to the critical systems or data, critical smart city operations are disrupted. If services, data or systems are unavailable for hours, days or even weeks, businesses in smart cities risk losing billions of dollars in revenue.

Data Integrity Management - Tampering with data integrity can cause large complications too. Through such, attackers can Influence access control, operations behavior or cause disruptions to city systems. The kind of data under the custody of banks and governments should be exceptionally accurate, hence their manipulation could cause serious economic or national security problems.

Data Privacy Management - Personalized data, this could be for example patient data in healthcare sector or financial details which is privileged and supposed to stay confidential. Citizen data privacy problems would then threaten the individual's trust in the services providers. As a result, businesses, institutions and cities risk losing effectiveness, revenues and growth.

Communications Fabric Availability - Traditional ICT infrastructure concerns are often discussed as the interconnectivity of networks and devices in the TCP/IP domain. The explosive growth in use of mobile broadband means that the future for IoT will include a reliance on 4G/5G provided by the telecommunications suppliers. These “vendors” are also responsible for the reliability and security in the SMS/MMS space that citizens still rely on for multi-factor authentication (MFA) and notifications.

What needs to be done

Advanced encryption protocols and access control systems for Smart Cities, coupled with continuous system monitoring to detect and prevent unauthorized access and suspicious modification to critical ICT infrastructure and data. Failover systems and servers can also be deployed to ensure that Smart City continues to run after active servers have been hacked, nevertheless that needs to follow a smart city cyber crisis management planning to establish incident identification and response parameters. Investing in state of the art solutions that support scalability can also help improve data availability.

Smart cities must therefore develop backup and cyber related disaster recovery planning through crisis management, to prepare for cyber-attacks and the collateral damage (disasters) that might impact the ICT infrastructure, which could cause devastating losses, or completely cripple a city. With an adequate disaster recovery plan, smart cities can recover their compromised systems in minutes or hours after an attack to prevent further disruption to the urban environment.

2. Technology Adoption and Vendor Management

What could go wrong

Smart cities deploy new and proven technologies within the critical infrastructure. Although systems and devices are intensively tested for weather-resistance and functionality, the same isn't as strictly applicable for cyber security. While solutions might match a cybersecurity checklist based compliance tests, they might not support cybersecurity by design or defense-in-depth and will remain effortlessly compromised by attackers. As a result, risks and breaches are transferred to the smart city residents and stakeholders without their consent. Vendors often fail to deliver appropriate quality assurance by exaggerating security abilities; over promising during sales promotions and failing to develop and deliver secure software or required security fixes after their products are deployed.

In other cases, vendors assume that systems will run on protected networks and are therefore safe, hence do not provide self-defending solutions. Devices using Internet of Things (IoT) and industrial systems are typical of such poor practices, enabling incidents on a daily basis and on a global scale.

What needs to be done

When implementing devices and systems, smart cities must ensure security tests are conducted to verify their safety and identified loopholes should be closed. Authentication, encryption, authorization, non-repudiation and software patches must be up-to-date at all times to ensure systems security and stability. Vendors must provide proper documentation on the security of their systems and devices with Service Level Agreements (SLA)-based timely responses for identified weaknesses. Vendors need to ensure seamless patching experience for functional components, patches should not impact live operations or cause infrastructure instability... Governments help by crafting contract language that clearly states the requirements expected of the vendor as well as liability in the event the vendor is found to be in breach of the contract. In some cases, vendor may be required to accept liability for serious mis-steps/failures to follow based on best practices with regard to cyber security, i.e. in the Equifax case...

All SLAs must incorporate on-time vulnerability patches, response to cyber-attacks and incidents within minimal time, 24/7/365. There is also a need for immediate response teams and curbing of cyber threats as soon as an attack is found, all part of a cyber crisis management strategy. Vendor monopolies and corruption must be prevented, quality enforcements upheld and justified, and selections verified to ensure that everything is in order and all systems implemented are healthy. All these must be verified with a certification process by an organizational body and reflected in the SLAs.

Smart cities should especially avoid running facilities on legacy systems that are vulnerable to attacks, incompatible with new technologies or which require third party technologies to bridge the age gap. Numerous semi-or-critical infrastructure facilities such as airports, banks, power stations and railways, have been identified to be running deprecated Windows XP and NT4, years after their announced end of life and support expiry.

For more information on technology adoption challenges and vendor related security concerns in smart city environments, please check our previously published research on the "Cyber Security Guidelines for Smart City Technology Adoption": https://securingsmartcities.org/wp-content/uploads/2016/03/Guidlines_for_Safe_Smart_Cities-1.pdf

3. Communications and Media Management

What could go wrong

The various forms of digital communication technologies and media (Online media, TV, newspapers, magazines...) help spread and disseminate information, which has different levels of criticality. Recent years have demonstrated different important aspects of communication, namely the importance of its availability (ability to deliver news when needed), integrity (ability to deliver correct and accurate information) and confidentiality (ability to communicate secret information safely). Non-availability of information to the city components or citizens obstructs their ability to be aware of events, also blocks their ability to deal with incidents and emergencies, examples could be severe weather or fire outbreaks, or city's ability to respond to cyber-attacks. Lack of information integrity on the other hand alters the right information from being collected or delivered, and obstructs the right decisions from being made, examples include cases such as emergencies, politics, technology adoption, pollution/environment, voting… Lack of confidence in the ability to share information privately also impacts the ability to communicate efficiently with the citizens or at the national level. While other concerns listed in this document could result in effects that impact the city infrastructure/performance, communications mismanagement directly influences the smart city governance, one of smart city's most important dimensions.

TV Station Hacked - http://www.bbc.co.uk/news/technology-37590375

What needs to be done

The protection of communications and media needs to be performed at many different layers, while a lot of measures could be established inside media organizations or through integrity regulations, smart cities need to guarantee a satisfying dissemination of information to citizens, which could require alternate communication and secure infrastructure in case of natural disasters or large attacks on the main ICT infrastructure; such could be orchestrated using municipal drones, which could be deployed upon need to share and spread communication signals, provide video reconnaissance, etc...

For more information on Smart city drones' safety, please refer to:
http://securingsmartcities.org/wp-content/uploads/2017/02/municipal_drones_FINAL.pdf

4. Energy Infrastructure Management

What could go wrong

The current generations of power operations and management, transmission and distribution are mostly controlled and monitored through SCADA (supervisory control and data acquisition) and other industrial systems. The electricity grid then consists of various networked devices using

different technologies (e.g. Power-line communication technologies, free-band wireless RS-232 links…), Installation of smart sensors, meters and grids also increase access points to the grid network. Hackers can use low-cost tools and software to launch attacks on the grid network, causing power generation instability, decreased efficiency, damage, shorter lifespan of high energy components of the power grid, prolonged blackouts, stealing of energy from users or tampering with users' proof of consumption. In addition to manipulating smart meters, hackers can exploit smart grid encryption issues. Attacks on the grid network can cost smart cities billions of dollars, or even loss of human life. Cyber-attacks in smart city environments are a life safety issue.

Crash Override - https://www.wired.com/story/crash-override-malware/

What needs to be done

Several measures can be put in place to prevent attacks on smart cities' energy management systems or detect intrusions before attacks are launched. Smart cities should strictly control change commands and change requests to energy facilities, systems, sensors, meters... and use the services of specialized monitoring systems or teams to monitor the behavior of critical services systems. Authentication, encryption and authorization technologies used on energy systems and equipment should be reviewed to ensure they meet highest protection standards and are up-to-date. System vulnerability checks and penetration tests should be periodically scheduled, ensuring that identified loopholes are closed and helping identify any ongoing attacks. Vendors in the USA and around the world are in developing technologies right now worldwide to monitor and deflect cyber-attacks on operational technologies.

Energy monitoring sensors are expected to be in place to report utilization behavior, deviations and efficiency; such would enable a definition of baselines and then the alerting on deviations from the baseline. Access to energy sensors and data should be restricted and monitored, having a cyber crisis management plan in place to prepare for worst case scenarios can help smart cities control and remediate cyber incidents directed towards critical energy systems.

5. Water Management

What could go wrong

Water facilities utilize industrial automation and control technologies to maximize resources utilization efficiency, monitor operations, and track trends. In modern water management systems in smart cities, every pressure point has a monitoring or remote-control sensor. Smart water metering systems are prone to different types of attacks, spoofing, jamming, interception, ransom or others which could be used to impair sensors functions. An attack launched on water treatment facilities could cause changes in water distribution and delivery, or even in the water chemical properties leading to malfunction, non-availability or non-usability of distributed freshwater... which in turn could lead to chaos in the population, especially if combined with other incidents.

What needs to be done

Water systems and facilities must be closely monitored, possibly using security drones. Access control and permissions must be strictly commanded using specialized teams. At a minimum,

advanced communication encryption protocols must be adopted to secure sensors used to control water management systems (possibly an out-of-band sensor networks). Continuous monitoring and tracking of water management systems and service properties/quality in the city can aide in the detection of dangerous events (e.g. water chemical properties changes), and deliver early alerts on any emerging issues. This can be done using a parallel network of sensors, monitoring effectiveness and quality of the distribution networks. Afterwards it's how the city responds to alerts and incidents that determines a speedy response and limits the extent of damage. Remote areas must maintain physical security on remote facilities, which are harder to supervise and where monitoring is done using fragile landlines or GSM connections which are easy to jam/manipulate, drone based monitoring missions could be helpful in such cases for physical security while advanced autonomous security systems protect the critical services systems.

6. Waste Management

What could go wrong

Smart waste management systems use connected sensors to track and control waste containers. They detect smell intensity or the presence of certain chemicals, garbage volume and signals for collection when the waste containers become ready. During garbage collection, cyber attackers can target the sensors as they relay the data required by the smart garbage collection systems to take action. Interrupting these systems and relaying fake data can have detrimental consequences on the waste management operations.

Fake data can also lead to wrong actions being taken on smart waste systems and if considering collection is performed by automated systems and robotic instruments, waste of energy resources and time, could occur long before being detected or reported by citizens, when issues become apparent. Interfering with waste management on a city scale, can affect public health in smart cities (environment and odor pollution, soil and water contamination, bugs, pesticides...).

What needs to be done

Security protocols and policies should be adopted to secure the smart city waste management systems, in addition to continuous monitoring for unusual logs, systems should also be tracked for efficiency and unusual behavior (e.g. waste unusual overload/collection is late, underload/collection is early). Manual overrides and fail-safe systems should be deployed on the waste management program to ensure operations continue if primary systems have been attacked. Regular penetration tests can also help to detect any weaknesses that could be abused by attackers.

For more information on waste management: https://www.fmmagazine.com.au/sectors/intelligent-waste-management-solutions-an-european-example/

7. Transport Management

What could go wrong

Smart cities use real-time data to inform citizens and residents on train, bus and subway schedules, delays and arrivals. Smart transport systems are also expected to guide smart autonomous vehicles

(anything from pizza delivery on the sidewalks or urban areas to cross-country tandem freight haulers and everything in-between). Smart city surveillance networks provide real time data, traffic congestion and other metrics from within the heart of the smart city. Real-time patterns on traffic, such as prevailing traffic condition and volume, are used to control traffic light and signals and best predict needed changes. Parking applications are also used by smart city residents to find parking slots available...

Attackers can attempt various attack vectors to cause damage to transportation systems, gaining unauthorized access, manipulating information, negatively influencing the behavior of commuters, causing overcrowding, delays, collisions on roads and highways, which could lead to injuries and damage in property or death... Attackers might also target the payment systems which can lead to financial losses (free passes) or crippling the affected systems (no passes).

Hacked SF Metro - https://www.theguardian.com/technology/2016/nov/28/passengers-free-ride-san-francisco-muni-ransomeware

What needs to be done

There are different measures to defend transportation systems: Security protocols and policies should be enforced to secure the processes by which the smart city systems and devices are selected, procured, managed, updated and accessed. Protection measures should be able to collectively defend the different city transportation control components (Roads/highways, bridges, freight, transit, rail, aviation, maritime...). Real-time network monitoring along with frequent regular penetration tests can help find weaknesses or intrusions, for which results also feed into enhanced software development and safer application designs.

8. Identity Management

What could go wrong

Smart cities identity management is also one of the pressing issues. Connected access control systems provide numerous benefits to the city, including but not limited to enhanced efficiency, speed, cost and even management of emergency situations. Nevertheless, access control systems are also attackers' entry point into smart cities infrastructure, systems and data. Eavesdropping and RFID cloning should be the least expected, as attackers attempt unauthorized access. Security equipment such as card readers and wireless devices are irresistible backdoors to cyber attackers mainly because currently they are easy targets with little or no product integrity. With unauthorized access to critical smart city systems, attackers can manipulate, delete or tamper with data, causing confusion and mayhem. Depending on the affected system, any of the smart city components could then go wrong.

What needs to be done

Robust security for sensitive data authorization between cards and card readers can safeguard card systems from unauthorized access as they only accept communication from approved readers. Valid ID or another authentication mechanism (e.g. biometrics or MFA) can also be used with cards, readers and tags for optimal security. If any wrongdoing is detected, card readers should be able to

report logs of suspicious activities to access controllers. Strong authentication and authorization protocols/techniques should be used not just to prevent unauthorized commands from being triggered, but also make it difficult for attackers to gain access to smart city systems and networks.

As different infrastructure technologies in the smart city network use different access control standards and protocols, some might be weaker than others. Unified access control security and identity management policies should be adopted by smart cities to close the gap between logical and physical security applications.

9. Environment Management

What could go wrong

The focus on environment management in smart cities is ecological and public safety. During cyber related incidents or emergency situations, emergency services are able to intervene quickly by deploying speedy and life-saving capabilities, such services should maintain high levels of integrity. When cyber attackers compromise environment management systems of smart cities, the city risks lack of information on developing fires, pollution, abrupt harsh weather conditions or others... For instance, an attack on the rain/weather monitoring systems can cause a false alarm or panic in an entire smart city. Cyber attackers can manipulate the sensors and send fake data to indicate an upcoming storm or tsunami in a coastal smart city, causing mass evacuations when there is no cause for alarm. Another example, is when attackers manipulate street lighting or other types of power consuming systems, causing malfunction and inefficiency, lower life, increased environmental impact, gas emissions… Smart cities might also fail to detect and predict natural disasters such as seismic earthquakes or floods, threatening the lives of city residents. Other cases of environment management could also be the case of cybersecurity threats, like the monitoring of lighting efficiency, machinery aging effects…

What needs to be done

Surveillance systems deployed by smart cities to monitor environmental threats should be highly available and reporting redundant findings that correlate. This also ensures that emergency services have real-time access to information sent from the operational control centers (instructions and directions). Communication between different smart city operators and heterogeneous systems within the local networks and the internet should be encrypted to secure the information being transferred. Trusted personnel and authorized users can access systems and critical data through strong multi-factor authentication protocols or digital certificates.

Thermography is a technology that involves the use of infrared imaging and measurement devices to measure thermal energy emitted by an object. Infrared thermography cameras produce images of invisible infrared or heat radiation and provide precise heat measurement capabilities without contact with the object. Such a technology could be useful in the smart cities to identify inefficient, aging, misbehaving or rogue devices (e.g. identified based on a change in the device heat signature...). Scans could be done by drones and mapped to a database where analytics could identify events and correlate thermal behavior on the city scale.

For more information on Infrared Thermography, please refer to:

http://www.maintworld.com/Applications/IR-Thermography-in-Maintenance

10. Drones Management

What could go wrong

Smart city drones offer support for daily use cases such as in transport, medical and agriculture. They also support emergency management such as fighting forest fires, coastal monitoring, infrastructure inspection and protection, augmentation of the police. Telecommunication surge capacity handling and disaster recovery services can leverage drones. Drones should be securely implemented, operated safely and available when needed for a mission.

The presence of citywide drone systems opens up multiple entry and integration points which attackers can target. Attackers can remotely target drones attempting to steal collected data or images which could negatively reflect on citizens privacy or other matters if utilized in further attacks. Drones can be physically targeted during maintenance, operation or storage, for the goals of electronic tampering, enabling a negative impact on the integrity of data collected, adopted routes or even added equipment/sensors. Drones can cause collisions, accidents, injuries…

Drones can be used both offensively and defensively, the same can be said of drone defenses

Example, Zigbee light bulb attack by drone - https://www.youtube.com/watch?v=Ed1OjAuRARU

What needs to be done

Smart city drones should be secured by deploying proper controls and infrastructure. The controls should be consistently evaluated for accuracy and proper functionality. Operators must comply with regulations and rules governing drone operations like compliance mandates.

The drones should be continuously monitored for weaknesses in design, maintenance or even when charging. Penetration tests should also be conducted regularly to ensure smart city drones are safe from intrusions. Specialized radars can be used to identify unknown rogue drones, misbehavior or jamming signals.

For more on Smart city drones' protection, please refer to: http://securingsmartcities.org/wp-content/uploads/2017/02/municipal_drones_FINAL.pdf

11. Physical Security Management

What could go wrong

Access control and monitoring systems are critical aspects of a smart city's physical security systems. Main gate access control, surveillance cameras, smart fences, access control panels, IP and PoE door locks, fiber optic cables, fire detectors and other security management systems are typical of smart city physical security remote controlled systems. Forest monitoring, borders/coastal monitoring and monitoring of fire and smoke are also part of smart city physical security systems.

Physical security devices are physically accessible and vulnerable to attacks when installed outdoors near perimeters. Cities might also have their physical security and cyber security managed independently, making it difficult to oversee the city's general security or correlate events. Cyber attackers will attempt to authorize rogue access, neutralize alerts, intercept digital recordings, creating false alarms...

What needs to be done

Physical security systems, unlike IT networks, are static. This means the network architecture is stable and changes shall rarely occur; information flow is routine and devices have limited connection to outside networks (in current standards). The known protocols used are also limited, making available solutions not just viable but also affordable. Centralized monitoring systems should be deployed to gather and assign appropriate actions to cases, a brief network disconnection of certain systems (wired or wireless) could mean interception and might necessitate a quick inspection through nearby cameras or via drone mission.

12. Healthcare Management

What could go wrong

Healthcare automation, connectivity and smartness brings in a lot of innovation and new methods to influence the living's health factor and life span, from taking intelligent decisions about the patient's symptoms, conditions and medications, to remote physical interfacing and assistance in critical operations. On the other hand, healthcare facilities have been lagging behind in issues of cyber-security and patients' data protection. There are two main areas of smart Healthcare systems which are of grave concern: Virtual (patient information system/data) and Physical (patient actual health). The complexity of healthcare systems renders patient health information and their records confidentiality, integrity and availability a challenging task. According to a study by Independent Security Evaluators (ISE), while hackers have used ransomware to compromise patient health records, the study state that remote intruders can also compromise patient systems through malicious software infections affecting active medical devices (e.g. Medical Scanners, infusion pumps, pacemakers...), they could also have the ability to cause denial of service for critical medical systems or delete/modify patients' data, implications could be lethal…

For more information: "Securing Hospitals: A research study and blueprint." Independent Security Evaluators, https://securityevaluators.com/hospitalhack/

What needs to be done

The smart devices/equipment deployed in the facility also need to comply with strict healthcare standards (HIPAA, ISO 27799:2016...) and be well protected against attacks. Network/systems segregation enables equipment to operate in separate networks with sufficient protection such as Firewalls and intrusion detection/prevention systems, direct access from other networks should be restricted/blocked. Radio communication steps should be taken to ensure that the devices implement sufficient protection against common attacks using the security provided by the radio protocols and vendors. Some of the requirements for healthcare connected systems include but are

not limited to: authentication, encryption, access control, protection against replay attacks, jamming, physical tampering protection.

13. Citizens Participation Management

What could go wrong

Smart cities engage their populations through electronic participation where civic duties such as voting and public decision-making take place over the internet. Smart cities allow citizens to take part in democratic processes and encourage them to take part in critical decision-making such as finding solutions to city challenges, enabling a shared responsibility, accountability and then-forth shared outcome and satisfaction. E-voting in smart cities should be planned to engage citizens in a convenient and fast process, ensuring that as many citizens as possible are able to be involved. When attackers gain access to these systems, they can cause disruption, ransom, manipulation of integrity and authenticity… preventing appropriate decision making. As a result, decision-making processes could fail, ending up with wrongful or negative decisions. Another concern is that even a minor sized issue can impact and undermine the integrity of the elections, systems must be guaranteed secure before e-voting is allowed.

What needs to be done

There have been intense debates in the last few years on the use of E-voting systems. Smart cities must assure their e-participation systems are safe and accurate at all times, such is a necessity to protect the city's own existence. Strongest encryption, authorization, authentication, authenticity protocols and verification measures should be expected on each side of such services, protecting e-voting integrity, processes and collection/counting mechanisms/systems.

14. Data Capacity and Processing Management

What could go wrong

Smart cities are highly driven by IoT, big data, as well as data analytics, there is a continuous need for storage and processing abilities to make use of collected data. Smart cities needs of data storage must be well defined and controlled, in order to achieve a healthy standing for data storage and processing abilities. Underestimation of requirements can lead to non-storable or non-processable data (non-usable services, data loss...), overestimation can lead to waste of financial resources.

What needs to be done

Projection and capacity analysis tools are therefore essential to build and define city needs in terms of processing and storage. Different techniques should be implemented to accurately analyze city storage requirements, historical progress and historical timeframe for which data will be kept and analyzed, such would help dictate the amount of storage needed, the processing efforts required and therefore help define the city needs in data lakes and processing power. Securing the forecasting controls and processes is also important to maintain accurate measures and recommendations.

15. Food/Fuel Transportation and Storage management

What could go wrong

Food and Fuel transportation are closely linked and should be carefully monitored and protected by any local or national CNI initiatives. If there is even the hint of a fuel crisis or blockade, it will usually trigger “panic” buying at the grocery stores. Towns, cities, countries that rely on imported food and/or fuel must consider and have plans in place to mitigate these risks. Petrol, Diesel, LPG, Dairy, Meat, Poultry, Soft Fruit all require special treatment and cannot sit in uncontrolled environments. IOT sensors used in these environments that have been attacked, manipulated or compromised could lead to, in the case of fuel transport, dangerous situations and in the case of food transport the knock-on effect of panic buying and food shortage or widespread food poisoning.

IOT for groceries - http://www.verisae.com/verisae-blog/benefits-of-big-data-and-iot-for-grocery-retailers

What needs to be done

As food and fuel storage and transport networks look to find improvements and efficiencies through greater adoption of IOT, all the security, availability and integrity concerns found in any move to IOT platforms must be addressed. Food facilities can soon be considered part of cities’ critical infrastructures and therefore should follow its policies and priorities by being controlled, maintained and defended similarly.

CONCLUSION

With the number of smart cities worldwide expected to grow, the market is worth more than $1.56 trillion by 2020 (Frost & Sullivan). The cities focus on offering better waste management, transportation, energy management and increased mobility to improve the lives of citizens. However, smart cities encounter various challenges such as cyber threats that impede optimal realization of benefits. There are continuous needs for the highest guarantees of data privacy, confidentiality, integrity and availability even while cities evolve and develop at a fast rate. The complexity of a smart city fast changing infrastructure and the fact that various vendors will be responsible for continuously implementing different services and systems makes the whole process highly challenging to control and maintain, requiring utmost seriousness and agility.

Smart cities are expected to enforce state-of-the-art security and policies to secure their data and networks, assuring businesses and residents of the city that they are safe and continuously happy. Nevertheless, that is expected to pose huge challenges to develop and maintain, especially in industrial facilities and systems. The smart city governments are expected to partner with the private sector to foster operations that meet city needs and requirements. In addition to the smart city security measures discussed in this report, a sound cyber crisis management plan must also be developed for efficient response to disasters and crises as they occur, minimizing further losses and damages.