Smart Cities Cyber Crisis Management

Sept 18, 2017

Authors

Mohamad Amin Hasbini, Senior Security Researcher, Kaspersky Lab

Raddad Ayoub, Advisory Partner, EY

Martin Tom-Petersen, CEO, Smart City Catalyst

Loïc Falletta, Owner and Principal Security Consultant at Yinkozi, Ltd

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

Alan Seow, Cybersecurity Practitioner

Sandeep Singh, Security Consultant

SECURING
SMART
CITIES

TOC

SECURING SMART CITIES

Introduction

Cybersecurity of Smart Cities is a controversial topic today. Researchers and professionals are debating the viability and sustainability of a large complex environment, which heavily relies on the digital infrastructure, especially from a cybersecurity perspective (1). Smart cities continuously deploy and update information and communication technology (ICT) to enhance the quality of life for citizens. The cities are typically evolved 'connected cities' that deploy large-scale data exchange across extensive domains. An integral part of the smart cities is their intelligent systems; systems offering highly sophisticated tools and functions, enabling advanced services at high efficiency. The smart water meter technology deployed in Barcelona saves about $58 million each year (1). Smart sensors are being used in a smart city in South Korea to control electricity and water usage, cutting operational costs by about 30%. According to a hypothetical study from 2015 (2), 93 million people can be affected in case of a power blackout caused by sophisticated cyber-attacks on 15 US states, it can also result in economic losses of up to one Trillion $. Although not all cyber breaches a smart city can experience are devastating or involve systems compromise and disclosure of sensitive information, it might just be a matter of time before worst-case scenarios escalate and take place. The threat of cyber-attacks is inevitable, especially if a city is not well-prepared.

(1) https://hbr.org/2017/04/smart-cities-are-going-to-be-a-security-nightmare
(2) https://www.lloyds.com/~/media/files/news-and-insight/risk-insight/2015/business-blackout/business-blackout20150708.pdf

Unlike current cities with independent operators and multiple stand-alone systems, smart cities will be themed by more centralized systems (virtually centralized not physically, e.g. in the cloud), automated tasks, integration of information, and correlation (Data Analytics). There are therefore considerable larger consequences of inadequately protected data, infrastructure and applications as they are used to process, transmit and store critical information. Cybersecurity involves the measures put in place to detect, safeguard and respond to cyber threats that can affect the operations of organizations, hence smart cities at large. Furthermore, while solutions manufacturers and vendors touch on cybersecurity when defining smart cities, most definitions don't prioritize it despite its essence in offering a sustainable city environment. In a previously published document (1) we identified the top smart city assets and processes that should be protected and guaranteed to the citizens, when it comes to life safety issues, mistakes should not be allowed.

(1) https://securingsmartcities.org/wp-content/uploads/2017/09/SSC-15-things-v1.3.pdf

The intensifying automation in smart cities can be attributed to many assets and services being influenced by data exchange. With critical services increasingly becoming interconnected, there is a need to protect infrastructure and services availability, citizens' privacy, data transfers, safety, and health by prioritizing cybersecurity in smart cities. However, a lack of maturity around policies and regulations in place to govern how

information and information assets (the basis of a smart city) should be handled and operated. This indicates that smart city stakeholders such as citizens, policymakers, solution providers, municipalities, manufacturers, technology vendors, among others, are forced to adapt to the smart city requirements with varying specifications and capabilities.

Few ICT (Information and Communication Technology) infrastructure operators have in place / and efficiently apply policies to protect critical assets that can meet the needs of the smart city and face threats on the numerous connected systems. Furthermore, smart cities may have a limited budget that will be preferably invested in new functions and capabilities rather than cybersecurity of the current infrastructure. Nevertheless, ICT operators deploy a wide range of cybersecurity controls that vary from one to another due to different protocols in use, architectural needs, compatibility, good practices, standards or policies for governance, though things then move towards the unknown when facing advanced cyber-attacks that cause complications to the availability, confidentiality or integrity of the municipal network and services.

Assuming cyber crises are one-time events caused by technical problems and require single solutions can be the beginning of peril for smart cities. Cyber crises call for high preparedness with sound cyber crisis management that encompasses a response life cycle starting from monitoring to reaction to response, resolution, and recovery. A smart city cyber crisis management plan stipulates the actions and processes to be carried out in the event of an attack to safeguard the smart city and its services. On the other hand, a cyber crisis response plan involves measures put in place to offer protection from routine activities such as distributed denial-of-service attacks and malware infections on a daily basis. It is important to note that not all cyber incidents in the smart city would be considered cyber crises, the smart city needs to accurately and legally define the circumstances by which a cyber crisis is detected and then how the related response process is activated and followed.

By definition, a cybersecurity crisis can be described as a breach, compromise or disruption of an organization's critical data and/or systems. It is also important how both the organization and the law define a cyber crisis and classify critical data and systems. The goal is to state for example, what types of data do you have access to and what are the critical systems, by which if either was breached, compromised or disrupted, would present a crisis or potential crisis to the organization, its clients, or the urban environment…

Motive of this paper:

The motive of this paper is to give smart cities a guideline or foundation from which a viable cyber crisis management policy can be developed. Numerous cities already have established crisis management and handling centers, the problem is that challenges are no longer limited to natural or operational causes. Even though smart cities will differ based on various aspects such as maturity levels, priorities, geographical size and demographical characteristics. Ideological, geopolitical or even financial motives could be behind new types of cyber threats to the cities stability and are expected to often target city-wide applications, data, and

technology. Without a converged strategy and transformed operations and handling of crises, cities will not be able to face modern types of threats and consequences could be severe. This paper focuses on the definition of smart city cyber crisis and the need for significant cyber crisis management planning in smart cities. The paper then covers smart city cyber crisis management measures that are needed before, during, after a disastrous attack.

Smart cities cyber threats and challenges

Smart city stakeholders are any personnel, organization or entity which have an interest or benefit from the development of the smart city environment. Smart city stakeholders are expected to be highly dependent on data exchange operations as various elements of smart cities are expected to be run on the ICT infrastructure; data is expected to be constantly flowing between data centers and smart city components. Data flows could occur across smart cities, borders and even industry sectors. These interactions are expected to happen on numerous levels, including but not limited to: ICT operators, citizens, banks, government institutions, transport organizations, power and industrial facilities, municipalities, regulatory agencies… Directed at applications, data at rest and technology, as well as city's structure and infrastructure, there are various types of threats a smart city is susceptible to. To be secure, smart cities must re-assess their security priorities and deploy specialized capabilities, while engaging management bodies and stakeholders, adopting new skills and know how to counter risks and emerging threats.

The digital age has come with pros and cons, smart cities being among the first beneficiaries. Rapid technological changes are driving supply chain integrations, faster research, faster design processes and advanced customer connections to mobility and emerging data analysis techniques, smart cities are will certainly benefit significantly from these advances in technology and accelerate innovation. Furthermore, businesses operating in smart cities will be more interconnected than they ever did, which heightens the impact of cyber threats and attacks on the city’s financial security, operational stability, intellectual property, reputation, competitive advantage, civil peace and compliance to regulations. Smart cities should be able to strike the balance between managing the evolving cybersecurity threat landscape and gaining the most from digital advantage while keeping an eye on its inherent risk if they are willing to invest in optimal cybersecurity.

Data breaches are reported on a daily basis and the types of threats being witnessed today were unimaginable a decade ago, especially when we think critical infrastructure. Sensitive information isn’t just being stolen from the government and public agencies, but also the private sector, a single cyber crisis can impact the citizens safety and cost smart cities a reputation they require to succeed and attract intelligent human capital while also affecting the trust in their innovative systems. In addition, failures to provision optimal cybersecurity will lead to breaches which create unplanned response expenses requiring the loss of funding leading budget cuts to other important programs affecting citizens. Despite the fact that only a few attacks usually succeed when compared to the total number of attacks, the real risk of

cyber crises calls for smart cities to have a response mechanism in place to mitigate a successful attack; just one large scale attack is all that is required to cause chaos; admitting the threat exists is a first step towards preparing for it. Governments prepare for Public Safety emergencies by provisioning Emergency Management departments. Typically, those departments assist police, fire, and environmental services agencies in their response to an incident. Cyber-attacks are going to cause collateral damages which these agencies will respond to while the Information Security Officer and Security Operations Center (SOC) mitigate the actual cyber incident. The more a city is inter-connected, the greater its vulnerability.

Smart cities increase their chances of success when they foster stakeholder trust in their strategies. Stakeholders and operators in smart cities should trust that they can access processes and systems on demand; that their privacy and identity are protected and their data and transactions are safe. With cybersecurity controls in place, smart cities can guarantee stakeholders the safety of their information. Despite the evolution of smart city cybersecurity technologies, the existing security models in use are outdated. Traditional cybersecurity models in smart cities are compliance-based, focused on protecting the back office, perimeter-oriented, and technology-based, hence might not be able to effectively offer protection from emerging threats. The current Cybersecurity defense models are based on securing a defined perimeter, a smart city by nature creates a borderless environment, connecting new technologies every day, adding more inter-connections and thus more opportunities for unauthorized intrusions!

Data is the fuel of Smart Cities, the more they collect, analyze and dispatch the more efficient they will become. Smart cities will store and process large amounts of data they receive/send from/to various sources/destinations. With such amounts of information residing locally or at third parties, there is need to ensure the cloud environments are governed by specific standards to ensure the safety and availability of information. An integration of on-premise infrastructure with cloud services blurs various system components, hampering system maintenance efforts. For instance, traffic lights rely on traffic data to operate efficiently and direct traffic along a highway. If the data is compromised, drivers would be misguided, leading to unknown hidden hazards or serious highway accidents. If signal times are set to long wait times massive traffic congestion will occur causing frustration and greater potential for road-rage incidents. The citizenry will quickly lose trust in its government's effectiveness to manage advanced technologies if incidents start occurring regularly.

Cyber terrorists are inventing sophisticated techniques to launch attacks on their targets, sometimes even using insiders. Attackers can gain unauthorized access to smart city systems to steal information or manipulate operations. These activities can result in significant losses in terms of finances, lives, time and even ruin the trust that the cities have worked hard to earn in the eyes of the public. Cyber criminals cannot be ignored. With advanced technologies that do not have inherent product integrity, significant efforts must be made to

defend and monitor the health of these Smart City systems. Without proper cybersecurity planning a city will find itself with its Smart City systems being held for ransom.

Attackers are driven to find ways to obtain and maintain unauthorized access without the knowledge of the smart city government/management. The compromise can go unknown for days, months or even years. Typically, attackers do not attempt immediate damage but instead:

- Sell access to other criminals, nation states or terrorist
- Wait for a specific timing to cause a certain damage which could be backed by Political, Economic, Socio-Cultural, Technological, Legal/Regulatory or Environmental (PESTLE) motivation
- Spy on the city operations to turn them to their advantage, financially, politically...
- Slowly and gradually cause frustrating problems for city users and businesses causing them to lose faith in a long-promised better environment, faster growth, and an enhanced living experience.

As per a study on critical infrastructure threats (1), the percentage of industrial computers under attack grew from 17% in July 2016 to more than 24% in December 2016. Every fourth targeted-attack detected in 2016 was aimed at industrial targets. Another example is when attackers infiltrated the power grid facilities in Ukraine and were able to cause blackouts in major regions in the country that lasted up to an hour and resulted in major disruption of ordinary living practices and civil peace (2).

(1) https://www.infosecurity-magazine.com/news/40-of-ics-critical-infrastructure/
(2) https://www.wired.com/story/crash-override-malware/

With increasing numbers of connected systems in smart cities, cyber attackers will attempt access to loopholes and vulnerabilities. The smart cities by standard will use combinations of software, hardware, and geospatial analytics to create better livable areas for the residents. Smart cities need accurate data to function properly, hence altered data can disrupt operations. Smart cities must prepare for the worst, preparation is not just about developing a crisis response plan, but also creating a cyber crisis management strategy to respond to a crisis once it occurs. A cyber crisis management plan can be the key to securing smart city systems and surviving attacks when they occur, admitting the fact that cyber threats continue and will continue to evolve.

SECURING SMART CITIES

The role of the smart city department (SCD)

The cybersecurity role of the smart city department (SCD) has been previously detailed in a separate document from Mar 2016 (1). The smart city department is expected to be part of numerous organizations, a team in charge of smart city operations and responsibilities. The SCD is expected to make part of every medium size to large size organization, being in charge of smart city functions, tools and a liaison contact with other smart city entities. In reality, SCDs or similar functions, have already been established in a number of cities and large organizations, strategically working on digital transformation programs for the development and compatibility of organizational processes with smart city requirements. SCDs initially will help in adapting efforts and changes needed to transform business processes and practices to better support smart environments, but the will also govern organizational performance, smart city compliance, legislative communication and collaboration with the smart city government entities.

(1) https://securingsmartcities.org/wp-content/uploads/2016/03/SCD-guidlines.pdf

The SCDs have cybersecurity responsibilities as the smart city is highly dependent on the ICT infrastructure. It will, therefore be responsible for cyber crisis management and will be expected to be in charge of coordinating and adapting organizational requirements and services to the smart city. Government SCD are expected to establish a cyber crisis handling team of specialist, which will be in charge of managing a cyber crisis on the city level and coordinating efforts, containment, and recovery. Regular organizations' SCDs are expected to manage the smart city services and requirements from their end, sharing their problems with the Government SCD, coordinating help and the need for help in times of crisis.

The role of drones in smart cities cyber crisis management

On land, in water or Flying, there are numerous roles to be played by drones inside smart cities, municipal drones program security has been previously detailed in a separate document. The role of drones is also expected in a cyber crisis incident, that role differs depending on the scale of the attacks, their extent and the needs that drones can fulfill through their agility, flexibility, and survivability though drones themselves can also be vulnerable.

Drones role in times of crisis could be critical for faster services recovery in the smart city, drones could provide support for the incident investigation and response, they could also help quickly investigate artifacts and collect evidence to crisis management team (example: from data centers) or even tracking of a user or a system connected to the network which is part of the attacks. Drones could also be directed to do tasks such as disconnecting a network cable, transmission tower or others…

Drones could also provide Infrastructure and communication support through establishing alternative communication networks over the city in case the regular infrastructure is not operational, such could be used for establishing basic critical services, recovery communication among the different stakeholders… To note such a measure would require a specialized drones program and an independent drones' infrastructure capable of operations using a separate infrastructure.

For more information on municipal drone programs, check our previously published paper on the smart cities municipal drone programs safety:

(1) https://securingsmartcities.org/wp-content/uploads/2017/02/municipal_drones_FINAL.pdf

The Smart city cyber crisis lifecycle

When an attacker targets an environment, a prolonged process unfolds from the initial intrusion through to an eventual data breach if the threat actor is left undetected. The impact could be minimized if the attackers are detected in an early stage, reducing the mean time to detect (MTTD) and the mean time to respond (MTTR) where threats are detected and terminated early in their lifecycle, thereby avoiding downstream consequences and costs. It is important to note that not all cyber incidents in the smart city would be considered cyber crises, the smart city needs to accurately and legally define the circumstances by which a cyber crisis is detected and then how the related response process is activated and followed.

A cyber crisis lifecycle typically involves the following steps:

1. **Preparing for a cyber incident:** This involves typically preparing during the peace times. A Smart City should be ready with cyber incident response plan and effectively conduct regular mock drills to ensure the stakeholders are fully aware and ready when in case of actual incidents.
2. **Detection of a cyber incident:** The information security measures should be able to detect and identify a cyber incident or crisis. Notifications on cyber-attacks could also come from third parties such as Homeland Security, MI5, and other cybersecurity agencies set up by regional and national governments.
3. **Cyber incident response:** When a cyber incident is reported, the incident response program is activated, and a response team is assigned to coordinate the investigative processes and an incident response plan.
4. **Ongoing investigation:** When an investigation is ongoing, reporting on findings should be well coordinated and reported to the relevant parties, threat intelligence should enable a better understanding of the attacks and their goals. Other local governments may be at risk as well and mutual aid agreements, as well as non-disclosure agreements, should be established.
5. **Involvement of third parties:** external experts could be contacted for investigative support and should be ready to get involved in investigations and being a point of

reference with technological or cybersecurity vendors. External experts can support in validating investigative results, confirming vulnerabilities and supporting remediation measures, experts could have witnessed resembling attacks and could provide quality advice accelerating response and recovery.

6. **Containment plan:** When an investigation reaches a certain understanding of the attack severity and scope, a containment plan is pushed to isolate affected parties or systems and recovering operations
7. **Communication with appropriate government authorities:** National Security involvement in incidents could happen in early stages or later stages of the attacks, depending on the case security and support needed. National Security agencies can support in different ways: e.g. requesting collaboration from other countries on investigating attacks or tracing attackers...
8. **Notification of stakeholders:** After the nature and scope of the cyber-attack is known, the city must reach out to affected stakeholders to notify them of the attack and how they have been affected in addition to other measures required from them.
9. **Full remediation:** The smart city would then develop and deploy a remediation plan, customized for the attack case, enabling the full recovery of services and the blockage of the threat.

A cyber crisis strategy should typically involve the following steps:

1. **Pre-Crisis: Smart cities cyber crisis planning**
    a. This is a phase where the city is providing normal services
    b. This is a phase of preparation and discovery of suspicious activities
    c. In this phase, risk assessments, anticipation and response plans are developed
    d. In this phase, organizations conduct mock cyber drills to evaluate the readiness to deal with any cyber crisis.
2. **In-Crisis: Smart city cyber crisis response and containment**
    a. In this phase, a threat is discovered and is judged to be on a crisis level
    b. In this phase, the threat is investigated, analyzed, contained and mitigated
    c. In this phase, all smart city components are expected in a high level of alertness and synchronization, to dissolve any nuisance
    d. In this phase, stakeholders and law enforcement agencies are notified and updated or occurrences.
3. **Post-Crisis: Smart city cyber crisis recovery targets and aftermath**
    a. In this phase, mitigated threats are monitored for signs of resurgence
    b. In this phase, the incident response case is concluded
    c. In this phase, improvement proposals are expected to appear for better resilience against similar attacks and faster conclusion of similar occurrences.
    d. In this phase, lawful measures are then followed to identify and prosecute attackers.

SECURING SMART CITIES

Pre-Crisis: Smart cities cyber crisis planning

Smart cities should effectively prepare for cyber crises by adopting a well-developed crisis management plan, they should also be able to handle multiple cyber incidents at the same time. A crisis management lifecycle involves different stages, each aimed at protecting smart cities from cyber-attack related risks and consequences. It also strengthens smart cities' security systems on an ongoing basis. Smart cities should strive to secure their critical systems and infrastructure. The value and classification of digital assets in a smart city should be clearly noted and regularly reassessed with prioritization, the most valuable smart city assets are allocated enough resources in proportionality to their significance.

Definitions: While preparing to respond to a crisis, smart cities are first expected to perform risk assessments to define scenarios by which smart city components could be abused or maliciously employed in an organized cyber-attack. These scenarios could later be tested if the smart city decides to hire external ethical testers to validate the smart city resilience or to test its own handling abilities of a crisis via live drills. The goal is to maximize efficiency when such events occur and minimize the number of tasks and resources required to fully recover from an incident.

Training: Smart cities stakeholders including residents and citizens, inside organizations or even at home, should be aware of how their personal access permissions and online behavior can be the cause of problems for themselves or the city. Smart cities are expected to offer training programs on cyber skills as part of maintaining proper vigilance on critical digital assets targeted by cyber attackers. The smart cities can then better understand what can happen in case of an incident through war-gaming and simulation of cyber events. This helps the leadership to understand the steps required to deal with an attack and whether the smart city is prepared to deal with an impending cyber crisis.

Escalation points: Escalation points and processes are a necessity in a distributed environment such as the smart city, abnormal events faced by separate teams and which might not be meaningful, could actually map and correlate to an organized malicious activity on the city level. Such processes need to ensure that the different entities have the tools and contacts they need to help the city discover the full potential impact of an incident while ensuring that the minimum number of false alarms get escalated to senior leadership. Processes, escalation points and stages of response, therefore need to be well developed, well documented, continuously updated, in a widely distributed handbook that the different city entities need to be aware of.

Smart cities organizations role: SCDs inside smart city organizations are expected to interface, sync and share information with the smart city government SCD, the goal is to keep a high level of readiness, cooperation and collaboration ongoing towards faster resolution of problems, especially in times of crisis. Organizational SCDs are also expected to share information on suspicious activities they suspect or identify on their services.

Large-scale training exercises: live training drills are expected to be done on the city scale to emulate a crisis and test its resilience and response. Live drills enable a better understanding of roles and responsibilities, though also help optimize containment and recovery speeds.

A smart city's preparedness is evolutionary and must be constantly evaluated to match up with the evolving nature of threats. When this happens, smart cities would be ready to effectively react and respond to cyber crisis after which the city can recover and get back to normal operations.

Readiness strategy

The organization and management of smart city crisis management team calls for proper readiness governance. Smart cities are expected to develop a response strategy to define how they manage, prioritize and communicate during a cyber crisis. The values of the smart city must be aligned with the response management strategy. A good strategy enables well-resourced and cost-effective techniques that are capable of influencing the whole city in case of a cyber incident. The strategy doesn't just minimize devastating effects on the city's revenue and operations, but also facilitates response planning. With good governance, smart cities support the coordination of programs across policy documentation, functional areas, incidents, processes, and well-defined responsibilities, roles, and protocols.

A crisis response strategy must typically address the following essential requirements:

- Create an independent crisis management team with clear roles and segregated duties. The goal is to efficiently find causes of a cyber-attack and practical remediation steps. Crisis Management Team members are expected to be accountable decision makers on crisis handling, control, monitoring, and recovery.
- Designate a champion/leader to coordinate actionable items with team members and facilitate cyber incident response cross-functional collaboration.
- Identify the allowed secure and reliable communication and rescue channels as part of a communication strategy
- Define escalation and coordination points and priorities to better coordinate and manage recovery.
- Test a crisis management plan against operational effectiveness using relevant training scenarios (e.g. war-gaming, live drills...). The goal is to ensure crisis management team members are skilled and ready for handling an incident.
- Define the cyber crisis incident response and recovery stages (business continuity), together with a decision framework based on milestones.
- Identify reporting mechanisms and restrictions to recognize what should and should not be reported and to whom.

- Perform Red and Blue Team exercises regularly to assess the chances of adversaries compromising smart city networks and systems and testing defenses, part of a crisis simulation exercise.
- Engage the team in charge of government affairs in the smart city or other liaison function of the government, to ensure regulatory agencies are well informed and involved in teams' orchestration. This step is critical to the commitment of different parties involved in city's critical infrastructure.
- Define ways to monitor threat intelligence; for any local or larger sentiments building up which may cause adversaries to launch attacks and on the city network and systems.
- Align IT, engineering and security management initiatives with response efforts, while also defining allowed communication channels, for communication with internal and external authorities
- Define smart city stakeholders' priorities and how they can be helped in the case of crisis.
- Define steps and processes with which the affected stakeholders will be supported
- Test and update plan and staff skills as often as needed

Technologies strategy

The administration and handling of cyber incidents are technocratic by nature: techniques for cyber threat management, crisis management, incident monitoring, detection, response and recovery are developed and deployed by teams in charge of IT and cybersecurity. After an incident, a technical investigative and forensic team conducts investigation and response to analyze security lapses, control failures and screen other associated systems related to the cyber incident. The following identifies some technologically significant measures to keep in mind in incidents management activities:

- Identification of required investigative and response tools and solutions to minimize risks and boost operational and security capabilities on a city scale.
- Identification of required forensic resources and skills, identify available technical capabilities
- Definition of short-term and medium to long-term solutions to be implemented after a cyber incident is detected.
- Avoid workarounds to meet short-term priorities, especially if such open additional risk
- Threat intelligence gathering techniques, usage, and sharing
- Identify and implement means of effectively performing centralized security monitoring and respond to attacks in real time.
- Technology solutions and their providers should be carefully evaluated and proper due diligence to be done before selecting a particular technology.

For more information on guidelines for smart city technology adoption please see SSC previously published document:

(1) http://securingsmartcities.org/wp-content/uploads/2016/03/Guidlines_for_Safe_Smart_Cities-1.pdf

Communication strategy

Smart cities should develop a strategy for public relations and a plan for communication with stakeholders upon a crisis. It must also integrate a team of public relations staff and government attorneys with the team in charge of crisis management, an executive leadership committee.

An appointment of a Cyber Crisis Secretariat (CCS) is desirable. CCS and its team can help to drive the management and resolution of a major Smart City cyber-attack crisis with timely assessments and recommendations as well as, the necessary post-crisis proposals and criminal investigations (if any). CCS therefore is vested with the power to direct the coordination of respective incident response leads (including advising on specific mitigation measures); and in the event of any breach, the associated public communications.

As communication allows stakeholders to be informed and assured that a problem is being handled in the most proper methods based on available information and circumstances, it also allows certain stakeholders feedback (e.g. citizens could suspect and report any suspicious activities if they face them). Hence, CCS presents a structured and coordinated communication approach.

A communication strategy could be expected to address the following requirements:

- Plan in advance a communication team, a public relations team and how they integrate, collaborate with the crisis management team.
- Media communications should be vetted to avoid misinformation.
- Define points of contact and communication decision makers
- Continuously notify affected or impacted stakeholders on containment and progress efforts

Communication of the crisis is crucial; smart cities should continuously respond to requests from business partners, investors, other government agencies, customers, vendors, the board of directors and regulators. The processes, plans, and methods of sharing information on the crisis with relevant stakeholders need to be ready to handle incoming requests. What is known regarding the cyber crisis should be proactively shared transparently with the public and with stakeholders. The smart city's response to the cyber-attack and intentions of what should be done can easily trigger negative reactions on the web, social media sites, these conversations should be monitored and addressed. Despite the level of trouble involved, smart cities can maintain order to the chaotic environment with a disciplined and properly structured crisis response. An organized, structured response with clearly articulated chronological events timeline with various vendors and technology partners, not only enables a better city response but also prepares the city for regulatory inquiries, litigation or

congressional inquiries in the future, it also shows a city is reactive and not helpless which is devastating. Governments that have already in existence an Office of Emergency Management (OEM) will be able to easily adjust OEM roles and responsibilities to include cyber incident management.

In-Crisis: Smart city cyber crisis response and containment

Smart cities should develop a cyber incident response plan with a predictable path despite the exact location, the extent of attack and incident impact being unpredictable. The response quality of smart city entities and/or executives to an incident can limit the impact of a cyber crisis or make it worse. Smart cities can limit the time needed to deal with issues, stakeholders impact, and financial losses while minimizing recovery costs and damages to the reputation of the connected cities. The smart city management should be ready to communicate to the public and orchestrate stakeholders' actions through well-defined and protected communication channels. This assures smart city stakeholders that whatever is being undertaken to counteract the cyber incident or crisis is good enough.

Smart city entities are responsible for acting as trained and following incident response handbook scenarios in limiting the reach, dealing with, containing and reporting of an incident, nevertheless, in reality, a smart city should expect undocumented and previously unknown scenarios which would require improvisation and strong leadership. Part of dealing with real-life scenarios, a smart city should consider being self-dependent in terms of services activation, cloud services availability, performance and functions, enabling independent stable operations even in rare cases of international links disconnections whether due to physical causes (submarine fiber cable faults, intentional or not) or digital causes (very large distributed denial of service attacks).

The monitoring and logging of the response in different smart city entities enable the city afterward to identify missed opportunities or processes that could be implemented better, maybe even recognize anomalies or insiders that negatively impacted smart city recovery.

During the incident response, while a smart city is focused on operational recovery, it is also expected to continuously monitor regular sources of attacks as to avoid coordinated attacks from multiple sources. The city might need to involve external parties to acquire needed resources and expertise to conduct specific tasks. In the following, we list some of the services that could be outsourced to external parties:

- Incident response and forensic services on compromised systems, data centers and networks as well as electronic monitoring. The specific services offered include analysis and forensic preservation of evidence, malware analysis, artifact analysis, network traffic monitoring and investigation logging, etc.

- Hunting for threat-related activities, the smart city could also establish bug bounty programs to enable whitehat researchers to find loopholes before threat actors do.
- Fraud mitigation services, including financial monitoring and tracking of transactions
- Customer support, including call centers and support ticketing services

While outsourcing is a method to acquire help upon need, there is a lot of debates around the security and quality of services offered when outsourcing is offered. Smart city core teams of specialist are expected to monitor, control and be accountable for outsourced resources activities and assigned tasks.

During an incident containment, a smart city is expected to exert number of actions to help further identify the threat and block its spreading and access. Such could require disconnecting systems, networks, data-centers or even complete organizations as a short-term containment plan in order to restore services. The long-term containment plan would require a different set of actions such as reconfiguring or patching certain systems on the city scale or even replacing certain systems if decided.

Smart cities need to evaluate the causes of the incident, especially on whether the attacks utilized weaknesses that are still open to abuse. Knowing that smart cities are data-driven, understanding potential vulnerabilities and the fact that hackers can launch attacks from various angles, repeatedly, helps prepare a smart city to perform a good containment. A containment strategy needs to isolate an incident efficiently, in order to allow recovery operations to start, it also needs to be validated and approved by the crisis management team after initial incident analysis and before being executed. Its effectiveness needs to be monitored and might require adaptive actions and amendments for enhanced efficacy.

Post-Crisis: Smart city cyber crisis recovery targets and aftermath

After responding and containing an attack, recovery of services needs to be taken into consideration towards restoring services to full productivity status within the minimum possible time period. Different scenarios should involve different recovery mechanisms and tests, for example recovering from a power shutdown problem on a wide scale and depending on the off time, could have affected other industrial or manufacturing services, or could have been the cause of medical issues for some citizens…

The smart city might require different methods to recover services, backups, backup systems, disaster recovery sites... Recovery should start with critical functions and applications (e.g. Critical infrastructure) and then move towards less critical ones, the goal is to restore most city functions in the best Recovery Time Objective (RTO). The recovery of functions should attempt to restore the most up-to-date or the best Recovery Point Objective (RPO). After recovery, threat vector should be patched or blocked before taking the service online. Monitoring and validation of correct service behavior then also needs to be done.

Cyber crises can also bring about regulatory action or legal consequences, whether related to pursuing attackers or caused by the damage due to non-availability of services which could also be represented by service level agreements among the different city stakeholders. Therefore, smart cities must determine available legal recourse depending on the case and offer a legal framework from which liabilities can be analyzed, response events and actions can be coordinated.

After the cyber crisis, a smart city should put measures in place to secure its critical infrastructure and systems from current and future threats. The smart city must be aware of its threats, IT assets, and vulnerabilities for examination within the city's business realm. Such can later on develop trust in the city capabilities and drive investments. It can also ensure that the smart city is able to achieve its goal of protecting its growth and enhancing the lives of its residents. When a crisis is concluded, evaluation of the current cyber crisis management plan and response is expected to happen, improvement proposals are expected to be reported to senior officials for enhanced resilience against future attacks and faster conclusion of similar occurrences. Lawful measures should also then be followed to identify and prosecute attackers.

Smart cities should consider the following cybersecurity elements to boost their crisis aftermath:

- Continuously monitor recovery stability and effectiveness, restore functions health to best standing
- Identify long-term strategy to close loopholes and causes of the problems
- Maintain a list of primary and support assets, a dynamic list of key stakeholders based on distance from sites, their abilities, and expertise
- Adapt response, strategies and plans to best deal with recent threats
- Seek legal advice on possible measures that could be taken to better deal with current and future events
- Develop a shared culture and vision to advance the smart city cyber safety
- Continuously measure and collect feedback on the trust of stakeholders and their believe in the city future

Conclusion

Cyber threats that affected businesses years ago are not the same as today's but we do have an opportunity to influence future threats for the benefit of our citizens. Cyber attackers and terrorists work to identify threats with few or no countermeasures. Cities are developing over the years and are emerging into smart digitized regions with centralization and automation. The increased connectivity makes anything vulnerable to cyber threats, hence the need to safeguard a city's most critical digital assets. However, it's not possible to protect a city completely from all threats, significant effort needs to be exerted to minimize financial, operational and risk to the public trust. In addition to investing in cybersecurity skills and

systems to safeguard assets and data, smart cities must develop a cyber crisis management plan to help curb emerging threats while at the same time pressing service providers and system vendors to build-in cyber security as well as take-on liability for products that fail to have inherent product integrity.

A crisis management plan is part of government due diligence and helps smart cities to manage cyber incidents as they occur, neutralizing or reducing the negative impacts of cyber incidents. Disaster recovery and business continuity plans should also be integrated into the plan. With off-site live/ready backups, smart cities can quickly get the affected operations and systems back up and be running. Being prepared for a cyber incident is a prime mission of government and should not be sacrificed for convenience. Smart cities should prepare for coordinated response by rehearsing, war gaming and taking part in other structure preparation and communication testing techniques. Every decision made in the face of a crisis can either heighten the safety and reputation risks, further destroying a smart city's values and stakeholders', or help block it, contain it and resolve it. Proper decisions can help prevent heightened risks and losses, "The Core of a Smart City Must Be Smart Governance."(1) . There is a need for fast response once an incident is reported. With crisis response teams on the ground and utilizing all capabilities responding in minutes to inspire confidence, act on insufficient information, take charge, communicate and lead with flexibility.

(1) https://go.forrester.com/blogs/11-05-15-the_key_to_being_a_smart_city_is_good_governance_smart_governance/

Even after the smart city cyber crisis, decisions must be logged, data captured, insurance claims handled, finances managed and legal and regulatory requirements met, that is how stakeholders trust is restored and retained, everyone knows there is no such reality as 100% cyber secure, but everyone wants to see such being given the righteous attention and seriousness. Cyber incidents give smart cities the opportunity to respond effectively and succeed, and the chance to enhance strategy and systems to improve services and operations. Smart city stakeholders must be trained to understand the risk of cyber threats and their likely effects on the city, its operations, services and what to expect in case of a cyber crisis. The city management must ensure that the city and its stakeholders are well-prepared for a cyber crisis, can communicate properly and respond immediately to events. With a properly structured, well-coordinated and an orderly crisis response, smart cities can enjoy relative cyber peace in abundance, while in the background the cyber security staff are managing and mitigating incidents. A properly planned smart city cyber crisis management solution coupled with efficient execution can overcome the worst of data breaches and cyber crises; preventing most such incidents. As cyber threats evolve and become more sophisticated, smart cities must evolve too and adopt new counteractive solutions, ensuring that their cyber crisis planning, education and awareness efforts are always up to the challenge.