Digital citizens in a smart city: The impact and security challenges of IoT on citizen's data privacy

Robert Benedik[1], Haider M. al-Khateeb [2,*]

[1] Northumbria University London Campus, Northumbria University, UK
[2] Wolverhampton Cyber Research Institute (WCRI), School of Mathematics and Computer Science, University of Wolverhampton, UK

* Correspondence: H.Al-Khateeb@wlv.ac.uk

Abstract**—**Cities are investing in smart technologies to improve efficiency, resilience against cyber attacks and quality of life for their residents. They provide enhanced services and can largely benefit the environment too. However, there are a variety of security implications during the transition towards a smart city. For example, anticipated risks have an impact on the citizens' safety, privacy and access to critical national infrastructure. Therefore, smart technologies must be carefully planned to maintain efficiency, security and overall desirability. We follow a holistic approach to review these risks with a proposed CyberSmart framework focusing on four domains namely Cybersecurity risk, Cyber Resilience, Data protection and privacy, and Governance (CRPG). The discussion is formed around data privacy alongside strategic solutions to address related aspects such as the management of operational risk, key stakeholder complexity, and lack of trust in new devices. The proposed framework helps to identify and build mitigating actions to support incident response planning with a focus on prevention and management. It also demonstrates the importance of collaboration to address resilience at a strategic level.

Keywords: cyber natural, smart environment, digital citizens, regulation, user privacy.

1 Introduction

The rapid evolution of Information and Communications Technology (ICT) has benefited and restructured how people interact both in their business and private lives. Alongside these innovations, companies developing digital and networked solutions have started integrating three principal technological systems into urban cites: the Internet of Things (IoT), cloud computing and big data analytics. With these system integrations, the "smart city" has been defined. As smart cities are driven by the data input of their citizens, challenges are posed by expectations of privacy and security of systems and data as a whole. According to studies [1], this involves capturing Personally Identifiable Information (PII) as well as data about citizens households and linking this data together to profile citizens to make decisions about them. For instance, research on user profiling shows that people can be classified and identified based on a short segment of driving data [2]. From a legal perspective, where clarity can often be found, privacy breaches are typically covered under laws such as the General Data Protection Regulation (GDPR) in Europe, and by sets of privacy laws across the United States (US). However, these statutes tend to lag contemporary technology deployments, including the quickly evolving "smart city". Besides privacy concerns, there are other many security considerations to be made in deployments of smart cities. Smart cities are prime targets for cyberattacks and the protection of collected sensitive data is of primary concern [3]. It has become evident over time that many manufacturers of "smart city systems" have primarily concentrated on developing functionality at the expense of securing their systems. It also remains unclear who is accountable to fix deployments within a smart city if a system is exploited or crashes, or who defines policy on how a system should be defended against possible cyberattack. It is evident with the development of smart technologies that new risks are not investigated thoroughly and there is a lack of regular forums that investigate this [3].

R. Benedik, and H. M. Al-Khateeb, "Digital Citizens in a Smart City: The Impact and Security Challenges of IoT on citizen's Data Privacy", in *Challenges in the IoT and Smart Environments, A Practitioners' Guide to Security. Advanced Sciences and Technologies for Security Applications*, R. Montasari et al., Ed. Cham: Springer International Publishing, 2021, pp. 93-122, Print ISBN: 978-3-030-87165-9, Electronic ISBN: 978-3-030-87166-6. DOI: 10.1007/978-3-030-87166-6_5. [online]. Available: https://doi.org/10.1007/978-3-030-87166-6_5

The widespread use of the Internet of Things which is the foundation of smart cities has caused many questions around security, data privacy and data protection. Therefore, having a robust framework and sophisticated protection models is critical in supporting both academic and industrial areas. Motivated by these reasons, the CyberSmart CRPG framework is proposed for smart city managers and stakeholders to support the development roadmap during the transition from an urban city to a smart city. It is predicted that now and, in the future, mitigating, controlling and managing existing and new risks will be a critical task due to the data and security risks and impacts highlighted in this paper.

In the remainder of this paper, Section 2 discusses the characteristic of smart cities from the literature review point of view of similar works in the field, followed by the current unidentified risks and vulnerabilities in smart cities in Section 3. Section 4 proposes a framework on how the different demands and aspects can be governed. Section 5 details a roadmap on the deployment of the framework against a model smart city. The conclusion and statement of future work are then shared in Section 6.

2 Background and related work

Increasing populations within cities mean that managing growth is a rising concern. With this sustained growth, urban areas are facing challenges and pressures that this influx brings. By employing more sophisticated technology, concerns such as traffic congestion, public safety and sanitation can be addressed and managed more efficiently and effectively. The building blocks of a smart city support these developments, incorporating networks and communication, processes, data management and security, trust and privacy [4]. In return using these technologies in a smart city may result in emerging and increased exposure to risk, which needs to be catered for properly.

2.1 Building blocks of a smart city

Urban agglomerations can trigger the development of a variety of problems that need solutions. The Smart City concept addresses this and has already demonstrably improved many factors of urban life. Examples include how transportation is monitored and used, supporting the education system, monitoring energy usage and allowing individuals to monitor their health and medical treatments [5]. These challenges are addressed through creativity, cognition, and cooperation among relevant stakeholders to design smart solutions [6].

Benefits from smart solutions have been recognised by governments, both local and national, and as adoption rises it begins to improve living standards and drive the move towards big data applications. It is recognised that many sectors of a city’s economy can be enhanced by big data applications. An example is surveillance monitoring through the usage of devices such as CCTV, which can be used to relieve congestion dynamically or protect the public by monitoring, detecting and preventing crime in its early stages [7].

At the outset of this burgeoning rise of smart city technology, there were a variety of different terminologies used to describe its constituent parts, including digital city, hybrid city, ubiquitous city, information city, wireless city and intelligent city [8]. The concept of a wireless city was often extremely confusing as people linked this to wireless communication such as public Wi-Fi provision. It became apparent that the varied names caused confusion, and the term smart city became the preferred choice. The word “smart” itself suggests artificial intelligence and automatic technologies such as self-configuration, self-healing, self-protection, and self-optimisation are used extensively across the components of the model [8]. As a whole the term smart city signposts technologies that allow modern cities to grow and thrive through increased productivity using clever solutions. Overall, smart cities use technology, to automate and improve city services [9], they are built from a network of items, these items are embedded with sensors connected to the Internet.

In a research paper on the concepts of smart cities, Sikora-Fernandez and Stawasz discuss that cities can be defined as smart if they have the dimensions [10] illustrated in Figure 1.

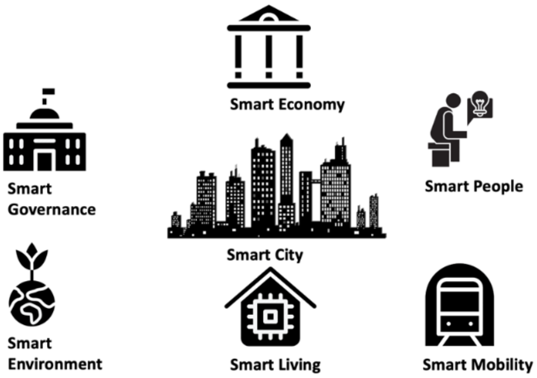


Figure 1. Smart City

To understand a smart city, it is important to realize how the technology supports its further development and how it supports new opportunities to promote a more sustainable and resilient way of living. A variety of studies have been conducted to research the components and infrastructure of smart cities; some have focused on the international point of view on smart buildings [11] and in favour of smart cities having a positive impact on the environment if used to their full capability. They also recognized improvements possible in security management using the technology provided, and the low operational costs to deliver the benefits [12]. [13] conducted a study where the author evaluated the efficiency of every energy source to investigate how smart energy systems supported a sustainable future. The authors concluded that, if products from the same energy source increasing then a greater efficiency is achieved with lower emission levels. During the study, Dincer and Acar were in favour of geothermal energy due to it being a cleaner and more sustainable resource. [14] carried out their research on the Internet of Things (IoT), and what the impact of smart water management would be on businesses. The creators proposed a model that would support both urban cities and extend beyond that to rural areas, which would be feasible if IoT development was integrated into smart city models. In [15], the authors researched smart mobility and transportation which highlighted the rapid expansion of Information and Communication Technologies (ICT) in smart cities. The authors suggested new frameworks should be created where people should know what they want and what they need to bridge the policy gap. Without this careful definition then policy implementation would fail.

The building blocks of a smart city can be categorised into four as shown in Figure 2, each of which will be discussed in the following sections [6].

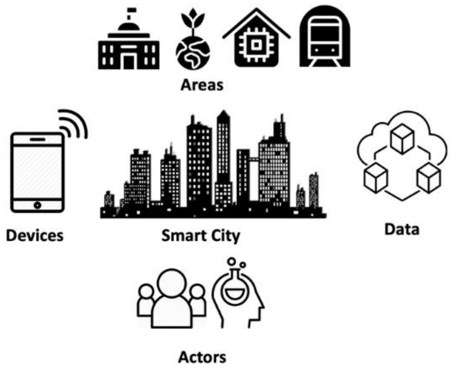


Figure 2. Building Blocks in a smart city

2.2 Actors in the smart city

To ensure a smart city is developed successfully, it is critical that there is an understanding of the needs and wants of the actors (stakeholders) within a city. Therefore, there is a requirement that time and research is invested to understand the market and what the key drivers and motivations are to appeal to the majority. The final solution of what a smart city looks like may be similar each time, but by understanding the actors it can be implemented by really focusing on what their motivations and interests are to be most effective. Actors within a smart city fall into the criteria below [6]:

- Individuals (residents, visitors, city activists)
- Businesses
- Vendors (hardware, software and system integrators)
- Government (national, regional, local)
- Academics (public, private or independent researchers)
- Organizations (multinational, non-governmental, philanthropies)

2.3 Areas of application of smart city technologies

When identifying areas within a city that can be improved by smart city technology, some are more receptive than others to enhanced technology. The main areas of focus are utilities, mobility, safety, health and education.

- Utilities (smart grids, smart meters)
- Mobility (smart parking services, smart transportation, smart traffic management)
- Safety (smart surveillance, smart identification)
- Health (smart healthcare)
- Education (smart education)
- Governance (smart governance)

2.4 Devices (What is IoT?)

Devices are recognised as different things to people. These could be smartphones, laptops or smartwatches for example. However, when looking into the building blocks of a smart city, the definition of a device expands way beyond this. Devices are used at a much larger scale and often connect and communicate with one another (machine-to-machine - M2M). The Internet of Things (IoT) is what makes the connection of these devices possible. IoT has different interpretations for different people. Initially, the classic internet was designed to be a network of computing devices and networking equipment (servers, routers switches firewalls etc.). However, IP cameras, various sensors, and smart assistants, smart meter readings, smart home appliances (such as Alexa), smart locks are some examples of when a physical object is developed with connectivity, computing, sensors and actuators to become an IoT. It should be noted however that many of these devices may not be attached to the Internet at all, but to private or encrypted networks to maintain their integrity. The term IoT may continue to be applied to these devices/sensors. In Figure 3 we can see many of the possible components of an IoT.

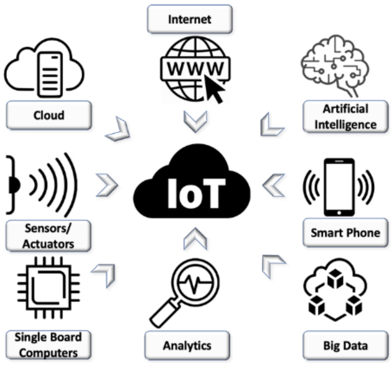


Figure 3. The IoT

But why IoT? By combining multiple inputs from the physical smart things, the overall outcome can increase in value for the user. The use of smart devices provides the opportunity for monitoring and analysis and to close the system loop - in turn allowing the production of an intelligent outcome. The beneficiaries of IoT include end-users as they gain the ability to monitor and control devices remotely, thus in turn they can use “the things” efficiently by saving time and resources. In turn, the lifespan of the service can be extended, and overall experience improved through this collaboration. Likewise, manufacturers benefit by linking IoT to smart devices to develop the value of the services around the product. By monitoring devices' in real-time, their location, condition, usage and performance can be monitored and tracked. This assists in product improvement, to offer enhanced services and upgrades in the lifecycle. Aggregating data too from multiple sources gives valuable insights which can then be monetised potentially, depending on user agreements/anonymization etc.

IoT is generally categorised into the following categories;

- Consumer IoT (smart home devices)
- Industrial IoT (agriculture, wind farms)
- Civic IoT (smart public transportation, smart water supply, smart electric grid)

There is no specific set architecture for IoT, but we can use the IoT architecture in Figure 4 as a guideline. Within the architecture is a base layer that manages the physical interaction through smart sensors to measure, feel, collect and control instruments. This data is then transferred into the upper layer, which collects the information and determines how the information is routed to alternative networks, devices and IoT.

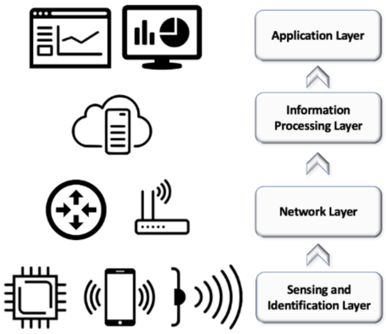

Application Layer
Information Processing Layer
Network Layer
Sensing and Identification Layer

Figure 4. IoT architecture

2.5 Data

The new most valuable resource in the world today has changed from oil to data. A modern city runs on data. In a smart world, data is a critical asset of an individual as well because it contains a vast amount of valuable personal and sensitive information including bank account details and history, medical records [16], passwords and location coordinates. This data can be accessed if the hardware or software is hacked due to vulnerabilities in its security, or via social engineering of someone who has legitimate access. It should be assumed that threat actors are actively targeting devices and that new vulnerabilities may be identified, spread and be used criminally – so vigilance is called for.

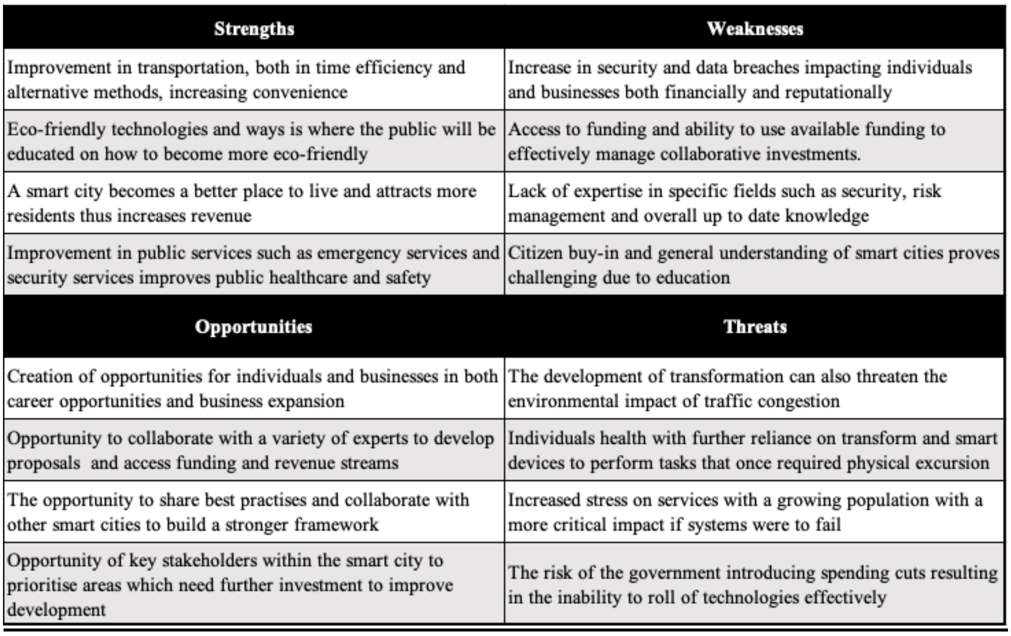
When it comes to gathering and processing large amounts of data, there are a variety of ways this can be performed, including capturing, transferring, storing, analysing, visualizing, securing and ensuring privacy [17]. Data set sizes vary, but over time are expanding as computing analysis allows and range from Gigabytes to Terabytes, Petabytes, Exabytes, and Zettabytes. Data and data management can be extremely confusing, and creating policies of how to access it, protect it and interpret it can often prove challenging. There are a variety of aspects linked to data itself, such as regulations and ownership which also need deep consideration by data processors. How a smart city can use the data it collects is reliant on many factors.

Cyber-attacks are an increasing threat due to the value of data and the level of information it contains. Consumers and companies often find that they have little control over data as IoT security does not alert them when data is being misused. This leads to an increase in regulatory risk and a requirement to strictly maintain data privacy.

Security is a critical component for computer systems. However, the level of security can largely differ across a range of IoT systems. Many of these issues can be due to inefficient security features, security design errors and default passwords as an example. IoT nodes may have a lifetime of several years, therefore, if there is a security issue on a node, it will affect the whole IoT system for the remainder of its deployment. Security also encompasses privacy, protecting the theft of data and defining access permissions between data of different sensitivities within a network.

3 Preparing for Unidentified New Risks and Vulnerabilities within a Smart City

Many risks and vulnerabilities are identified and expected in a smart city. The array of devices, technologies and open systems that are interconnected does not come risk-free. While the expected risks and vulnerabilities are managed with controls and contingencies implemented, there are also those unexpected vulnerabilities that need to be managed. This discussion delves into the challenges that are faced by smart technologies and how smart city managers can mitigate and manage them [18]. Figure 5 shows a high-level Strength, Weaknesses, Opportunities and Threats (SWOT) analysis of factors influencing Smart Cities.



Strengths	Weaknesses
Improvement in transportation, both in time efficiency and alternative methods, increasing convenience	Increase in security and data breaches impacting individuals and businesses both financially and reputationally
Eco-friendly technologies and ways is where the public will be educated on how to become more eco-friendly	Access to funding and ability to use available funding to effectively manage collaborative investments.
A smart city becomes a better place to live and attracts more residents thus increases revenue	Lack of expertise in specific fields such as security, risk management and overall up to date knowledge
Improvement in public services such as emergency services and security services improves public healthcare and safety	Citizen buy-in and general understanding of smart cities proves challenging due to education
Opportunities	**Threats**
Creation of opportunities for individuals and businesses in both career opportunities and business expansion	The development of transformation can also threaten the environmental impact of traffic congestion
Opportunity to collaborate with a variety of experts to develop proposals and access funding and revenue streams	Individuals health with further reliance on transform and smart devices to perform tasks that once required physical excursion
The opportunity to share best practises and collaborate with other smart cities to build a stronger framework	Increased stress on services with a growing population with a more critical impact if systems were to fail
Opportunity of key stakeholders within the smart city to prioritise areas which need further investment to improve development	The risk of the government introducing spending cuts resulting in the inability to roll of technologies effectively

Figure 5. SWOT analysis of factors influencing Smart Cities

Three key technology attributes to support the creation and reasons for having a smart city, but in turn, they also carry their risks are:
1. **Speed and Range**: interconnecting smart devices prove extremely efficient in daily lives.
2. **Interconnection**: complex interdependencies across services are created. Networks support critical services.
3. **Innovation**: The use of innovative technologies provides the novelty of many enhanced services.

While these all show how a smart city can provide many advantages there are also increased risks;

- Operational Risk: Due to the increased reliance on technologies and devices, significant impacts can be incurred due to inadequate or failed processes and systems.
- Management Complexity: Larger areas of expertise are required, and agreements may be harder to reach.
- Ambiguity and Lack of Trust: The level of data that is stored is a growing concern especially with the media awareness of incidents.

3.1 Challenge #1: Operational Risk Management within a Smart City

The threat of increased operational risk within a smart city is largely down to the scale and complexity of interconnected technologies and devices [19]. Not all cybersecurity managers are aware of the scale of vulnerabilities that are linked to devices that are spread across a city [20].

Smart technology is operated in silos and often split across a city's operational domains [21]. These are integrated to support both critical and non-critical processes. Organisational silos can limit the advantages of smart technology and due to the large interconnections can significantly increase the operational risk. Due to this interconnection, if one device contains a failure this is likely to passes on to connecting devices and potentially creating major disruption. Key stakeholders within IT and cybersecurity are required to manage the risk across this broad structure of interconnected devices and technologies and minimise the risks and manage incidents along with security managers.

Operational risk becomes more apparent due to the fact there is so much to learn within how smart city technologies operate and there is a shortage of qualified Smart City and cybersecurity personnel. AI technologies open up new risks as these are more unpredictable in their decision making and data handling. Cyber-attacks may also be incurred from members within the framework who identify a vulnerability and use it to advantage such as stealing data for financial benefits. The more dependant the technology becomes, the more of a target it can be.

3.2 Challenge #2: Management Structure and Key Stakeholder Complexity

With a smart city comes the management and stakeholder complexity. Due to existing processes and services already being available a smart city builds additional layers, which means that processes can range from basic manual ones to brand new automated smart technology ones.

This interconnection and complexity create more opportunities to identify weak security points and take advantage of this. Due to the array of risks that would be present, it is difficult to allocate a risk owner within the management structure. Furthermore, the newness and advantages that may be seen in certain devices may overpower the ability to identify risks. This also comes with the limited expertise within cybersecurity in smart city officials. Further development needs to be completed on risk management and framework standards. Another added complication is the ability for stakeholders to communicate what smart city device requirements are needed accurately to external stakeholders. Lack of authority means that a city could invest in technologies that can be damaging to the city and its citizens.

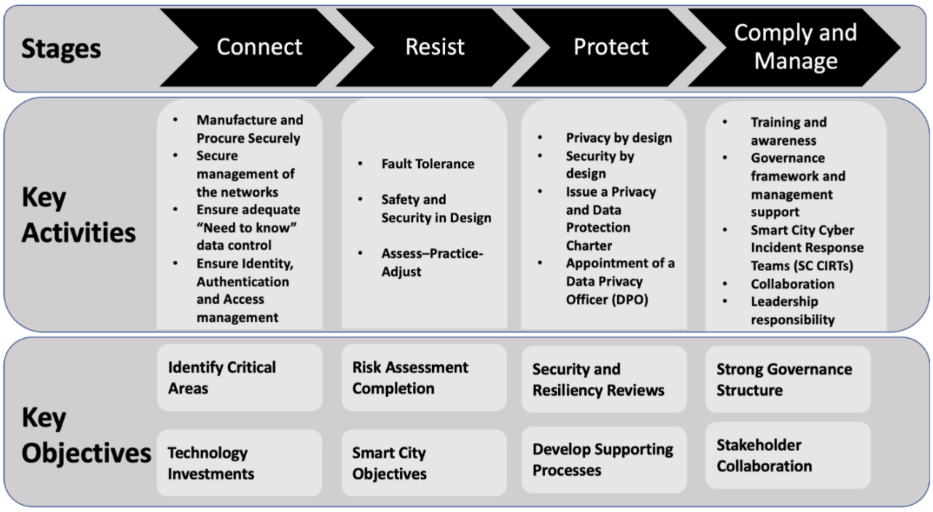
3.3 Challenge #3: Lack of Confidence and Trust in New Devices and Technologies

Distrust and uncertainty are other major challenges that come with the development of technology. For example, when a major data breach has occurred from a fault in a newly installed system, this has a major impact on the public's confidence often resulting in people not wanting to use a potential service [19].

As much as there are some clear benefits for certain technologies which collect data, for example, security surveillance, having so many interconnected devices cause unpredictable behaviour [22]. If the behaviour is unpredictable it means the risk is more difficult to manage and it can be likely that inadequate controls are in place.

4 CyberSmart CRPG Framework

There are several factors for consideration when developing a smart city. Many of the aspects that form a smart city are integrated over a long period and piece by piece. There are also different reasons as to why a city chooses to develop into a smart city. This could be to become more environmentally friendly or to rebuild after a catastrophe or even to improve general day to day living and convenience. Due to the nature of smart cities, new or enhanced risks are a growing concern. In the design stage of smart city technologies, these risks and related controls need to be assessed. Figure 6 presents the different stages within the CRPG framework and their related activities and objectives.



Stages	Connect	Resist	Protect	Comply and Manage
Key Activities	• Manufacture and Procure Securely • Secure management of the networks • Ensure adequate "Need to know" data control • Ensure Identity, Authentication and Access management	• Fault Tolerance • Safety and Security in Design • Assess–Practice-Adjust	• Privacy by design • Security by design • Issue a Privacy and Data Protection Charter • Appointment of a Data Privacy Officer (DPO)	• Training and awareness • Governance framework and management support • Smart City Cyber Incident Response Teams (SC CIRTs) • Collaboration • Leadership responsibility
Key Objectives	Identify Critical Areas Technology Investments	Risk Assessment Completion Smart City Objectives	Security and Resiliency Reviews Develop Supporting Processes	Strong Governance Structure Stakeholder Collaboration

Figure 6. Smart City - CyberSmart CRPG Framework

In Figure 7, we demonstrate the 4 domains addressed by our framework to facilitate such assessment.

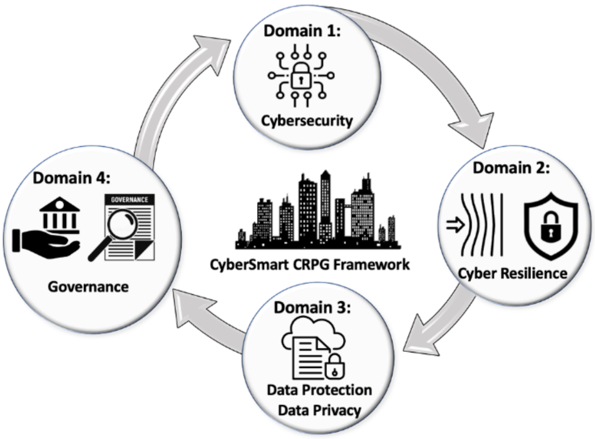


Figure 7 – CyberSmart CRPG Framework

Additionally, due to the extensive range of cybersecurity and data risks that exist within a smart city, Figure 8 shows elements proposed to ensure these risks are thoroughly researched with adequate controls implemented. This in turn will maximise the benefits that a smart city has to offer.

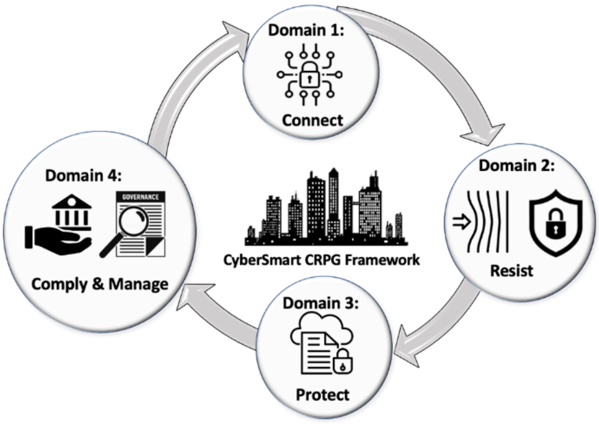


Figure 8. Connect, Resist, Protect, Comply and Manage elements within CyberSmart CRPG framework

4.1 Domain 1: Cybersecurity

When assessing privacy and security within smart technologies, consideration of risk mitigation must be made for both digital and physical aspects of privacy and security. People who operate these systems within smart cities must work together to identify and mitigate these risks thoroughly. To collaborate and manage these endeavours all parties within the city must come together. This includes business owners, the general public, religious organisations, governments and any other communities and residents. Three key elements are defined within a risk (R): vulnerability (V), threat (T) and consequence(C) as shown in Figure 9. If any of these elements increase, so does the risk. This provides a guideline on how to assess risk and how advanced the controls need to be to mitigate the risk. This is presented in a mathematical formula: R = V x T x C.

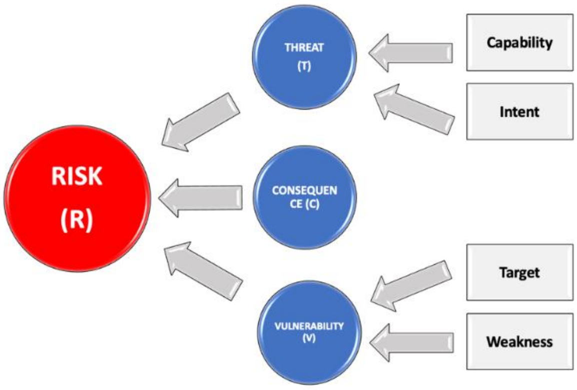


Figure 9. Cybersecurity Risk and its contributing factors

This same risk expression is also relevant within cybersecurity and privacy. Within a smart city and its connectivity, thorough investigations are required for cybersecurity and privacy risks within all fields of a smart city environment. When identifying vulnerabilities and threats within a smart city, enterprise information technology (IT) environments can be used as model guidelines as they contain similar cybersecurity risks and threats. Having said that; smart cities contain a much wider range of technologies and implementations, so there are likely to be more risks identified. In many instances, it has been evident that security and privacy risks are taken underestimated. Cyber-defence is required to be managed effectively by monitoring physical cyber interactions and producing effective policies that communicate effects and systemic risk. This should all be embedded within planning and operations.

4.1.1 Connect

Due to the extensive range of cybersecurity and data risks that exist within a smart city, the general philosophy “Connect” has been developed and proposed to act as a framework to ensure these risks are thoroughly researched with adequate controls implemented. This in turn will maximise the benefits that a smart city has to offer. The approach comprises four elements:

1. **Manufacture and Procure Securely**: Devices should be securely manufactured and enforced with the following characteristics:

- Devices must have the capability to allow regular maintenance checks which will mitigate the vulnerabilities and utilise cryptographic integrity and authenticity protection
- Default passwords must be able to be changed to user-defined and user-managed passwords. By implementing two-factor authentication will create greater security protection
- Cryptographic functions must be utilised with devices and systems, encrypting communications sent from devices must be a necessity
- Devices should be correctly certified. Conformance tests should be completed that are based on recognized security certifications

2. **Secure management of the networks**: Use the comprehensive zero-trust approach to enforce security. Create and maintain an asset list of devices and applications to minimise the threat landscape

- Deploy network segmentation for better access control and improved security
- Integrate logs to security information and event management system (SIEM)
- Take the whitelisting approach (whitelist only legitimate applications) and block everything else

3. **Ensure adequate "Need to know" data control:** Provide education on data obtaining and storage to ensure that only necessary data is collected, stored and maintained correctly.

4. **Ensure Identity, Authentication and Access management:** Ensure that every device is identified and authenticated on the network supported by strong authentication methods such as Multi-Factor Authentication (MFA). Cloud-enabled authentication functions can be used to support internet-connected devices.

4.2 Domain 2: Cyber Resilience

Within smart cities, cyber resilience is in place to ensure critical outcomes and processes are delivered in the event of a major disruption and low impact everyday glitches. Due to the reliance smart cities have on technologies, it can cause major disruption if there is a system failure or an outage on its key technologies. Therefore, cyber resilience is a crucial element as it will ensure that a contingency is in place to adapt and recover in the event of a technology failure [23]. Smart cities are required to provide services and technologies to their citizens while also protecting their safety [24] and security [3]. This also includes monitoring daily operations and vital signs such as emergency response times, pollution risks or traffic control. Cyber resilience requires adequate risk management to identify and prioritise these elements as it covers such a wide specification. In the event of a cyber risk coming to fruition, there is a wide range of impacts that can occur that resilience measures and actions must be taken across regions and nations, including third-party managed network and cloud computing infrastructures.

4.2.1 Resist

The term "Resist" is a design feature or contingency practice in the case of a failure occurring. The objective is to ensure that any attack surface is minimised to provide resiliency and robustness. Contingencies will be made available to provide an alternative solution whilst incident management practice will manage communication and response. There are a variety of methods by which cyber resilience can be maintained and managed. Under "Resist" three high-level possibilities of actions are suggested:

1. **Fault Tolerance:** When creating adequate contingencies, it is important to first identify operations within the smart city where if operations were to become unavailable it would have a higher or critical impact.

- **Infrastructure Redundancy:** Infrastructure redundancy for critical networks components is vital for a Smart City being operational 24x7. However, having the additional capacity for resilience comes at a cost.
- **Data backups and recovery**: To minimise the risk of data being lost, it is essential that the data is stored in several locations, and with at least one off-site copy. This provides a backup service to ensure the maintenance of the running of the infrastructure. This may also include a workaround where an alternative device is used for a temporary period to maintain the process.

2. **Safety and Security in Design**:
Devices and systems should be embedded with alternative contingencies in place. If a device becomes unavailable due to a technological fault or planned maintenance where it needs to be out of action, the contingency method can support this service for a temporary period.

3. **Assess–Practice-Adjust**: Ensuring resilience in a Smart City requires constant preparedness should any kind of scenario occur. This should include simulated outages, stress testing and penetration testing of the infrastructure. Practising these scenarios can improve the business processes which are already in place based on the outcome of these scenarios. The Assess-Practice-Adjust cycle must occur frequently within Smart City operations.

4.3 Domain 3: Data Protection and Data Privacy

A sound understanding of data privacy and the impacts of materialising risks are critical [25]. An enormous amount of data is collected and analysed daily by using data mining and statistical methods. These methods may result in limited data security, leading to potential disclosure of personal and sensitive data which could have an extremely detrimental impact.

Due to the constant learning and understanding around what privacy is, it has historically been extremely difficult to define the term privacy, especially since privacy definitions have been reflections on contemporary contexts. In 1967 a definition was released by the International Commission of Jurists in Stockholm, which captures the importance of privacy: "*The right to privacy is the right to be left alone to live one's own life with the minimum degree of interference*" [26]. Previous to that the Universal Declaration of Human Rights released earlier in 1948: "*No one shall be subjected to arbitrary interference with his privacy, family, home, or correspondence*" [27]. One of the main concerns contemporarily is around the subject of big data and privacy. When obtaining the materials required for collation and analysis, the risk of privacy is always a concern as care must be taken to ensure the appropriate level of data anonymisation is used. However, it is extremely difficult to maintain anonymity [28] whilst collating large quantities of data which can potentially result in correlations in the data allowing the users to be uniquely fingerprinted.

4.3.1 Fair Information Practice Principles

In 1974, the US Congress approved the Fair Information Practice Principles Act. This discusses how data is collected and that there must be a rationale as to why it is needed. It covers the importance of transparency and giving notice to people on when, and why, the data is being collected. These principles may be relating to now out of date reports, but cover the fundamentals of national privacy laws and policies in various countries:

- General Data Protection Regulation (GDPR) – European Union
- Personal Information Protection and Electronic Documents (PIPEDA) – Canada
- Californian Consumer Privacy Act (CCPA) – United States
- OECD Privacy Guidelines (The Organisation for Economic Co-operation and Development – International standard

In the taxonomy of privacy, privacy could be jeopardized and breached in many different ways [29]. The below four domains were further split into subcategories:

- Information collection: surveillance, interrogation, recording, monitoring people's conversations and activities
- Information processing: processing information that was collected without the subject's consent. Not being transparent on what the data held on the subject is or providing the opportunity to correct this if the data is inaccurate.
- Information dissemination: breach of confidentiality, disclosure, increased accessibility, blackmail, appropriation, distortion
- Invasion: intrusion, decisional interference

It is important to understand what data can be exposed voluntarily and the impact this then has on its protection. People have different boundaries on what data they wish to protect. Social Media is a huge example of this, some people regularly post their activities where profiles on people can be developed on their routines, hobbies and interests. Others feel the need to post little, or not at all, and are extremely cautious on what they allow to be made public.

The overall problem with big data is that its content cannot be wholly erased. Just as libraries used to keep old books in printed format, the Wayback Machine (https://archive.org/) is something like a search engine that archives pages on the web. This data is intended to be retained forever as webpages themselves are ephemeral. This means if there is something stored here that someone legitimately no longer wishes to be available to the public under the EU's GDPR laws, failure to remove it can be interpreted as a privacy violation. Copies from the Wayback Machine can also be made in an uncontrolled fashion, meaning that there is no way of knowing how many copies of this data are stored, or where. Depending on the content of the data it could have severe consequences to somebody's wellbeing, and the location of that data is important to its removal. There is no compulsion to remove data for example stored outside the EU GDPR area in response to a requirement – so it may exist perpetually. As a compromise to make data extremely hard to find, people work with intermediaries such as search engines which are often the portal to this data. If the results in the search engines are masked, then this makes it extremely difficult for the data to be obtained from the main search engines in a territory-bound manner.

4.3.2 Breach of Privacy

The historical influence and development of technology privacy laws show a continuous focus on privacy concerns. The law has often failed to keep up to speed with technological development, which is why broad principles like FIPPs are important. When there has been a development of an innovative new product, such as the smartphone, where all security and privacy concerns are taken into account before launch? If inventors launch a product or service today and have not taken into account the in-depth privacy laws, who will be held accountable and potentially face significant fines and in some cases prison sentences, should privacy of the consumer be breached? Trivial examples of data breaches could be from leaving a laptop on the train, dropping a smartphone in a bar or clicking on a suspicious "phishing email" which results in the user entering data into a fake or hacked website.

When it comes to a personal data breach, not only is it that the data has been accessed that is the concern, but also what is done with that data. Ransomware is one example, where the threat to publish or pass on a victim's data can be used. If a data breach incurs this data can be sold, corrupted, deleted, lost or destroyed. These can have serious and devastating impacts on businesses but most affected individuals. If a security breach occurs, the type of breach must be identified promptly. If it has turned into a material personal data breach, some actions are required to be taken to monitor, control and report this. In the UK the Information Commissioner's Office (ICO) may need to be informed as part of this process. If a company fails to adhere to the personal data breach reporting and monitoring processes, it could be responsible for failing to protect customers from an ethical and practical point. Resulting in not managing data breaches effectively from a practical point of view can lead to significant government fines and potential lawsuits leading to prison sentences. When new technology is developed privacy must be always at the forefront during the development stages. In the same breath, it is also essential that companies are using the latest tools available and their technology is being maintained to an adequate level to prevent these devastating consequences.

4.3.3 The current approach to privacy breaches/harms

The European Union privacy laws are embodied within General Data Protection Regulation (GDPR). The US has a variety of privacy laws that are mainly "state-specific" with California perhaps being one of the strongest sets. Within both the US and EU individual personal rights, which include the generation, use and disclosure of personal data along with the responsibilities of the data controller are covered within the practical principles of FIPPs. There are many common factors between the US and EU when it comes to privacy harms and implementing privacy protection within the design of technology, with the differences mainly occurring in implementations, such as obtaining content and notification of breaches. EU legislation is standard across all domains and applies equally to all data controllers. The US however does not implement this transparency. In the US privacy laws and legislation are domain-specific. There are also differences in how privacy by design is promoted, how enhanced data security is implemented and how access rights and data consent is applied. Due to the differences in how legislation and policies are implemented, it can cause some confusion and result in increased compliance and regulatory risk. Smart city technologies are constantly challenging this legislation and policies with regards to privacy.

4.3.4 Smart city security concerns

When it comes to smart cities, there are two main security concerns:

1. Security of physical ICT prone to cyber attacks
2. Security of data at rest, in use and motion across the technologies and infrastructure

For a smart city to operate in the way it is intended, it utilises a complex build of groups of digital technology and ICT infrastructure. Due to the heavy reliance on software, there is always the risk of cyber-attacks and new vectors being discovered. Depending on how a device is networked can result in a variety of different entry points from where a hacker can launch a cyber-attack and attempt to alter, disrupt, destroy, deceive or degrade the systems and data.

Cyber-attacks fall under the below three forms focusing on the CIA triad namely Confidentiality, Integrity, Availability:

- **Confidentiality attacks:** This will look at data that is held on the device, how to extract the data and monitor activity to potentially obtain further confidential data (packet sniffing, password attacks, port scanning, phishing, social engineering)
- **Integrity attacks:** This will look to manipulate/change its information and settings; this could also involve installing malware and viruses [30] (Data diddling attacks, Man-in-the-middle attacks, Session hijacking attacks)
- **Availability attacks:** These focus on obtaining full control of the system to force them to be closed or restrict/decline service (DoS, DDoS, SYN flood/ICMP flood attacks, electrical power attacks)

For smart cities to mitigate the risk of the attacks such as the above, its overall security model needs to be comprehensive, later and in-depth, to be cyber resilient and explicitly incorporate the city's privacy and data protection responses.

4.3.5 Identifying data privacy and security risks within a smart city

There are a variety of different concerns linked to smart city technologies and data privacy. One aspect to review when assessing the risks is to look at the ethical consequences of mass surveillance (intended or a side-effect) that comes with smart city technology. This includes predictive profiling of habits and social sorting for example through the use of big data analysis [31]. There are often pros and cons relating to these points when implementing new technologies. If mass surveillance is used as an example, there is an argument that the surveillance is a breach of people's values and basic privacy rights. On the other hand, mass surveillance can be used to support businesses by monitoring footfall, product demand and trending behaviours, thus creating commercial opportunities and jobs through expansion and growth by reacting accurately to market needs [31].

There is no black and white when it comes to privacy. Through the constant innovations and new technologies implemented within smart cities that touch on our daily lives, it no longer becomes a question if an individual would like to remain completely anonymous and not disclose any personal information. It would now be extremely difficult to live an anonymous life, for example avoiding online purchases, using email, smartphones and online banking which are almost ubiquitous in the modern world. Privacy however is still protected by legislative and regulatory measures and remains a significant focus for many individuals. The aim is to ensure the development of new technology incorporates the implementation of proportionate and regulatory-defined data privacy and security measures. There is no one definitive answer or implementation. A suite of controls needs to be reviewed and implemented to ensure that risk is mitigated or controlled. These controls focus on a range of aspects such as regulatory and legal requirements, technical security, and data storage to name a few. Risks and controls will always need to be regularly reviewed as new technology brings new opportunity and risk, and a cyber-attacker can discover new methods to target a network to penetrate or compromise it.

Moreover, ethical concerns play a large role in smart privacy, for example how mass surveillance is managed. Mass surveillance, such as CCTV has a range of advantages and disadvantages, for example, it can be considered extremely useful in protecting the public if a crime has taken place to understand what happened and assist in identifying the suspect and stop it from happening again. Another positive factor would be promoting business growth and reaching out to a target audience by monitoring trending behaviour linked to certain products, which in turn supports business expansion and the economy by providing job opportunities. An argument against mass surveillance is that individuals may not always be able to consent to personal data being held on them and they are uncomfortable with how the data is being managed and used beyond their explicit permission. To live in the modern world, the general use of email, social media and online shopping all fall under the mass surveillance category – under general terms and conditions - therefore it is extremely difficult for an individual to take control. It is therefore essential that data privacy regulations and security measures are considered when implementing smart technologies. A suite of controls is used to ensure regulatory and legal requirements are adhered to and are required to be reviewed regularly to identify any new risks that could potentially arise.

Another issue with this is the understanding of terms and conditions. Because they are often not fully understood and can be extremely complex, people cannot always act in their own best interests when it comes to protecting their data and privacy. A second market solution is companies promoting the advantages of consumer privacy and data security and developing this into their technologies to attract consumers and develop consumer loyalty. This approach as it is unable to garner revenue from behavioural tracking characteristics is likely to be offered with a fee and will ensure that privacy and security settings within the technologies used are regularly enhanced to ensure optimum protection for customers. It will also allow individuals to control and manage their privacy granularly along with supporting companies and public authorities to enhance the protection of operational security, data resources and customer privacy.

Privacy Enhancing Technologies (PET), as defined by the European Commission, are also used, which support the protection of Personally Identifiable Information (PII) and controls how PII should be managed by “different services”. PETs help protect PII on websites and smart devices, they are also embodied in ad blockers, cookie blockers and removers. Smart cities, also manage data that is handled by data brokers, this data can be obtained by surveillance devices and card readers as an example. Other alternatives to PETs intended to protect confidentiality are private information retrieval (PIR), statistical disclosure control (SDC) and privacy-preserving data mining (PPDM).

4.3.6 Policies, regulations and legalities

Regulatory and legal requirements need to be under constant review to keep up with the constant technological development. When it comes to “urban big data” privacy and security concerns need to be thoroughly addressed. The policy, regulatory and legal landscape needs to be revised not only within smart cities but also at a national level through active revision to ensure it remains fit-for-purpose.

4.3.7 Fair information practice principles (FIPPs)

FIPPs clarifies the main principles when it comes to data use, handling and storage along with the responsibilities of the data controllers. When FIPPs is put into practice there are some significant difficulties. Due to the importance of FIPPs and growing concern of data use and abuse, it has become apparent these controls are essential, and thus many countries have published their revised sets of FIPPs. In the US it was via the Consumer Privacy Bill of Rights in the EU - the General Data Protection Regulation (GDPR).
It is argued that there are gaps in FIPPs, one example is that there is still a huge risk on how data can be shared and manipulated which is not always explicitly called out and if it is not explicitly prohibited will be exploited.

4.3.8 Privacy by design (PbD)

FIPPs would play an important role in supporting the development of smart cities through the adoption of privacy by design. As introduced and expanded by Ann Cavoukian, the key principle linked to Privacy by Design (PbD) is that privacy is the automatic blanket mode of operation. Therefore unless an individual specifically agrees to data being made available or used, it will automatically be processed and stored as private. Privacy is embedded into key principles which allow for different modes of implementation.

This solution is extremely advantageous to the individual and their control, positioned as positive-sum rather than zero-sum where the aim is to maximise privacy rights and security rather than having to look at compromising these by relying on trade-offs.

4.3.9 Security by design (SbD)

Security by design works alongside privacy by design. Risk assessments are completed and revisited in the early stages of a product launch to act as a preventative measure in providing security protection. This process includes in-depth testing and pilot testing within a laboratory environment to ensure security measures are effective and comprehensive before a product is fully launched. Cybersecurity plays a major role in the whole process and the product needs to be monitored throughout its lifespan to ensure cybersecurity measures remain effective with necessary action taken if a fix is required or if a data subject needs to be made aware of a potential breach or risk [32]. Security by design encourages users to also take preventative measures, such as using strong access controls, password management and end to end encryption.

4.3.10 Protect

Due to the nature of smart cities, there must be robust privacy and data controls in place as the risks are much higher due to the level and quantity of data held. Record retention policies should be followed to ensure the retention periods of data are fair, only data required to be held is obtained and the use and processing of data are transparent. To ensure data security is practised, cities have privacy and data protection principles in place front and centre. To help implement these principles, the following are three basic key principles that should be applied and followed in smart cities:

1. **Issue a Privacy and Data Protection Charter**: This charter will encompass guidelines on implementing privacy by design (PbD) and privacy by default when developing smart city devices. This will not only mitigate risks on security crimes but will also provide the public with the confidence that data management is secure.
2. **Promote Transparency and appoint a Data Privacy Officer**: This will ensure someone is responsible for incident management and risk oversight within data protection and privacy. Transparency will be a priority, as regular reporting will be issued to show the strengths and weaknesses within the smart city and any breaches that need to be raised. This person will ensure devices and individuals are compliant with policy and regulations and spread awareness on best practices and be responsible for them.
3. **Establish Data Governance Contracts with Third Parties**: Third parties need evidence that they are compliant with privacy and data protection regulations. If the third party provides a service where they are managing individuals' data, not only do they need to be compliant with regulations, but contracts need to be in place to ensure clarity on who owns the data and who is responsible for incident management should a breach be incurred.

4.4 Domain 4: Governance

Companies could potentially not take into consideration what the key priorities, needs and interests are of the city and its residents and act solely in the interest of the company [18]. Due to the smart technologies being in such an early stage, cities need to be cautious in the long-term investments that are made. Smart City officials must monitor developments and intervene when necessary for both private and public interests. Governance in this field encompasses two complex factors:

- **Cultural Diversity and Disparate Visions:** Residents within a city consist of a range of different cultures and principles. Not every individual and business will have the same objective, therefore, collaboration across a range of governmental, business, residential and other stakeholders is essential in understanding the needs of the city and how this will fit into the smart city objectives.
- **Fluid Boundaries and Limited Authorities:** Due to the nature of technologies within a smart city, the political and organisational boundaries are ever-changing over time. Having someone responsible for this risk management can be challenging to achieve in itself.

4.4.1 Training and awareness

When developing smart cities there is an essential requirement for education and development of training policies. Whereas FIPPs, privacy-by-design and security-by-design deliver practical results, they would not be utilised to their full potential without supporting users' understanding of the technology. Users should also be provided with guidance on how they are impacted by systems and how to use them, whilst demonstrating protection for their privacy and security. To support this area, four types of national education and training programmes are highly encouraged:

- General Education Programme: this target audience is the general public. It provides an overall understanding of how to protect against privacy and security threats and the steps required to take to ensure this is put physically into practice. It also covers the technologies embedded within a smart city and the privacy and security risks threats that are linked
- School Children Education Programme: This focuses on educating school children on data privacy and how data is generated on them. This can include avenues such as social media usage and understanding the risks of what personal data is made available.
- Local Authority Education Programme: This focuses on the education for local authority staff and what their responsibility is when it comes to data protection and how to assess and mitigate privacy and security risks
- Technology Companies Education Programme: This mainly focuses on SMEs and new businesses that may not have the education programmes that a large established company would typically have. This provides opportunities for these businesses to understand what best practices to implement and what their responsibilities are to the public and customers.

4.4.2 The governance framework and management support

Governance provides a framework where decisions can be made, and a strategic direction is set and agreed upon. Governance also includes the practical implementation and monitoring of regulations. Management provides the driving force to achieve the goals in implementing and running the necessary services. Both these aspects complement and support the set-up and maintenance of technologies and systems while adhering to legal and regulatory requirements.

Today it is predominantly found that smart cities have been developed with minimal support in this area, resulting in clear gaps in privacy and security management. To gain the trust of the users and facilitate faster adoption of smart city technologies this approach must be replaced with a more organised one to maintain direction and achieve strategic objectives. Oversight and compliance require incorporation into existing (and future) practical deployments, managing governance and day-to-day delivery with an emergency response team to hand to provide that trust for citizens. Putting these factors in place will hugely improve a smart city's potential, promote key learning to support future sustainable development.

4.4.3 Smart City Cyber Incident Response Teams (SC CIRTs)

Smart City Cyber Incident Response Teams (SC CIRTs) play a critical role in incident management, mainly managing cybersecurity incidents such as hacking, data theft, system disruption or termination. They are a team of key individuals that manage incident response and security. Due to the nature of their job, they have a range of planned scenarios with planned responses to effectively deal with and manage an incident to best practice. The scenarios are revised regularly to ensure they remain current and effective and also highlight any new risks that need to be planned for.

4.4.4 Comply and Manage

Some key principles support comprehensive cooperation and coordination in governance within a smart city. These are:

- **Accountability**: Due to the complex nature of smart cities, it must be clear where accountability lies, for example in the storage of data, incident management, education and risk assessments.
- **Collaboration**: To successfully develop and maintain a smart city it is key for experts in different areas to collaborate or utilise collaborative models [33] powered by technology to identify and manage risks and create mitigating controls. Residents within the smart city should also have involvement as its important concerns are addressed, and everyone's needs and best interests are understood.

- **Leadership responsibility:** It is a requirement to have a clear leadership structure that has responsibility for the city's security and resiliency. The elected officials are to understand the needs of their residents while also being aware of privacy and security risks.
- **Trust and Transparency:** To create trust within a city between residents, businesses and local authorities, transparency is key. Not only do residents have a right to be able to see relevant data but it also raises awareness on cybersecurity issues and best practices going forward.

From these principles, the following recommendations can be actioned led by the advisory board:
1. **Coordinate Forums and Promote Collaboration:** By installing regular forums to raise concerns, share best practices and share information promotes collaboration with a range of expertise and across different perspectives to achieve the best outcomes.
2. **Organise Roadshows:** Leadership needs to organise roadshows or roundtable events to raise topics and debate and resolve issues around the smart city. Early engagement within communities and throughout will ensure that smart technologies do not worsen existing discriminations and inequalities.
3. Provide Transparent and Frequent Communication: By communicating key messages, recent changes, decision making, and concerns will build trust within the community through its transparency.

5 On The Development and Creation of a Secure and Resilient Smart City

During the early stages of smart city planning and development, it must be a priority to implement security and resilience. A roadmap should be developed by smart city managers in these early stages. Regarding the CyberSmart CRPG Framework, "Connect", "Resist", "Protect" and "Comply and Manage" should be aspects of consideration when building the roadmap.
It is a common error that security, privacy and resilience are not taken into consideration until it is too late. It is also a problem if such a matter is not strategically planned for by the city's senior management board. Figure 10 illustrates an example for such a roadmap with three clear functions;

- Provides a starting point: this ensures individuals understand what the current state of play is and supports to process of achieving an end goal.
- Engagement Awareness: This supports the collaboration of key stakeholders' input by creating an avenue to share ideas, raise key issues and identify solutions.
- Environmental Factors: This is where internal and external factors come into consideration, such as changes to laws and regulations, technology developments and changes to consumer needs.

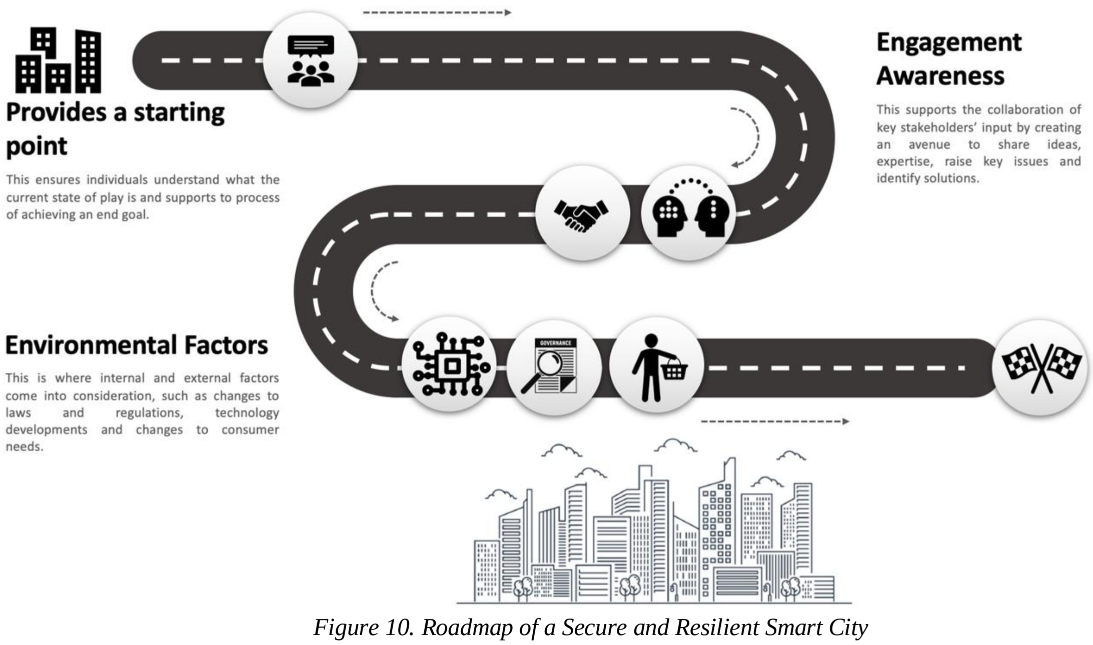

Provides a starting point
This ensures individuals understand what the current state of play is and supports to process of achieving an end goal.
Engagement Awareness
This supports the collaboration of key stakeholders' input by creating an avenue to share ideas, expertise, raise key issues and identify solutions.
Environmental Factors
This is where internal and external factors come into consideration, such as changes to laws and regulations, technology developments and changes to consumer needs.
GOVERNANCE

Figure 10. Roadmap of a Secure and Resilient Smart City

Each city is unique, consisting of different sizes, cultures, style of governance, priorities and needs. However, even though there are varying elements within a smart city, a roadmap should still follow a set of key elements [18]:

1. **Create Smart City Objectives:** This element focuses on what the overall vision is for the city, what are the reasons for becoming a smart city and what are the key impacts this will have.
2. **Create a Strong Governance Structure:** Ensure security and resilience issues are handled with a collaborative approach to achieve the best possible outcomes. Governance should provide transparency to members on key issues and actions.
3. **Complete Security and Resiliency Reviews:** Create adequate security, resilience and data protection policies. Understand what gaps exist within the city and develop controls to close these gaps. Provide education to the public on security awareness.
4. **Effective Risk Assessment Completion:** By completing risk assessments on each of the smart city's domains allows for adequate contingencies to be implemented should the main technologies or devices become unavailable. During the risk assessment process, a full impact assessment should be completed to understand the impacts, whether these are financial, reputational or policy-related and how best to prevent or minimise them.
5. **Identify Critical Areas and Develop Supporting Processes:** Complete a review of the cities critical areas and understand what processes or third parties support this. This ensures high-quality data which is especially important for example, in the event of system failure the impacts and required stakeholders are ready to hand.
6. **Stakeholder Collaboration:** Ensure a range where key stakeholders have identified that offer different areas of expertise to build the best smart city possible.
7. **Technology Investments:** To build a robust smart city, money must be invested into technologies and devices. Detailed risk assessments should be completed on the implementation of different systems to understand the benefits and risks to make an informed decision.

6 Conclusion

Smart cities have real value to offer, however, there are also serious risks that can impact privacy and therefore the safety of its citizens. Taking a proactive approach to developing and maintaining a smart city will ensure that the full benefits are appropriately utilised, and adequate risk management is built in. In this study, several challenges have been defined and discussed such as operational risk management within smart cities, management structure and key stakeholders complexity, and lack of confidence and trust in new devices and technology. Therefore, a CRPG framework have been proposed and discussed to analyse and map risk to mitigation activities with a particular focus on data protection and data privacy,

Furthermore, as cities vary, needs and wants can vary enormously, therefore, when developing a smart city, collaboration should be facilitated through appropriate frameworks to acknowledge the size, sectors, cultures, history, and economic strength across a diverse steering group. Having clear objectives in place on what improvements are a priority, provides focus on the main reasons to build the smart city. For example, if there is a growing concern for the environment, clear objectives around this need to be established, and strong monitoring and performance tracking put in place. Likewise, educational needs must be planned for the public to raise awareness and ensure participation. The more buy-in that is received from the public, the faster benefits can be realised, and the next steps put in place to benefit all across the longer-term vision.

Following the outcomes of this study, we also wanted to shed light on the emerging concept of Digital Twins [5], a cutting-edge technology that we expect will act as a guide in effectively planning for the future. These technological advances support a city to provide enhanced services, recourses and improve assets. This promotes a better quality of life and provides opportunities for growth and development securely. By embedding digital twins within a smart city framework, we anticipate improved responses to disasters and emergencies.

References

[1] C. Coletta, and R. Kitchin, "Algorhythmic governance: Regulating the 'heartbeat' of a city using the Internet of Things," *Big Data & Society*, vol. 4, no. 2, pp. 2053951717742418, 2017. https://doi.org/10.1177/2053951717742418

[2] G. Ahmadi-Assalemi, H. M. al-Khateeb, C. Maple, G. Epiphaniou, M. Hammoudeh, H. Jahankhani, and P. Pillai, “Optimising driver profiling through behaviour modelling of in-car sensor and global positioning system data,” *Computers & Electrical Engineering*, vol. 91, pp. 107047, 2021/05/01/, 2021. https://doi.org/10.1016/j.compeleceng.2021.107047

[3] G. Ahmadi-Assalemi, H. Al-Khateeb, G. Epiphaniou, and C. Maple, “Cyber Resilience and Incident Response in Smart Cities: A Systematic Literature Review,” *Smart Cities*, vol. 3, no. 3, pp. 894-927, 2020. https://doi.org/10.3390/smartcities3030046

[4] S. Albishi, B. Soh, A. Ullah, and F. Algarni, “Challenges and Solutions for Applications and Technologies in the Internet of Things,” *Procedia Computer Science*, vol. 124, pp. 608-614, 2017/01/01/, 2017. https://doi.org/10.1016/j.procs.2017.12.196

[5] G. Ahmadi-Assalemi, H. Al-Khateeb, C. Maple, G. Epiphaniou, Z. A. Alhaboby, S. Alkaabi, and D. Alhaboby, "Digital Twins for Precision Healthcare," *Cyber Defence in the Age of AI, Smart Societies and Augmented Humanity*, H. Jahankhani, S. Kendzierskyj, N. Chelvachandran and J. Ibarra, eds., Springer International Publishing, 2020, pp. 133-158. https://doi.org/10.1007/978-3-030-35746-7_8

[6] A. Lisdorf, *Demystifying Smart Cities: Practical Perspectives on How Cities Can Leverage the Potential of New Technologies*: Springer, 2019. https://doi.org/10.1007/978-1-4842-5377-9

[7] V. Chang, S. Sharma, and C.-S. Li, “Smart cities in the 21st century,” *Technological Forecasting and Social Change*, vol. 153, pp. 119447, 2020/04/01/, 2020. https://doi.org/10.1016/j.techfore.2018.09.002

[8] T. V. Kumar, "Smart Environment for Smart Cities," *Smart Environment for Smart Cities*, pp. 1-53: Springer, 2020. https://doi.org/10.1007/978-981-13-6822-6

[9] A. Caragliu, C. Del Bo, and P. Nijkamp, “Smart Cities in Europe,” *Journal of Urban Technology*, vol. 18, no. 2, pp. 65-82, 2011/04/01, 2011. https://doi.org/10.1080/10630732.2011.601117

[10] D. Sikora-Fernandez, and D. Stawasz, “THE CONCEPT OF SMART CITY IN THE THEORY AND PRACTICE OF URBAN DEVELOPMENT MANAGEMENT,” *Romanian Journal of Regional Science*, vol. 10, no. 1, pp. 86-99, 2016.

[11] F. Al-Turjman, “The road towards plant phenotyping via WSNs: An overview,” *Computers and Electronics in Agriculture*, vol. 161, pp. 4-13, 2019/06/01/, 2019. https://doi.org/10.1016/j.compag.2018.09.018

[12] F. Al-Turjman, and J. P. Lemayian, “Intelligence, security, and vehicular sensor networks in internet of things (IoT)-enabled smart-cities: An overview,” *Computers & Electrical Engineering*, vol. 87, pp. 106776, 2020/10/01/, 2020. https://doi.org/10.1016/j.compeleceng.2020.106776

[13] I. Dincer, and C. Acar, “Smart energy systems for a sustainable future,” *Applied Energy*, vol. 194, pp. 225-235, 2017/05/15/, 2017. https://doi.org/10.1016/j.apenergy.2016.12.058

[14] T. Robles, R. Alcarria, D. Martín, A. Morales, M. Navarro, R. Calero, S. Iglesias, and M. López, "An Internet of Things-Based Model for Smart Water Management." pp. 821-826. https://doi.org/10.1109/WAINA.2014.129

[15] D. Snellen, and G. de Hollander, “ICT'S change transport and mobility: mind the policy gap!,” *Transportation Research Procedia*, vol. 26, pp. 3-12, 2017/01/01/, 2017. https://doi.org/10.1016/j.trpro.2017.07.003

[16] H. Jahankhani, S. Kendzierskyj, A. Jamal, G. Epiphaniou, and H. Al-Khateeb, *Blockchain and Clinical Trial: Securing Patient Data*: Springer, 2019. https://doi.org/10.1007/978-3-030-11289-9

[17] A. Dehghantanha, and K.-K. R. Choo, *Handbook of big data and IoT security*: Springer, 2019. https://doi.org/10.1007/978-3-030-10543-3

[18] EastWest Institute, *Smart and Safe - Risk Reduction in Tomorrow's Cities*, 2018. https://www.eastwest.ngo/sites/default/files/ideas-files/ewi-smart-and-safe-cities.pdf

[19] E. Ismagilova, L. Hughes, N. P. Rana, and Y. K. Dwivedi, "Security, Privacy and Risks Within Smart Cities: Literature Review and Development of a Smart City Interaction Framework," *Information Systems Frontiers*, 2020/07/21, 2020. https://doi.org/10.1007/s10796-020-10044-1

[20] R. Kitchin, and M. Dodge, "The (In)Security of Smart Cities: Vulnerabilities, Risks, Mitigation, and Prevention," *Journal of Urban Technology*, vol. 26, no. 2, pp. 47-65, 2019/04/03, 2019. https://doi.org/10.1080/10630732.2017.1408002

[21] G. Ahmadi-Assalemi, H. M. al-Khateeb, G. Epiphaniou, J. Cosson, H. Jahankhani, and P. Pillai, "Federated Blockchain-Based Tracking and Liability Attribution Framework for Employees and Cyber-Physical Objects in a Smart Workplace." pp. 1-9. https://doi.org/10.1109/ICGS3.2019.8688297

[22] L. Cui, G. Xie, Y. Qu, L. Gao, and Y. Yang, "Security and Privacy in Smart Cities: Challenges and Opportunities," *IEEE Access*, vol. 6, pp. 46134-46145, 2018. https://doi.org/10.1109/ACCESS.2018.2853985

[23] R. O. Andrade, S. G. Yoo, L. Tello-Oquendo, and I. Ortiz-Garcés, "Chapter 12 - Cybersecurity, sustainability, and resilience capabilities of a smart city," *Smart Cities and the un SDGs*, A. Visvizi and R. Pérez del Hoyo, eds., pp. 181-193: Elsevier, 2021. https://doi.org/10.1016/B978-0-323-85151-0.00012-9

[24] N. Ersotelos, M. Bottarelli, H. Al-Khateeb, G. Epiphaniou, Z. Alhaboby, P. Pillai, and A. Aggoun, "Blockchain and IoMT against Physical Abuse: Bullying in Schools as a Case Study," *Journal of Sensor and Actuator Networks*, vol. 10, no. 1, pp. 1, 2021. https://doi.org/10.3390/jsan10010001

[25] V. Torra, *Data privacy: Foundations, new developments and the big data challenge*: Springer, 2017.

[26] International Commission of Jurists, "The right to privacy: working paper, Stockholm, Sweden, May 22-23," 1967. https://www.icj.org/nordic-conference-of-jurists-the-right-to-privacy-working-paper-stockholm-sweden-may-22-23-1967/

[27] United Nations, "Universal Declaration of Human Rights," 2015. https://www.un.org/en/universal-declaration-human-rights/

[28] H. Haughey, G. Epiphaniou, and H. M. al-Khateeb, "Anonymity networks and the fragile cyber ecosystem," *Network Security*, vol. 2016, no. 3, pp. 10-18, 2016. https://doi.org/10.1016/S1353-4858(16)30028-9

[29] D. J. Solove, "A Taxonomy of Privacy," *University of Pennsylvania Law Review*, vol. 154, no. 3, pp. 477-564, 2005-2006, 2005.

[30] M. Irshad, H. M. Al-Khateeb, A. Mansour, M. Ashawa, and M. Hamisu, "Effective methods to detect metamorphic malware: a systematic review," *International Journal of Electronic Security and Digital Forensics*, vol. 10, no. 2, pp. 138-154, 2018. https://doi.org/10.1504/ijesdf.2018.090948

[31] J. W. Woensdregt, H. M. Al-Khateeb, G. Epiphaniou, and H. Jahankhani, "AdPExT: Designing a Tool to Assess Information Gleaned from Browsers by Online Advertising Platforms." pp. 204-212. https://doi.org/10.1109/ICGS3.2019.8688328

[32] E. Haber, and A. Tamò-Larrieux, "Privacy and security by design: Comparing the EU and Israeli approaches to embedding privacy and security," *Computer Law & Security Review*, vol. 37, pp. 105409, 2020/07/01/, 2020. https://doi.org/10.1016/j.clsr.2020.105409

[33] Y. Al-Husaini, H. Al-Khateeb, M. Warren, L. Pan, and G. Epiphaniou, "Collaborative Digital Forensic Investigations Model for Law Enforcement: Oman as a Case Study," *Security and Organization within IoT and Smart Cities*, pp. 157-180: CRC Press, 2020. http://dx.doi.org/10.1201/9781003018636-9