Information Security Management for Cyber Security Challenges in Smart Cities Security and Privacy

إدارة أمن المعلومات لتحديات الأمن السيبراني في أمن وخصوصية المدن الذكية

by

AZZAM OTHMAN

**A dissertation submitted in partial fulfilment
of the requirements for the degree of**

MSc INFORMATION TECHNOLOGY MANAGEMENT

**at
The British University in Dubai**

April 2022

DECLARATION

I warrant that the content of this research is the direct result of my own work and that any use made in it of published or unpublished copyright material falls within the limits permitted by international copyright conventions.

I understand that a copy of my research will be deposited in the University Library for permanent retention.

I hereby agree that the material mentioned above for which I am author and copyright holder may be copied and distributed by The British University in Dubai for the purposes of research, private study or education and that The British University in Dubai may recover from purchasers the costs incurred in such copying and distribution, where appropriate.

I understand that The British University in Dubai may make a digital copy available in the institutional repository.

I understand that I may apply to the University to retain the right to withhold or to restrict access to my thesis for a period which shall not normally exceed four calendar years from the congregation at which the degree is conferred, the length of the period to be specified in the application, together with the precise reasons for making that application.

Signature of the student

COPYRIGHT AND INFORMATION TO USERS

ABSTRACT

Information security management universally needed and has become popular in our digital world. A growing proportion of human activities, such as social interactions, entertainment, shopping, and gathering information, are now mediated by digital services and devices that are needed to be protected 24/7 based on the information security triangle Confidentiality, Integrity, and Availability. Currently, there are more than 12.3 billion IoT devices connected to our digital world recording everything around us such as street cameras, smart security devices, smart refrigerators, smart watches, etc. These devices collect most of our daily time information as our health by smart watches, refrigerator needs, air condition status, GPS information, and so on. Much of our daily life activities and privacy collected by these digital devices connected to the Internet. The main objective of this research is to answer the question whether information security management can protect our daily life and privacy information to be able to live in safe life in our smart cities or not. The findings of this study suggest that lack of in-house expertise, insufficient funding, difficulty in locating right security talent, poor leadership and lack of accountability are the top cyber-security challenges. In addition, it was found that organizations are mediocrely prepared to detect, prevent and respond to cyber-threats. Furthermore, it was revealed that individuals have mediocre level of security awareness.

ملخص الدراسة

إدارة أمن المعلومات مطلوبة عالمياً وأصبحت شائعة في عالمنا الرقمي. يتم الآن التوسط في نسبة متزايدة من الأنشطة البشرية ، مثل التفاعلات الاجتماعية والترفيه والتسوق وجمع المعلومات ، من خلال الخدمات والأجهزة الرقمية اللازمة للحماية على مدار الساعة طوال أيام الأسبوع استنادًا إلى مثلث أمن المعلومات ، السرية والنزاهة والتوافر. حالياً، هناك أكثر من 12.3 مليار جهاز إنترنت الأشياء متصل بعالمنا الرقمي يسجل كل شيء من حولنا مثل كاميرات الشوارع ، وأجهزة الأمن الذكية ، والثلاجات الذكية ، والساعات الذكية ، وما إلى ذلك. تجمع هذه الأجهزة معظم معلومات الوقت اليومية لدينا. الصحة من خلال الساعات الذكية واحتياجات الثلاجة وحالة تكييف الهواء ومعلومات GPS وما إلى ذلك. يتم جمع الكثير من أنشطتنا اليومية والخصوصية بواسطة هذه الأجهزة الرقمية المتصلة بالإنترنت. يتمثل جوهر هذا البحث في الإجابة على سؤال ما إذا كانت إدارة أمن المعلومات يمكن أن تحمي الحياة اليومية ومعلومات الخصوصية لتتمكن من العيش في حياة آمنة في مدننا الذكية أم لا. تشير نتائج هذه الدراسة إلى أن الافتقار إلى الخبرة الداخلية ، والتمويل غير الكافي ، وصعوبة تحديد المواهب الأمنية المناسبة ، وضعف القيادة ، وغياب المساءلة هي أهم تحديات الأمن السيبراني. بالإضافة إلى ذلك ، وجد أن المنظمات مستعدة بشكل متوسط لاكتشاف التهديدات السيبرانية ومنعها والاستجابة لها. علاوة على ذلك ، تم الكشف عن أن الأفراد لديهم مستوى متوسط من الوعي الأمني.

ACKNOWLEDGEMENT

In the name of Allah, the most gracious and the most merciful. Firstly, I am thankful to Almighty Allah for giving me the ability, knowledge, strength to undertake my learning journey at the British University In Dubai and reaching the final stage of it by accomplishing the presented study.

Secondly, the completion of this undertaking could not have been possible without the participation and assistance of so many people whose names may not all be enumerated. Their contributions are sincerely appreciated and gratefully acknowledged. To all relatives, friends and others who in one way or another shared their support, either morally, financially and physically, thank you.

Nonetheless, I would like to express my sincere gratitude to my supervisor Dr. Cornelius Ncube for his support during the process of preparing my dissertation. His guidance was of great help and pointed me to the correct direction whilst providing knowledge and experience to achieve the study in its final form.

TABLE OF CONTENTS

List of Figures

List of tables

List of abbreviations

IoT	- Internet of Things
SSL	- Secure Sockets Layer
TLS	- Transport Layer Security
SIEM	- Security Information and Event Management
IDS	- Intrusion Detection System
IPS	- Intrusion Prevention System
CIA	- Confidentiality, Integrity and Availability
CNSS	- Committee on National Security Systems
IT	- Information Technology
EISP	- Enterprise Information Security Policy
ISSP	- Issue-Specific Security Policies
SysP	- System-Specific Policies
SETA	- Security Education Training and Awareness
RFID	- Radio Frequency Identification
DoS	- Denial of Service
ICT	- Information and Communication Technologies
ITU	- International Telecommunication Union
DPA	- Data Protection Act
GDPR	- General Data Protection Regulation
USB	- Universal Serial Bus
APT	- Advanced Persistent Threats
AI	- Artificial Intelligence
UAE	- United Arab Emirates
DDOS	- Distributed Denial of Service
UK	- United Kingdom
CISSP	- Certified Information Systems Security Professional

HR	- Human Resources
SANS	- SysAdmin, Audit, Network and Security
CIS	- Center for Internet Security
MAC	- Media Access Control
RBAC	- Rule-Based Access Control
CISM	- Certified Information Security Manager
SCADA	- Supervisory Control And Data Acquisition
CPMTD	- Cyber-Physical Moving Target Defense
CIT	- Crisis Intervention Team
OBD	- On-Board Diagnostics
EDR	- Event Data Recorder
GPS	- Global Positioning satellite
BAS	- Building Automation Systems
UAV	- Unmanned Aerial Vehicle
AR	- Augmented reality
HVAC	- Heating, Ventilation, and Air Conditioning
PLC	- Programmable Logic Controllers
IEEE	- Institute of Electrical and Electronics Engineers
KNX	- Konnex
OSI	- Open System Interconnection
ISO	- International Organization for Standardization
VPN	- Virtual Private Network
AAA	- Authentication, Authorization, and Accounting
BMS	- Building Management System
IET	- Institution of Engineering and Technology
STOA	- Science & Technology Options Assessment
WBAN	- Wireless Body Area Networks

FAHP	- Fuzzy Analytical Hierarchy Process
GCC	- Gulf Cooperation Council
SPSS	- Statistical Package for the Social Sciences
XSS	- Cross-site scripting
BYOD	- bring your own device
BYOA	- bring your own apps
RADIUS	- Remote Authentication Dial-In User Service
ANSI	- American National Standards Institute
TIA	- Telecommunication Industry Association
ASHRAE	- American Society of Heating, Refrigerating and Air-Conditioning Engineer

CHAPTER 1: INTRODUCTION

1.1 Overview

Over the past few years, cybersecurity issues are haunting the news around the globe, issues such as massive hacking, ransomware, infecting computers containing sensitive data, credit card theft and personal data leakage are rising each and every day. Due to the increasing number of attacks, it has become difficult to grasp the scope of the problems and solutions. The complexity of the issue makes it hard for non-technical people to understand, but the omnipresence of various tools and technologies in various sectors of activity has raised concerns for everyone. Research aims to solve the problems and assist in making a more secure world in the future. With the current high rate in the world population increase, the demands and requirements are increasing proportionally. In a similar manner, the cities around the world are rapidly growing into mega cities, and cities that are currently occupied by more than 10 million residents are expected to reach 41 cities in 2030 (Mohamed et al. 2020). The complexity of governing such huge cities will increase correspondingly as the population increases, and providing higher quality living standards becomes challenging. A number of studies have investigated the matter of challenges in megacities and found out that environment, traffic, energy, water resources, waste management and scarcity of resources are the main challenges in megacities (Priester et al. 2013; Li et al. 2015; Kumar et al. 2015; Li et al. 2018). Those studies have proposed multiple suggestions to overcome such challenges, one eminent solution to the problem is transforming them into smart cities (Chourabi et al. 2012; Li et al. 2018; Kumar et al. 2020). Recent breakthroughs in telecommunication technologies have allowed more devices to connect to the internet and with higher speeds, internet of things (IoT) devices are now more affordable and more prevalent than ever, with 12.3 billion connected IoT devices (Lueth, 2022), in addition to improvements in cloud computing, smart grids and other elements. Such innovations are key components and could massively aid in moving toward implementing a smart city (Baig et al. 2017). Utilizing such technologies can lead to a better optimization of the city's resources, improve the citizens' welfare, provide a safer environment and improved energy efficiency. But at the same time, depending heavily on connected devices and IoT can expose the city to cyber-attacks, exposing the resident's and government's sensitive data, harming the infrastructure and reducing the safety of the city (Elmaghraby and Losavio, 2014; Belgaum et al. 2018; Hamid et al. 2019; Mohamed et al. 2020). It is worth noting that several cybersecurity measures and technologies are currently being employed, such as the utilization of transport-level encryption mechanisms such as SSL/TLS (Usmonov et al. 2017), in addition to conventional methods of data protection, including SIEM, IDS/ IPS, cryptographic information protection facility and antiviruses. However, multiple studies are suggesting that the use of the previous methods may not be very effective (Biryukov et al. 2015; Skatkov and Shevchenko, 2015; Gai et al. 2016). Therefore, the researchers are proposing several new methods, such as the use of big data technologies as its potential benefits for cybersecurity is the capability of identifying and detection primary and secondary indications of computer attacks and abnormal behaviors, as well as the classification of mass cyber-attacks that were previously unknown (Petrenko and Makoveichuk, 2017). The neglect of utilizing basic tools and approaches of data protection by developers have allowed several vulnerabilities to be exploited and taken advantage of by attackers of IoT devices. In addition, some manufacturers do not take into consideration the classification of the processed information at the design stage of the systems, which leads the developed devices to deal with confidential data in its most diverse forms such as personal data (Usmonov et al. 2017).

While the previously mentioned cybersecurity techniques and methods can be used to counter attack hackers, new and more complex cyber-attacks are constantly being developed (Mohamed et al. 2020).

Therefore, it is essential to investigate the shortcomings of the performance of the implemented information and cyber security management, and to what extent security layers and techniques protect the digital life of the residents of smart cities. In addition, the amount of cyber security knowledge of the individuals has to be examined to determine whether they have adequate cyber security knowledge to protect themselves.

1.1.1 Information security

The notion of information security has been discussed thoroughly in the literature, researchers have identified information security management, principles, practices, economics and the threats of information security in smart cities (Anderson and Moore, 2006; Whiteman and Mattord, 2011; stamp, 2011; Whitman and Mattord, 2013; Ijaz et al. 2016). Computer security, as a holistic point of view can be defined as the freedom of danger or undesirable actions such as malignant and accidental abuse, it is also a measure to what extent a system can resist penetration by users from the outside, as well as misuse by users from the inside (Neumann, 1994). Another definition by Stytz (2003) states that computer security seeks ensuring confidentiality, integrity and availability (CIA) for systems that perform computing tasks. However, Anderson (2003) argues that these definitions are so expansive that they unintentionally include activities that do not belong to information or computer security. Alternatively, he has proposed a definition that solves the problems with previous attempts in defining security. He defined information security as “A well-informed sense of assurance that information risks and controls are in balance” (Anderson, 2003, p. 310).

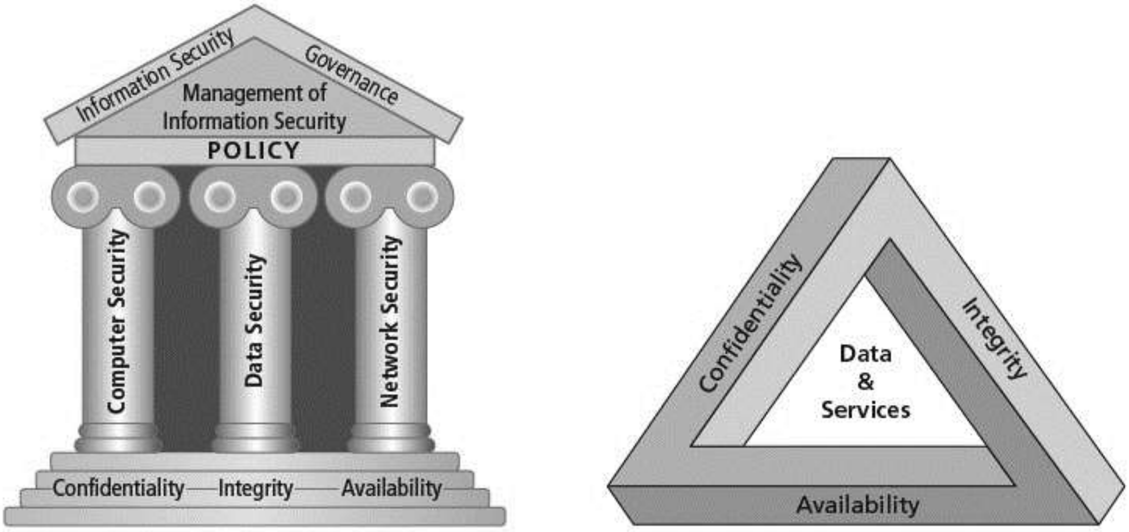


Figure 1: The components of information security and the C.I.A triad (Whiteman and Mattord, 2018, p. 11)

Figure 1 demonstrates the expansive areas that are included in information security as described by the committee on national security systems (CNSS). The model of Information by CNSS that contains computer security, data security and network security has emerged from a notion established by the industry of computer security named C.I.A, which is based on three features that provide its value to the corporations. These three features are confidentiality, integrity and availability, the significance of these characteristics has always been valid, however, Whiteman and Mattord (2018) argue that the C.I.A model is no longer sufficient in addressing the frequently varying information security environment. According to the authors, the threats to the C.I.A model has emerged into a plethora of events, including theft, intended or unintended damage, modifications that are unauthorized, destruction and other threats that are induced by human or non-human abuse.

1.1.1.1 Information security management

On the other hand, the management of information security refers to being in charge of a specific program that consists of functions known as "the six Ps", which are planning, policy, programs, protection, people and project management. As a feature of the management group, the information security management group works like any remaining management units by utilizing the normal qualities of initiative and managements. Notwithstanding, the InfoSec management groups objectives and goals contrast from those of the IT and general management networks in that the information security management group is centered on the protected activity of the association. Furthermore, a portion of the information security management group's objectives and targets might be in opposition to or require settlements with the objectives of the IT management group. The essential focal point of the IT team is to guarantee the powerful and proficient handling of data, while the essential focal point of the information security team is to guarantee that the system is up to the C.I.A model. The *planning* function of the information security management refers to the essential activities that underpin designing, creating and implementing information security strategies. The *Policy* Function implies the combination of guidelines that was set by the organization and decree specific activities. In the context of information security, policy is divided into three categories: Enterprise information security policy (EISP), Issue-specific security policies (ISSPs) and system-specific policies (SysPs). The *programs* function refers to the information security operations that are precisely administrated as distinct entities, such as the security education training and awareness (SETA) program, which provides the employees with critical information to maintain and/or enhance their knowledge in security. *Protection* function is implemented through a group of management actions, such as protection mechanisms and risk assessment and control. The *People* function is considered to be the most essential link in the program of information security, this function involves security staff and the security of the staff. Finally, the *projects* function refers to the implementation of project management principles to all components of the information security program (Whitman and Mattord, 2013).

1.1.1.2 Information security principles

Whiteman and Mattord (2018) have defined seven key principles of information security; namely:

- Confidentiality
- Integrity
- Availability
- Authentication and identification,
- Authorization
- Accountability
- Privacy

Confidentiality makes certain that the users who need to access information are only those with the right privileges are able to do so, the confidentiality of information means that it is protected from exposure to unauthorized entities. The integrity of the information means that it is complete, uncorrupted and complete. It becomes vulnerable if it damaged, destroyed or corrupted. Availability implies that authorized users are allowed to access information without interference, and to collect the information in the requested format. Authenticity refers to state of the data being original and untampered with, the information is considered authentic only when it is in same condition when it was placed, created, transferred or stored.

1.1.1.3 Information security economics

The discipline of information security economics has become prosperous in the past few years. As people have perceived that the shortcomings in security systems is due to bad incentives as much as it because of bad designs, system failures are more likely to happen when the user that is supposed to protect it is not the user that suffers when it actually fails. Furthermore, the increasing utilization of security techniques and mechanisms that enables a power user rather than excluding individuals that are not supposed to be users in the first place, have introduced many policy and strategic concerns (Anderson and Moore, 2006). There has been an increasing spending priority toward information security among companies, this increment in spending is due to the fact that companies are purchasing software to identify viruses and malware, complicated encryption mechanisms, firewalls, hardware and automatic data backup solutions (Larsen, 1999). A study by power (2001) has revealed that losses due to security attacks and breaches averaged over $2 million per firm, which may indicate the reason behind the increasing priority in information security spending. Studies in the field of information security economics have found out that for a particular potential loss, an organization is not essentially required to prioritize investing on data with highest vulnerability, since data with extreme vulnerability could be excessively costly to protect. Rather, a better strategy for such organization is to focus its investments on data sets with medium vulnerability (Gordon and Loeb, 2002).

1.1.1.4 Threats of information security in smart cities

A smart city is established by combining multiple elements, and incorporate the status of various infrastructures, governance, residents' health and education and management via information and communication technologies (ICT). Consequently, ICTs operate by utilizing and integrating innovative technologies that consists of electronics, sensors and networks, all of which rely heavily on internet connection to operate (Hall et al. 2000). Thus, a smart city is certainly subjected to information security threats since its backbone is relying on internet connection. Multiple studies have looked into the matter of information security threats in smart cities (Elmaghraby and Losavio, 2014; Ijaz et al. 2016; Belgaum et al. 2018), some of these threats include (but not limited to): RFID tags abuse and killing, denial of service (DoS) attacks, spoofing, malwares, phising, fruads etc. This topic will be discussed in details in chapter 3.

1.1.2 Cybersecurity

The terms “cybersecurity” and “information security” is usually utilized by people in the same context interchangeably; however, while the two terms are similar and overlap each other, the terms are actually different (Von Solms and Van Niekerk, 2013). The researchers argue that cybersecurity actually extends beyond the limits of information security, in addition to protecting the information resources, it includes the users themselves. The human factor in information security is usually referred to as the part of human in the process of security, while in cyber security the humans are possible targets of attacks. Furthermore, it is safe to presume that one could depict a cybersecurity incident by using characteristics used to identify information security, which implies that a cybersecurity incident would lead to a breach in the C.I.A triad of information. However, the authors have proposed several scenarios where cybersecurity attacks that do not resemble the officially characterized scope of information security, such as cyber bullying, home automation, digital media and cyber terrorism (Von Solms and Van Niekerk, 2013). Figure 2 illustrates the relationship between the three overlapping concepts, which are information security, ICT security and cybersecurity. The notion of information security expands beyond ICT security with the intention of shielding the information, in a similar manner; cyber-security expands beyond information security as to protect the users and any other assets, which may have been prone to threats as results of vulnerabilities evolving from using ICT. Craigen et al. (2014) argue that the literature lacks a broadly agreed on and brief definition that grasps the multidimensional nature of cybersecurity may results in hurdling the technological advancement by supporting the dominant perspective of cybersecurity, while the disciplines that are ought to be supporting the solutions to complex security challenges are separated.

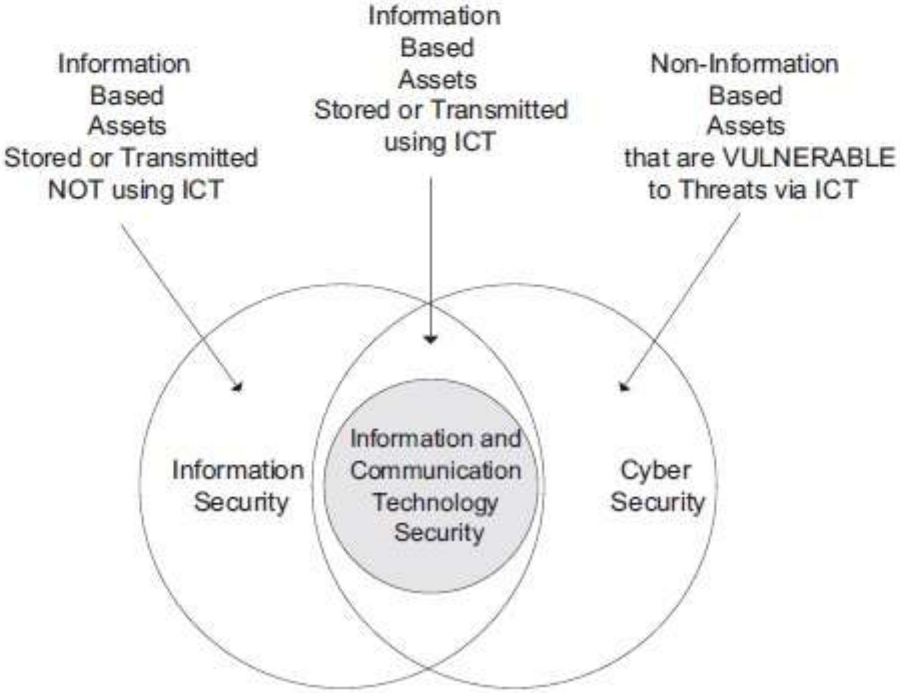

Information Based Assets Stored or Transmitted NOT using ICT
Information Based Assets Stored or Transmitted using ICT
Non-Information Based Assets that are VULNERABLE to Threats via ICT
Information Security
Information and Communication Technology Security
Cyber Security

Figure 2: the relationship between information communication security, information security and cyber security (Von Solms and Van Niekerk, 2013, p.101)

Nonetheless, there are several cybersecurity definitions present in the literature, these definitions are demonstrated in table 1.

Table 1: Definitions of cybersecurity

Cybersecurity definition	**Author(s)**

Protecting a computer system on the internet by taking certain measures against attacks or unauthorized access.	Merriam Webster Dictionary
Cybersecurity is the combination of guidelines, policies, tools, security concepts, actions, training and technologies that could be utilized to protect the organizations' and users' possessions. Those possessions encompass online computing equipment's, applications, personnel, telecommunication systems, infrastructures and information that are stored or transmitted throughout the cyber environment.	International telecommunication Union (ITU) (2008)
Cybersecurity necessitates the protection of information, computers and networks from penetration or from malignant harm.	Lewis, 2006
Cybersecurity includes decreasing the risk of software malignant attacks, as well as computer and networks. It involves tools used to identify penetrations, antiviruses, communications encryptions and block unauthorized access.	Amoroso, 2006
"The ability to protect or defend the use of cyber-space from cyber-attacks.	CNSS, 2010

1.1.2.1 The domains of cybersecurity

In order to safeguard against cybercrime, a robust cybersecurity strategy must have layers of protection. Cyber-attacks may include accessing, altering or corrupting data, attempt to interrupt business process or access organizations' sensitive data (Jang-Jaccard and Nepal, 2014). Therefore, cybersecurity defense mechanisms must address the following domains:

- **Cloud security,** the quick adaptation rate towards the clouds, has energized worries on a critical issue for the threats of communication and information security. Moreover, various unexplored security dangers and difficulties have been acquainted from this migration with the clouds, disintegrating a significant part of the adequacy of conventional safeguarding methods (Zissis and Lekkas, 2012).
- **Network security,** enabling administrators to improve the protection of their networks by employing cybersecurity mechanisms to alert any questionable network activity. Researchers are developing threat evaluation techniques which utilize information fusion, which will assist in countering cyber-attacks (Kuhl et al. 2007).
- **Disaster recovery/business continuity plan,** enterprises nowadays rely heavily on computerized data, and the number of firms whom are relying on such data is increasing every day. Organizations are ought to have methods and technologies to counter an unexpected event, such as power outage or a cybersecurity attack, while exposing critical operations to minimum interruption. It is of paramount significance that companies have planned for disaster recovery (Omar et al. 2011).
- **Storage security** tops the chart of a study conducted by Delahunty (2009) regarding storage concerns, an example of storage security measure is a set of procedures and configurations, which renders storage resources unattainable to unauthorized users and only available to trusted networks and authorized users.
- **Critical infrastructure security,** the critical infrastructure systems that shape the backbone of an advanced society and their dependable and secure activity are of vital significance to public safety and monetary imperativeness. Thus, the cyber framework

shapes the foundation of a country's critical infrastructures, which implies that a significant security attack on cyber systems could fundamentally affect the solid and safe tasks of the actual systems that depend on it (Ten et al. 2010).

- **End-user education,** employing specific security training and educational programs to raise the level of employees' security awareness, such as avoiding suspicious links or the use of untrusted networks (Whitman and Mattord, 2013).
- **Information security,** assuring the confidentiality, integrity and availability of the data through measures such as data protection act (DPA) or general data protection regulation (GDPR) (Tankard, 2016).

1.1.2.2 Threats of cybersecurity

Cybersecurity involves the comprehension of the various cyber-attacks and the employment of defense mechanisms and countermeasures, which ensures that the C.I.A triad of information is intact (Goodman and Lin, 2007). According to numerous experts in cybersecurity, *malware* is the first choice to perform cyber-attacks and breach sensitive data. Attackers utilize malware to compromise the system without the rightful owner being aware of the attack, usually, the attacks fall under many classes, including spyware, viruses, Trojan horses and many others. A typical malware attack taints the system by various methods, including propagating from an infected device to another by loading itself into a USB flash drive and spreading itself in other devices. Another method is by deceiving individuals into visiting a malware-infected webpage, or fooling users to launch infected files (Jang-Jaccard and Nepal, 2014). *Ransomware* is also considered a cybersecurity threat, it works by locking down system files, and in some cases, encrypting them, rendering the whole system inaccessible. Typically, the attackers threaten to destroy or corrupt the data, or publishing sensitive data online, unless the victim paid a ransom to the attackers (Thomas, 2018). Another threat to cyber security is the distributed *denial-of-service (DDoS) attacks*, such attacks aim to crash a server or a network by overwhelming it with traffic, typically from numerous synchronized systems. DDoS attacks may ensue substantial financial and reputation losses for organizations, thus, it is critical to take countermeasures through distinct detection and source identification (Semerci et al. 2018). In addition, *Advanced persistent threats (APT)* attacks is also considered a cybersecurity threat. In such attack, the invader penetrates a system and stays undiscovered for a prolonged period of time, while also keeping the system and network untampered with, which allows the invader to steal sensitive information and spy on the corporate activities without activating any defensive measure. The work of Ghafir and Presnol (2014) presents an overview of several research proposals to APT detection and provided a classification of these researches.

1.1.3 Smart cities

Cities around the globe have a significant impact on the world's economy as a pivotal point of consumption and production, responsible of the generation of a huge share of the globe's gross domestic product (Cohen, 2006). Since the industrial revolution, the population growth has stretched to an unparalleled level. in 2016, it is estimated by the United Nations that 54.5% of the globe's population are resident in civilized settlements, this percentage is expected to increase to 67% by 2050 (United Nations, 2016). Considering this rapid growth, the governments are mandated to conduct major developments to their respective cities' infrastructures to handle the growing demands of the residents. The fast increase in cities' populations will eventually lead to a plethora of issues, such as pollution, conflicts over water resources, traffic congestions, health systems that cannot cope with the increasing population. Such issues may exceed the capability of supplying sufficient services for the residents (Neirotti et al. 2014). The move towards smart cities have become an evolving occurrence, especially with the rapid increase in civilized population growth and the exponential advancements in technology (Ijaz et al. 2016). However, what exactly is a smart city? According to Baig et al. (2017), a smart city is a technologically advanced urban area that consists mainly of four components: smart grids, building automation systems, unmanned aerial vehicles and smart vehicles. The smart city envisions a connected environment that is achieved through maintainable enabling technologies such as the cloud and IoT. Additionally, numerous sorts of IoT sensors should be employed to enable the use of a multitude of services such as smart parking, traffic congestion level monitoring, smart traffic and street lighting and structural health awareness. Figure 3 demonstrates a high-level overview of interconnected smart city component.

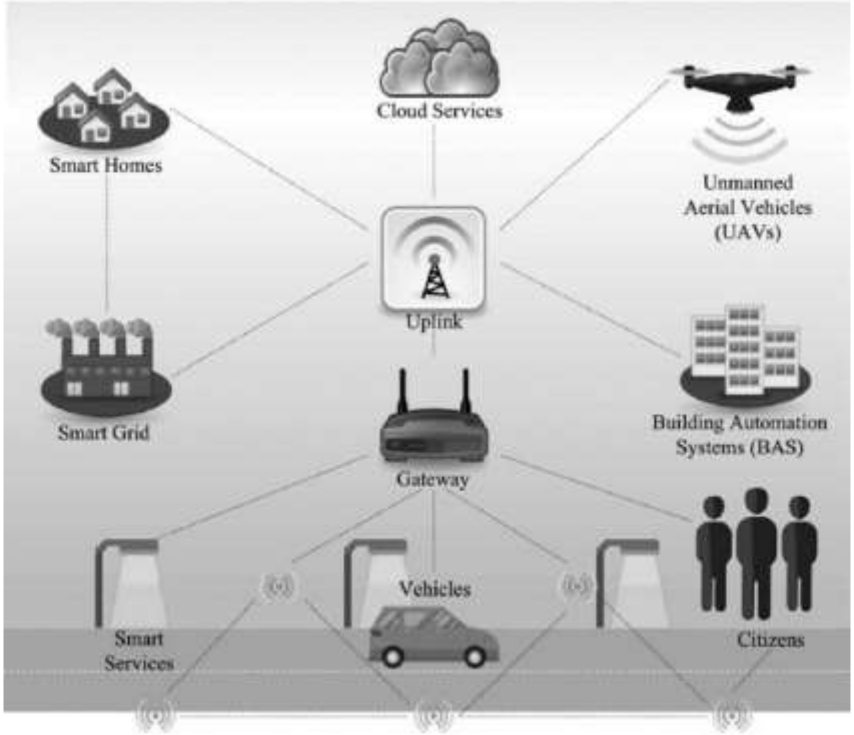
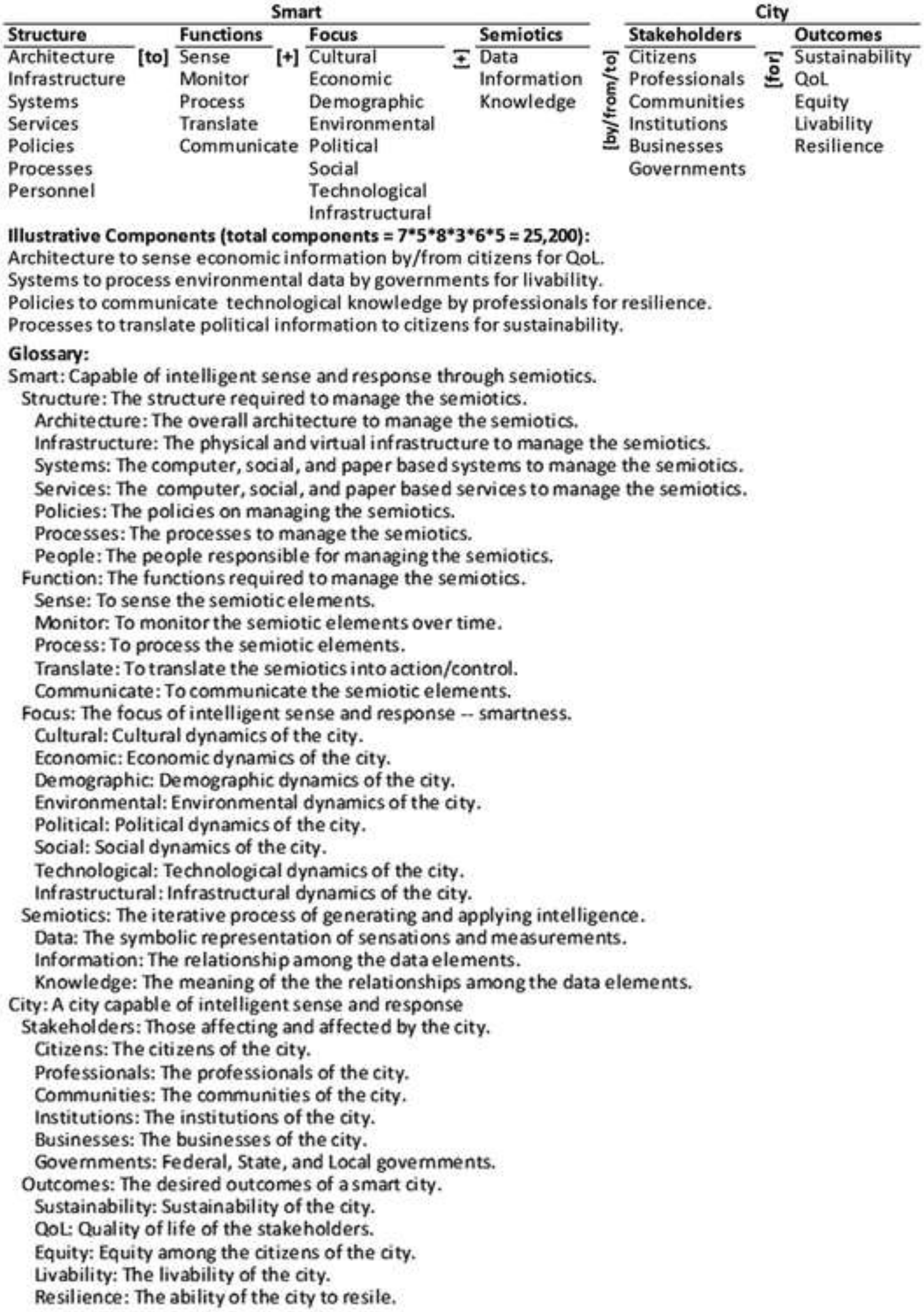


Figure 3: High-level overview of interconnected smart city components (Baig et al. 2017, p. 2)

Ijaz et al. (2016) argues that a smart city should consist of major five components, namely, smart commerce (real estate, banking and finance), smart environment (energy management, waste management and water management), smart governance (government, security, health, infrastructure and education, smart communication (identity and communication) and smart mobility (transport and traffic). Ramaprasad et al. (2017) have proposed a unified definition of a smart city that represents a high-level ontology as depicted by previous research. Figure 4 demonstrates the unified definition proposed by ramaprasad et al. (2017).



Smart								City		
Structure		**Functions**		**Focus**		**Semiotics**		**Stakeholders**		**Outcomes**
Architecture	**[to]**	Sense	**[+]**	Cultural	**[+]**	Data	**[by/from/to]**	Citizens	**[for]**	Sustainability
Infrastructure		Monitor		Economic		Information		Professionals		QoL
Systems		Process		Demographic		Knowledge		Communities		Equity
Services		Translate		Environmental				Institutions		Livability
Policies		Communicate		Political				Businesses		Resilience
Processes				Social				Governments		
Personnel				Technological						
				Infrastructural						

Illustrative Components (total components = 7*5*8*3*6*5 = 25,200):
Architecture to sense economic information by/from citizens for QoL.
Systems to process environmental data by governments for livability.
Policies to communicate technological knowledge by professionals for resilience.
Processes to translate political information to citizens for sustainability.

Glossary:
Smart: Capable of intelligent sense and response through semiotics.
Structure: The structure required to manage the semiotics.
Architecture: The overall architecture to manage the semiotics.
Infrastructure: The physical and virtual infrastructure to manage the semiotics.
Systems: The computer, social, and paper based systems to manage the semiotics.
Services: The computer, social, and paper based services to manage the semiotics.
Policies: The policies on managing the semiotics.
Processes: The processes to manage the semiotics.
People: The people responsible for managing the semiotics.
Function: The functions required to manage the semiotics.
Sense: To sense the semiotic elements.
Monitor: To monitor the semiotic elements over time.
Process: To process the semiotic elements.
Translate: To translate the semiotics into action/control.
Communicate: To communicate the semiotic elements.
Focus: The focus of intelligent sense and response -- smartness.
Cultural: Cultural dynamics of the city.
Economic: Economic dynamics of the city.
Demographic: Demographic dynamics of the city.
Environmental: Environmental dynamics of the city.
Political: Political dynamics of the city.
Social: Social dynamics of the city.
Technological: Technological dynamics of the city.
Infrastructural: Infrastructural dynamics of the city.
Semiotics: The iterative process of generating and applying intelligence.
Data: The symbolic representation of sensations and measurements.
Information: The relationship among the data elements.
Knowledge: The meaning of the the relationships among the data elements.
City: A city capable of intelligent sense and response
Stakeholders: Those affecting and affected by the city.
Citizens: The citizens of the city.
Professionals: The professionals of the city.
Communities: The communities of the city.
Institutions: The institutions of the city.
Businesses: The businesses of the city.
Governments: Federal, State, and Local governments.
Outcomes: The desired outcomes of a smart city.
Sustainability: Sustainability of the city.
QoL: Quality of life of the stakeholders.
Equity: Equity among the citizens of the city.
Livability: The livability of the city.
Resilience: The ability of the city to resile.

Figure 4: A unified definition of smart city (Ramaprasad et al. 2017, p. 17)

1.1.3.1 Components of a smart city

This section will discuss in details the different components that make a smart city. In addition to the components mentioned earlier in this dissertation, there are a few more to truly construct a smart city, these components are discussed below.

- **Smart infrastructure:** Information and communication technologies (ICT) greatly enhances the capability of infrastructure management, making it more efficient and effective. The use of ICT in the field of smart grid could help in optimizing electricity consumption. Recent progression in wireless and automotive have aided in the evolving of vehicular ad hoc networks (VANETs), consequently helping intelligent transportation systems to provide a slew of safety and information features to the public (Ota et al. 2017). Other fields included are sensor networks, digital infrastructure management and waste and water management (Belgaum, 2018).
- **Smart technology:** The use of smart technologies includes the utilization of physical logical implementations that have the ability to automatically adapt and modify the attitude to better suit the environment, as well as sensing the surroundings with sensors. These advanced technologies offer a significant contribution in the growth of economy, multiple facilities such as factories, hospitals, restaurants etc. could be transformed into automated systems that operate without human interactions, therefore publicizing the data to the individuals for better decision making and processing (Alansari et al. 2016).
- **Smart buildings:** These buildings utilize network devices and equipment's, as well as the utilization of additional systems to manage and control renewable energy resources. Smart

buildings also utilize ICT to allow them to control and communicate with its appliances and devices, in addition to communicating to other buildings and adapt to the grid's condition. Smart buildings comprise of sensors, actuators, controllers, central unit, interface, network and smart meters (Morvaj et al. 2011).

- **Smart government:** As a response to the fast developments in digital technologies, a smart government is considered an evolution of e-government, paving the way to devise new methods for the government to enhance the engagement with citizens, compatibility and accountability (Gil-Garcia et al. 2016). Smart government is considered a major component of a smart city, it allows an open channel between the government and citizens (G2C), government and businesses (G2B) and government to government (G2G) to interchange ideas or transactions more effective and transparent (Mellouli et al. 2014). This channel is facilitated with the use of ICT, through the application of IoT-enabled artificial intelligence (AI) technologies, efficiency of governance and the residents' life quality can be vastly improved (Kankanhalli et al. 2019).
- **Smart healthcare:** The progressively aging population and the increase in chronic diseases have burdened modern healthcare systems (Baker et al. 2017). The utilization of IoT has been broadly considered a possible solution to relieve the pressure off health care system. The literature has looked into the use of IoT to monitor patients with particular illnesses, or serve a specific scenario, like monitoring a patient's progress while rehabilitating (Gope and Hwang, 2015; Zhu et al. 2015; Chang 2016).
- **Smart Security:** Through the design of intelligent systems that are based on IoT, researchers were able to innovate security devices that are cost efficient and effective in

protecting residents' and organizations' properties (Kodali et al. 2016; Saifuzzaman et al. 2017). Some examples may also include surveillance and biometrics, intelligent menace detection, advanced cyber protection through firewalls and antiviruses (Belgaum, 2018).

- **Smart mobility:** Mobility is considered to be a significant facility to underpin the operation of an urban area (Staricco, 2013). Nonetheless, the growth in population in urban areas have led to an increase demand on transportation, which in turn produces several issues, such as time consumption due to congestions, increased carbon footprint, unoptimized costs and timing of public transportation, traffic accidents, etc. Thus, the introduction of smart mobility has the potential to aid in remedying the above-mentioned issues (Benevolo et al. 2016). It relies on physical structure, ICT and functional technology, these components are mandatory to have a reliable, intelligent and high-quality solutions (Nam and pardo, 2011).

1.1.3.2 Challenges of transforming into a smart city

A smart city presents a potential solution to the negative impacts that accompanies the rapid growth in population; therefore, the move towards a smart city might seem a rational strategy for the governments to implement. However, to accomplish such a marvelous endeavor, a number of challenges emerge. The work of Ejaz and anpalagan (2019) provided an insight on the potential challenges that should be addressed before proceeding into the transformation process. The first challenge is *planning*, as cities are formed by comprehending the human behavior, it is critical to examine the urban dynamics, citizens' involvement and open data. Rushing the transformation into a smart city may lead to a plethora of unfinished projects that are a waste of funds. In addition, retrofitting existing obsolete infrastructure in order to create a smarter city is very difficult. The next challenge *costs and quality*, it has always been a rough decision to either implement a low cost / low quality solution or a higher quality but more expensive solution. For a smart city, it is necessary to only utilize high quality components, since they produce more accurate results and less prone to failure. Because a smart city relies mainly on ICT, IoT, sensors etc. any failure of any of those components may halt the operation of the whole system. The most important challenge facing smart city is *security and privacy*, the scale of ICT utilization is so massive that even a low threat incident could have impactful negative consequences. Moreover, sometimes IoT devices could be invasive and collecting confidential residents' data, which is an inevitable flaw that may make people uncomfortable. Another challenge is the *risks* that are associated with smart cities, the authors argue that these risks include technology risks, a new technology may not perform as anticipated. Operational risks, an operation is subjected to not function to its maximum capacity due to inapt operator. Construction risks, unpredicted hardships or difficulties may occur throughout the construction phase. Market risks, the demand of a new service may not match the projected target, which may cause extra cost that could have been avoided, or put into a more feasible project.

1.2 The Problem Statement and Research Questions

The United Arab Emirates has taken the initiative to transform its cities into smart cities (Breslow, 2021), since it has been an attraction for expats for decades, the population have been rapidly increasing ever since. According to the smart city index 2021, Abu Dhabi and Dubai have been ranked as the smartest cities in the Middle East for the second year in row (Kumar, 2021). However, transforming into a smart city is accompanied with a number of challenges, as many smart solutions that are vital components of a smart city necessitate the utilization of ICTs and IoTs, a requirement that raises concerns for information security. The amount of data that is being collected, processed and stored is massive. Thus, any information security incident could result in massive damage, whether it is residents' personal data, healthcare, critical infrastructure or government data. The leak of such sensitive data due to a cyber-attack will directly conflict with the main purpose of a smart city, which is providing a better life quality and facilitate transactions between the residents and the governments, since a cyber-attack could render certain services completely unresponsive. Nonetheless, identifying recent cyber-attacks that targeted smart cities and security/privacy weaknesses, and implementing specific cybersecurity measures could prevent such incidents from occurring.

This research aims to address the following questions:

1- What are the main information security challenges that are faced by the organizations of Dubai and Abu Dhabi?

2- To what extent are the organizations of Dubai and Abu Dhabi prepared to detect, prevent or respond to information security threats?

3- Do we have the needed knowledge to protect ourselves enough?

1.3 Research Objectives

Addressing the research questions will aid decision makers in the UAE to visualize the significance of information security in the context of smart cities. This research aims:

1- To develop an understanding about recent and contemporary types of cybersecurity threats that targets smart cities, Abu Dhabi and Dubai in particular.

2- To measure the level of awareness among the residents of Abu Dhabi and Dubai about cybersecurity threats, and whether they take enough measures to protect themselves of such threats.

3- To examine the level of readiness for cyber-attacks and the current measures and tools that are implanted in the UAE.

1.4 Research Map

Table 2: Research map

Research problem	Research Aim	Research Objectives	Research Questions	Underlying Theory/Theories
The UAE rapid increase in population and urbanization has called upon the necessity to transform its cities into smart cities; However, the transformation into a smart city has key challenges, one of them being cybersecurity challenges. The problem stems from the need of developing awareness about the recent cyber-attacks and threats that interrupt the operation of a smart city, as well as	Examine the recent challengers in cybersecurity for a smart city, cyber-attacks and potential threats which may harm the harmony and balance of the residents' life, implement security measures and insure accurate and timely risk detection.	To develop an understanding about recent and contemporary types of cybersecurity threats that targets smart cities, Abu Dhabi and Dubai in particular.	What are the main information security challenges that are faced by the organizations of Dubai and Abu Dhabi?	Among the challenges of transforming into a smart city, cybersecurity is a key challenge that may hamper the progress and operation of a smart city, since it relies heavily on the utilization of ICT and IoT.
		To measure the level of awareness among the residents of Abu Dhabi and Dubai about cybersecurity threats, and whether they take enough measures to protect themselves of such threats.	To what extent are the organizations of Dubai and Abu Dhabi prepared to detect, prevent or respond to information security threats?	
		To examine the level of	Do we have the needed	

developing a framework that could be implemented to prevent cyber-attacks and activate proper measures and technologies to achieve high level of cybersecurity.		readiness for cyber-attacks and the current measures and tools that are implanted in the UAE.	knowledge to protect ourselves enough?	
		To propose a framework that can be implemented by decision makers in the UAE that aims to activate proper cybersecurity measures, tools and technologies against threats and cyber-attacks.		

1.5 Dissertation Structure

This dissertation is divided into 7 chapters, which are discussed in details in table 3.

Table 3: Dissertation structure

Chapter number	**Description**
Chapter 1: Introduction	This chapter serves as a pre-amble to this thesis, it discusses an overview of the topic, main concepts and key definitions, the research map and objectives. It assists the reader to comprehend and grasp the purpose of this research.

Chapter 2: Information Security Management in Smart Cities	Chapter 2 contains key topics and technical details about information security management in smart cities, the concepts of IoT devices, asset registration, risk assessment, data classification, policies and procedures, security awareness, security control effectiveness, cyber security and benefits of implementing information security management in smart cities.
Chapter 3: Literature review	This chapter provides an insight into the latest research in the field of cybersecurity challenges in smart cities; it explores key cybersecurity challenges and frameworks to be implemented (if any) by decision makers in smart cities.
Chapter 4: Research methodology	This chapter will discuss the research methodologies that will be implemented to accomplish the objectives of this study, as well as the tools and techniques that is employed in the study.
Chapter 5: Results	Chapter 5 will include detailed analysis of the results obtained by implementing the research methodology, quantitative descriptive analysis will be carried out to help in understanding the current situation, as well as identify key threats and cyber-attacks based on the results of the analysis.
Chapter 6: Discussion	This chapter will discuss in details the results obtained from the gathered data about the key challenges of cybersecurity, as well as proposing a framework based on the results and the analysis of the data.
Chapter 7: Conclusion	This chapter presents an overview of the research outcomes, limitations and suggested future work and research opportunities.

Chapter 2: Information Security Management in Smart Cities

People live in safe and smart cities for the best and easy life practice to be able to reach the sustainable future. Countries do yearly show for the best and new technologies to invest in the digital convert. Shows provide the focus on the smart cities' challenges in the cybersecurity world. Now we live in the time of IoT. Internet of things provide more challenges to write and enforce new policies and procedures to the best strategic plans for the best solutions to deal with the best practice of repel of the technologies weaknesses. In the addition of creating information security awareness with more and more strong economy for the solution of smart cities which supports the internet technologies (Aljazeera net, November 1, 2019). The smart city is an urban development project that uses information and communication technology to improve the efficiency and effectiveness of its operations. Its core technology is based on the concept of privacy, security, and authenticity. We propose a comprehensive approach for addressing the privacy and security issues of the data management interface of smart city applications. It is based on the concept of Holistic Big Data Integrated AI. The Big Data analytics-assisted privacy scheme has been implemented to improve the efficiency and security of the data management interface of smart city applications. It also supports the flexibility of the data management interface (Chen et al, 2021).

2.1 Scope of IoT devices

The existence of DDOS attacks on Internet of Things networks is considered very dangerous. Due to their nature, the researches activities mainly focus on the use of machine learning techniques to develop effective defense measures against such attacks. This paper aims to introduce a novel approach that combines the use of traffic flow data and machine learning to predict the attack frequency. (Rambabu and Venkatram, 2021). Due to its numerous advantages, such as its ability to provide real-time connectivity, the Internet of Things has been widely used. Its primary task is ensuring that the various protocols are used to allow the proper communication between various applications and devices. As the number of applications for Internet of Things (IoT) continues to grow, it is necessary to modify the protocols to address the various issues that arise. Current state of the Internet of Things application layer protocols and their adaptation are to improve performance. Machine learning can help develop and implement new protocols that can adapt dynamically (Donta et al. 2021). Many of the devices deployed for the Internet of Things are being used in the wild. These include monitoring critical infrastructures such as power grids and telecom towers. Current approaches rely on a secret key that can be stored in a non-volatile memory. This method is vulnerable to exploitation due to its energy-consuming nature (Vaidya et al. 2021). The Internet of Things (IOT) is a wide-scale network that enables various devices to communicate with each other. Its growing popularity has caused various security concerns. Our study aims to explain the various reasons why IOT security is important and what the latest research is doing to improve it (Garg and Singh, 2021).

2.2 Asset Registration

Urban planning is shifting towards smart city development (SC). This involves the use of various technologies and soft assets to enhance the efficiency and effectiveness of the urban community. Different approaches are used to identify and measure intangible or soft assets. They are often linked to other assets and are unique to each individual. Different frameworks and methods are used to measure intangible assets. This makes it possible to identify and understand the various roles of these assets and how they are interrelated within a multi-tier urban development project. Developing a strategy that focuses on the use of soft assets can help improve the efficiency and effectiveness of local government units. This can be done through the development of an evaluation framework that addresses the various aspects of soft assets. This can help improve the effectiveness of local government units (Wataya and Shaw, 2019).

The most recurring components of a smart cities are technology, people, education, innovation and creativity. Smart Cities are envisioned to enhance the democratic process and provide the community with an alternative method of interaction. However, they also face various challenges such as transparency, accountability, and isolation. The technologies of smart cities do a good development of the democratic system, some hard "they also face various challenges such as transparency, accountability, and isolation" (Heaton & Parlikad, 2019). The most important step to do in information security while dealing with assets is the asset registering. You cannot protect your assets without registering the assets, and add every asset with its component such as vulnerability risk assessment; people risk assessment, and application risk assessment. (Leal, 2016).

2.3 Risk Assessment

States now implementing new technologies to convert into the smart cities. It is very critical to take the concepts of the smart cities as technology with people. Many challenges to solve for converting cities into smart cities. The main component of smart cities the IoT, with the use of artificial intelligence, and the implementation of the block chain (Singh et al. 2020). The use of (AI) in the risk assessment can provide new dimensions as the AI can detect the intrusion, data hack and data leakage (Raghuvanshi & Singh, 2020). So, this is the challenge we need to implement and to protect our lives and privacy from red teams attacks using traditional ways or even to do hacks using the (AI) systems. (Al Sharif & Pokharel, 2021). Risk assessment and treatment together called processes of risk management. They are the most important milestone in information security on the scope of company, organization and smart cities. It is also, the hardest mile stone in implementing information security, this is the process of collecting the risks, evaluate them and treat them. this process provides us the most important risks to deal with plus the ability to treat them based on the most important treatment against confidentiality, integrity, an availability (Kalinin et al. 2021). This process provides us how much information security controls to implement besides the amount of money to spend on each information security control which is called security appetite. To be able to reach the residual risk which is the processes of the security acceptance where the upper management can accept it. In the ISO27001, there are six ways to implement risk management (Kosutic, 2021a).

1. Risk assessment methodology

Which is the method you want to identify risks with risk treatment.

2. Risk assessment implementation

In this step you need to prepare an excel sheet to identify every risk against the technology because information security is layers from down to top and the layers are information, applications, operating systems, hardware, network and physical security controls.

With identifying the risk against confidentiality, integrity and availability by quantitative or qualitative measures.

3. Risk treatment implementation

Now for each security risk with the mark in the previous step we do need to implement the needed security controls to lower the risk to the acceptable level.

4. The assessment report

The representing and writing the report of the previous steps for the upper management, the risk owners and the information security themselves.

5. Statement of applicability

This paper's statement of applicability is the smart cities profile of security. This paper is very important because the auditors will use it to provide the security ISO27001 certificate. This statement will provide us of the security controls when to implement and how to implement it.

6. Risk treatment plan.

This is the process of moving from the papers to practically implement the security controls. This is the process of the asset owner of the security controls and when he/she going to implement it with a time frame. In this plan you have to have upper management agreement on the security controls implementation time and money. Alternatively, you will not move any step forward.

2.4 Data Classification

Sixty-nine information security controls were grouped in sixteen groups. These groups can be summarized as access control, identification and authentication, physical access controls (Shoulder surfing protection), physical control (Shoulder surfing protection), attack resistant, attack tolerant, Secure System and Service Acquisition, System hardening, Attack Monitoring, and the strategy security of security controls based on the 5W1H (Who, What, Where, When, Why, and How) (Han, et al. 2021). The use of machine classifications to clarify the data input in the ability of using data mining is a practical way of using mathematics algorithms to identify information security attacks and data leakage to provide a high percent of information security (Olga et al. 2021). The UK government classify information into three levels 1. Officially, which is made by public or information is to be published to the public. 2. Secret, which is data used internally and it, should be taken considering not to be published. 3. Top secret which is the most critical information and must be protected with the highest security controls because any loss of this information; it could cause to harm people or economic situation to the organization (Shrestha et al. 2020). CISSP knowledge, which is one of the best information securities in the world. The CISSP provide four of data classifications. 1. Public as data can be announced into the public. 2. Private, which is data, can be used internally as the HR data. 3. Secret data, which can be allocated into the managers, and this data must be protected strongly. Moreover, 5. Top secret, which must be allocated to the top management or the board of directors. This data must be protected as much as possible because this data can harm people or organizations, or the good impression of the smart city. “The primary purpose of data classification is to indicate the level of confidentiality, integrity, and availability protection that is required for each type of data set.” (Maymí & Harris, 2021).

2.5 Policies and Procedures

More stress in the work environment leads to not follow the policies inside the organization (Trang & Nastjuk, 2021). Information security policies are the base line to the information security process. The smart city must implement the information security polices to be able to protect the city in the digital world and meat the smart city protections objectives. Policies can evaluate the information security program and process. Without the existence of the information security Polises; security violations cannot be identified. Management must fully support and enforce the information security policies (Flick & Morehouse, 2010). In the time of the support from management support. Policies must be implemented, evaluated, and updated by the information security team (Watson & Jones, 2013). In Socio-Cyber-Physical Systems; the team identified information security for the analysis of the applicability and requirements of the information security by a sophisticated algorithm (Ouchani, 2021). Organization and smart cities investments are in Mellions on the hardware securities such as firewalls but not that much in security policies and procedures that provide the persons behavior in the digital world (Dario Forte). Information security policies were made to enhance employee's behavior against the compliance systems (Xu et al. 2021). Smart cities must have a master policy, this general policy produced by the upper management. It describes the amount of information security must be accepted by the management. Then there must be an issue specific policy that address an issue such as password policy, email policy, and vulnerably policy etc. The procedures are steps to do in particular of steps related to information security. The steps could be done by personnel's, systems or third party (Maymí & Harris, 2021).

2.6 Security Awareness

Information security awareness program and training provide the employees and smart cities citizens their important role on how to protect themselves and the sensitive data from discloser or corruption. This process of awareness is to make people of smart cities know how to protect themselves from social engineering attacks (Wright, 2008). Social engineering attacks means a thief or racketeer person introduce him/herself as a formal person's need some information allow him/her the access to a sensitives, secret or top secret classified data, people are always the weakest ring in the information security chain (Gardner & Thomas, 2014). "Awareness is communications. Awareness is understanding risks. Awareness is being proactive to those risks with sensible solutions" (Wiles et al. 2008).

2.7 Security controls effectiveness

SysAdmin, audit, network and security critical security controls are a suggested group of activities for cyber protection, which deliver particular and workable methods to halt today's most persistent and dangerous attacks (“At least 3 of Sans”, 2021). Security controls are layers as the physical layer including guards, locked doors, and cameras. Digital security layer as antivirus, two-factor authentication, and firewalls. Cyber security controls that prevent attacks as DDOS prevention and data leakage prevention, and intrusion prevention systems. Cloud security systems such as data encryptions and all cloud security control keep data safe. It is important to invest in security controls and their reactiveness. Such information security training must be evaluated to make sure the information security training changes to the best (Abraham & Chengalur-Smith, 2019). Machines learning can be used in the world of information security controls effectiveness by using the most known machine learning techniques. This study developed a new information security control effectiveness to detect the anomalies in the logs of the information security controls (Sarker, 2021). Fuzzy reasoning algorithm is used to detect information security attacks by mining the data logs of the information security control than using data classification to detect the network access controls (Zhang & Hu, 2021). “Information security is the backbone of current intelligent systems, such as the Internet of Things (IoT), smart grids, and Machine-to-Machine (M2M) communication.” in the new era of technologies we have new communication types such as IoT, smart grid technologies system and M2M machine to machine of communication. In addition, these technologies generate new kinds of communications with communications data as big data. This opens new doors of risks and attacks that we need to have new technologies to be able to protect such kind of data by taking the risks of these technologies seriously. New security controls needed and check the ability of these security controls in protecting this new kind of generated data. (Hamdoun & Sagheer, 2020). The evaluation of the physical security controls is very important. We can become surer of our physical security controls by calculating the wight of these security controls. This technique is very useful to make sure that our physical security controls are efficient in a quantity manner. (Liu et al. 2021).

2.7.1 Audit security controls to assure conformity of information security

The audit security control is a comprehensive evaluation for all information security controls that measures the applicability and ability of the security controls (Nahar, 2020). There are two kinds of audits. External auditing and internal auditing. The external auditing done by third parties who grant the certification of information security standards. The most known international of external audits are ISO27001 lead audit and Certified Information Security Manager CISM. Alternatively, there is an internal audit, which is mandatory by the governance regulations (Gantz, 2014). Organizations with extremely sensitive data such as financial as banks must do information security audit frequently worldwide information security standards do this audit once or two times per year (Gillis, 2021). It is especially important to do a security audit to determine the vulnerability assessment and the meat of risks evaluations in the organizations' infrastructures. It is to check the available security and risks. The need to check security policies and procedures with the enforcement of their rules. The protection against cyber security attacks. The confidentiality of data flow. Check against compliance. Updates of measures evaluations and enforcement. The enforcement of security awareness against social engineering. The ability of incident response immediately as needed in incident handling. In addition, the check of all organization structures against information security controls, as they needed in all their needed places in data, applications, hardware, and physical controls (Nahar, 2020). Some audit specifically measures the systems access such as Mandatory Access Control (MAC). Some access audit internally is who has access, to where having the access, and the time to have the access as in Rule-Based Access Control (RBAC) (Dubrawsky & Faircloth, 2007). ISO27001 gap analysis is a great initial of a system security auditISO27001 auditors checks security controls by the statement of applicability prepared by the team of ISO27001 implementation (Al-Karaki et al. 2020).

2.7.2 Perform the assets owner review

It is very important to register the assets inside the organization and register each asset to its owner to be able to get approval in case you need it. By registering the asset owner, you can easily and effectively reach the owner of the asset in case of any incident or evaluate the assets against confidentiality, integrity, and availability. This way you can classify the asset with the help of the asset owner. Because the asset owner is the most qualified person that can classify the asset correctly in all information security levels as smart cities through organizations to the mobile systems. The department asset owner can easily assign asset access to the write person with the ability to revoke it when needed. Asset owner registering is a management role (Maymí & Harris, 2021). The asset owner can specify why security controls are worth the expenses being spent on them. He/she can easily identify the threats on the asset. This is to limit the exposure on the valuable assets (Thomas R. Peltier). The asset owner assigns the goals of the assets with its values then writing a document why choosing this value (Tariq, 2019). The upper management is the one responsible to choose the asset owner. They know the asset owner that can identify and evaluate and solve risks. The one who has the full power to do it. The asset owners should check the list of their own assets to see if there is any missing assets must be added to the list with their own vulnerabilities, risks likelihood with the determining the risk level (Kosutic, 2017a).

2.8 Cyber Security

In the next 30 years, 70% of worldwide people will live in cities (Omar, 2021). Cities are developing and converting to become smart cities more often than before. This will add more challenges in the cybersecurity field. As vulnerabilities in all systems, day by day come to be real threats on the government systems and the personal systems. Any attack or break on any level of infrastructure beginning on the personal mobile systems up to the government will put the overall technologies at risk (Ma, 2021). “Three core considerations during transformation are population risk awareness, effective process and adoption of disruptive technologies “(Omar, 2021)

Cybersecurity discusses and solve the most sensitive systems in smart cities as the denial of service of the most important services as the SCADA systems. In addition, cybersecurity solves critical risks such as privacy protection, eavesdropping, malicious attacks, and many more. (Ma, 2021). The deep learning of artificial intelligence is involved widely in smart cities cybersecurity to detect any abnormally behaviors. Deep learning is very important in urban modeling as the best route for traffic based on the cameras, as the best parking can be used. Infrastructure, transportation, urban management, resilience and sustainability, education, health, security and privacy (Ma, 2021). “Cybercrime is a full-time job, and fighting it requires both intense focus and an expansive vision”. Cyberattack frequency is increasing rabidly and there is no a one book or action to solve them all. The responsibility first is on the system vendors that must security, encrypt their system, and report to the smart city leaders. Other actions such as vulnerability assessment and treatment with penetration testing must be available in the leader’s plans (Vigoli, 2021). Now is the employee and the user is the weakest link. Information security is changing from information security to information security culture. This way we can protect us as smart cities users from social engineering attacks that make cybersecurity attacks more easily. There is a little regulation for the cryptocurrency that manages its use; that is why it will be a weakness and high risk in its use. (Hanson, 2021). As the election became online. Furthermore, advanced cybersecurity threats can go through the systems silently and change whatever hackers want; more regulations and cybersecurity techniques must be implemented to be able to prevent such attacks. (Marks, 2021).

2.8.1 Vulnerability Assessment

Planning and implementation of technology in smart cities is needed to be on all infrastructure levels. The complex dimensions of IT implementation in smart cities opens new very high risks to people's lifestyles because of vulnerabilities. (Al Sharif & Pokharel, 2021). In the study on a smart city in India (Kawyitri & Shekhar, 2021) that the smart city is more vulnerable in financial systems but less vulnerable in social activities systems. In smart cities, "major security issues present at perception layer, network layer and application layer of IoT architecture." (Raghuvanshi & Singh, 2020). The solutions for vulnerabilities assessments and management must be on all levels build the smart cities. Levels of IT infrastructures on the government level, the level of the smart IT vendors. With the level of the people specialized to check and find technical vulnerabilities in the IT devices with having the tools to do vulnerability management to solve the most common known vulnerabilities, to the level of the e-government that provides smart devices the ability to interact with the e-governments facilities online. In addition, there must be policies and procedures to manage the access into the e-governments facilities to avoid the non-technical vulnerabilities in the same time with the fully technical vulnerabilities. (Li & Liao, 2018). AI algorithms can detect vulnerabilities by collecting data from different smart cities devices such as IoT and highlight it to be managed such as AI can detect an attack of detecting leakage of sensitive information. In the same manner there could be a weakness by the AI that could do bias based on certain races, colored people or even gender as Amazon algorithm did before against women. These vulnerabilities in AI detecting vulnerabilities must be evaluated regularly (Ahmad et al., 2022).

2.8.2 Penetration Testing

With the growth of smart cities. Smart cities must be ready for cyber-attacks on the ICT. It must have the ability to detect attacks immediately. Again, we can use deep learning AI systems to detect cyber-attacks. (Mohammadpourfardet al. 2021). block-chain is technology can save the stability of the smart cities as everything is encrypted and can be filled with governments data access and interactions as government payments. (Bagloee et al. 2021). Ordinary people technical skills are weak. This can make the task of cyber-security against attacks difficult. This must rise the alarm to awaken people against cyber-security attacks. The ability of doing penetration testing on smart cities ICT need very well planning and procedures. (Yamin, et al. 2021). Simulation attacks must be made on the critical smart cities components such as electricity systems to report the ability of the immunity of this system against cyberattacks. (Choeum & Choi, 2021). There are models to do penetration texting to evaluate the immunity of the systems against cyber-attacks. the model simulates real attacks such as Denial Service Attacks and Intrusion Attacks (Fu et al. 2021). Cyber Physical Systems penetration testing is implemented side by side with the ICT systems. “Cyber-physical moving target defense (CPMTD) technique that focuses on both attack prevention and detection to mitigate such static vulnerabilities and provide a combination of defense strategies for power system.” (Hu et al. 2021). An important action needed after every penetration testing on any

ICT in the smart city is the lesson learned to be able not to fall in the same problems again. It is the ability to document the evaluation of the results and reports, understand the attacks vectors and the motivations, the impact of the threat, and continue to develop systems hardening and steps forwards to protect ourselves. (Miller et al. 2021). It is important to build security intelligence centers to provide us of alarms immediately of attacks to be able to take the needed provides immediately to stop the attacks on time with the ability to consider where the attacked exactly and what systems with what sensitive information or what sensitive systems such as power or water systems attacked. (Miloslavskaya, 2021).

2.9 Benefits of implementing information security management in smart cities

There are no full solutions to information security problems. They talk about firewalls, Anti-viruses, or frameworks. Because how can you deal with an angry employee or a hacker who interrupted the services? The ISO27001 compliance can solve these problems as you implement it step by step through your organization's levels. Implementing the compliance framework in your smart city can bring business benefits (Dejan Kosutic, 2017b). “Operations security is all about ensuring that people, applications, equipment, and the overall environment are properly and adequately secured" (Maymí & Harris, 2021). Therefore, the implementation of information security management, which is the compliance framework, is to protect the information against confidentiality, integrity, and availability. The ability to protect the information from unauthorized access, unauthorized change, or unauthorized shutting down the services in the organizations leads the smart city. (Kosutic, 2022). The implementation of the compliance on the smart cities CIT provides a better image because people make sure their life is going to be easier and their privacy will be protected. People who have sensitive and confidential data. Thus, they can depend on the smart city infrastructure in their daily technology use of their financial and social engineering transactions. Smart cities can be protected by lowering the amount of incidence on the information which is the city people’s privacy and the incidence on the infrastructures by taking the needed action in real-time. The compliance will optimize all operations on all smart city infrastructures because the responsibilities and the business processes will know. Hence, it is the asset owner again. Which is responsible for an amount of the information and infrastructure. Implementing compliance minimizes the risk of any valuable information. Compliance deals with legislation so incidence rights can be taken in court. One of the most important benefits of implementing compliance is the lesson learned and records keeping. This benefit makes incidences tracked easily and the root cause of problems found quickly and accurately. This benefit also leads to the corrective action and the prevention action. (Kosutic, 2021b). Some of the benefits of implementing information security in smart cities include data protection by improving compliance and information security regulations (Kitchin, 2016), providing excellent image for the smart cities in the eye of customers who have sensitive privacy and data (Tragos et al. 2014) and improving financial gains with the ability of lowering expenses of information security incidents (Li & Liao, 2018).

Chapter 3: Literature review

It is noticeable that the world’s population is growing rapidly; therefore, the demand of these users is also increasing. Smart cities are emerging to contain the increasing number of people. It is true that the emerging of smart cities would create several social and economic opportunities. However, new security challenges would arise, these challenges must be tackled with a lot of attention and dedication. This section addresses the most notable cyber security challenges that face smart cities.

3.1 Current and Future Challenges Facing Smart Cities

Elmaghraby and Losavio (2013) mentioned that humans are already connected to everything around them using their smart phones. This require the city’s services, infrastructures, and transportation to be all interconnected. According to Elmaghraby and Losavio (2013), this will create multiple challenges. For example, most citizens are currently using smart phones and social media, and as a result, a lot of data about their private lives, locations, and information are available online. This will significantly make it easier for hackers to invade their privacy. However, owning a smart phone is essential to live in a smart city. Also, additional security problems would arise, such as: the ease of accessing illegal documents and information which may result in cyber-attacks. Consequently, Elmaghraby and Losavio (2013) introduced a model to represent the interactions between people, their surrounding environment, and servers. In that model, there are three areas of information to be protected, and they are as follows:

1. Information available for use and accessibility.
2. Information's integrity and authenticity.
3. Confidentiality and privacy of the information.

After that, Elmaghraby and Losavio (2013) stated the main standards relating privacy and cyber privacy, and they are as follows:

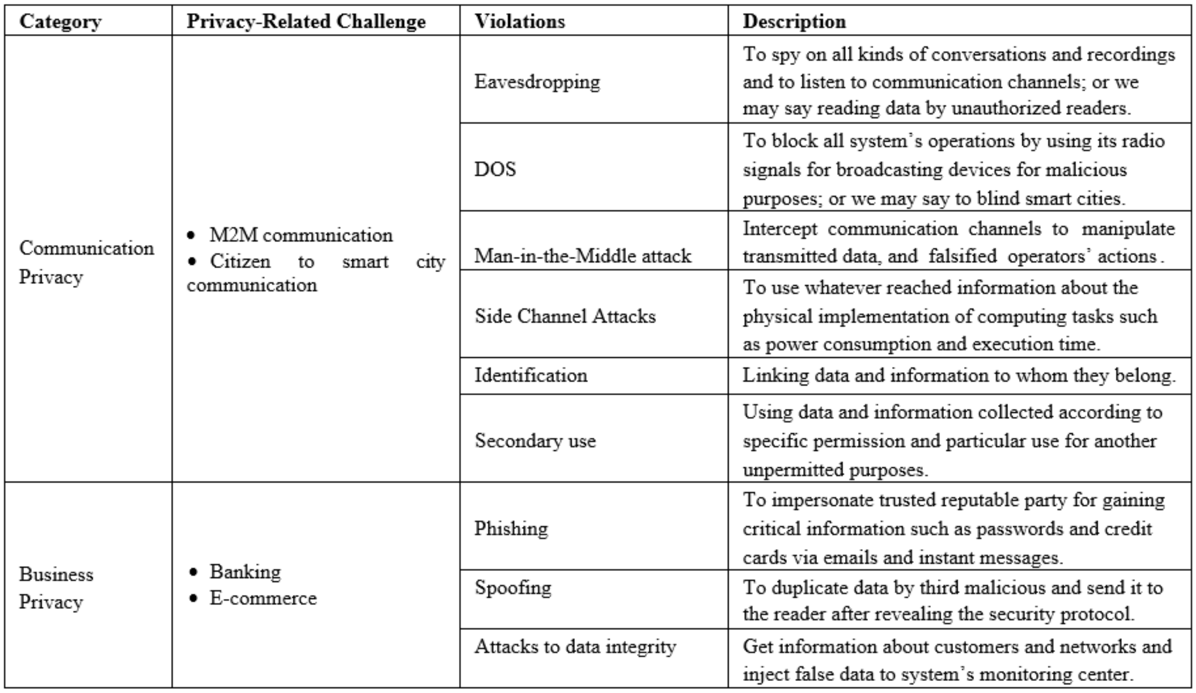
1. Home activities have the highest level of protection from hackers and intruders. The law and judicial system punish those who violate this kind of privacy.
2. Activities that extend outside the home will also be protected, however, the level of protection varies with the type of activity.
3. Public activities and activities that involve a third party will have a minimal to no protection. This is because privacy is absent in such activities.
4. Activities that are subject to public regulations will have lesser protection than public activities. This is because that these activities may be used by the government to gather the data; they need to enhance the operation of the smart city.
5. Activities that explicitly mention that data will be collected and analyzed during it.

Elmaghraby and Losavio (2013) found that in transportation, automobiles can be a major source of data, this is because cars nowadays have multiple systems such as the On-Board Diagnostic Computers (OBD 2), which can be used to gather data about the engine status and behavior, Event Data Recorder (EDR), it is a device that records and preserves a lot of information about the vehicle itself and the activities happened in side, and of course, the Global Positioning Satellite (GPS), that can be used to determine the location of the vehicle at any time. The data gathered by these systems may be considered dangerous if the wrong person has access to it. However, usually the owner of the vehicle has complete control over who accesses the data. Additionally, the law charges anyone who tries to break into these data. These data can be used to build interconnected systems to then achieve smart transportation. This can be accomplished by analyzing information such as: breaking points, acceleration, speed, and location to predict when an accident will happen and who will be the driver who is most likely to get into accidents. The data can also be used to monitor bad driving habits. However, as Elmaghraby and Losavio (2013) mentioned, doing so will raise many questions about the privacy and security of these passengers. This issue can be addressed by taking extreme legal and technical measures by the government, and by using the routine activities theory, which is a part of crime theory, to test information security, discover weaknesses, and suggest solutions to the IT team.

AlDairi and Tawalbeh (2017) intended to evaluate to provide an overview about major security violations in smart cities that are related to mobile technologies. They mentioned that a smart city must possess five important components: (1) state of art communication and information technologies, (2) services and infrastructure, (3) transportation management, (4) buildings, (5) the city as a whole. A smart city must incorporate all these aspects together, the mission of a smart city is to promote cooperation between the public and private sectors. A smart city must as well address the most important challenges that faces the world, such as: limited resources, and global warming. AlDairi and Tawalbeh (2017) also discussed the six dimensions of any smart city, and they are: (1) smart governance, (2) smart economy, (3) smart people, (4) smart mobility, (5) smart living, and (6) smart environment. From that, it is noticed that smart cities are huge entities that must always meet the changing needs of the people while also meeting the requirements on the social, economic, and political aspect. According to AlDairi and Tawalbeh (2017), this creates a lot of problems, one of them being privacy and security. The security issues involve protecting the data, servers, and networks from cyber-attacks, nevertheless, this is not an easy task because there are several obstacles that prevents security maturity in smart cities, one of the obstacles is, vendors who supply smart cities with their software and hardware products do not perform sufficient testing on cyber security. Another major obstacle is, in smart cities, the integration between all systems within the city is very much needed, however, this means a single attack on one of the systems will damage the whole process. After that, there are major issues in the current speed of response to problems in smart cities, which is also accompanied with issues and weakness in most recovery plans for most smart cities.

In the review of AlDairi and Tawalbeh (2017), multiple privacy issues have been discussed as well. Table 4 summarizes some of the major privacy violations in smart cities.

Table 4: Major privacy issues in smart cities.



Category	Privacy-Related Challenge	Violations	Description
Communication Privacy	• M2M communication • Citizen to smart city communication	Eavesdropping	To spy on all kinds of conversations and recordings and to listen to communication channels; or we may say reading data by unauthorized readers.
		DOS	To block all system's operations by using its radio signals for broadcasting devices for malicious purposes; or we may say to blind smart cities.
		Man-in-the-Middle attack	Intercept communication channels to manipulate transmitted data, and falsified operators' actions .
		Side Channel Attacks	To use whatever reached information about the physical implementation of computing tasks such as power consumption and execution time.
		Identification	Linking data and information to whom they belong.
		Secondary use	Using data and information collected according to specific permission and particular use for another unpermitted purposes.
Business Privacy	• Banking • E-commerce	Phishing	To impersonate trusted reputable party for gaining critical information such as passwords and credit cards via emails and instant messages.
		Spoofing	To duplicate data by third malicious and send it to the reader after revealing the security protocol.
		Attacks to data integrity	Get information about customers and networks and inject false data to system's monitoring center.

Baig et al. (2017) presents a comprehensive view of security in smart cities. This includes how to detect security threats and how to conduct a digital search in the context of the smart city depending on previous accidents to help in preventing the same accidents to happen in the future. The study conducted by Baig et al. (2017) will be based on four main keys, in which the authors think are the typical components in any smart city, and they are as follows: (1) Smart grids, (2) Unmanned Aerial Vehicles (UAV's), (3) Building Automation Systems (BAS), and (4) Smart Vehicles. Also, all necessary Internet of Things (IoT) sensors will be available such as: traffic level sensors, noise mapping sensors, and optimal route detection sensors.

In the review of Baig et al. (2017), the security issues in each of the four keys are investigated. Nowadays. Smart grids play a huge role in mitigating global warming and high energy demand. This is achieved by gathering data from the user about their energy consumption using smart meters, then, analyze the data to recognize energy consumption patterns and optimize the supply and demand. However, smart grids have multiple security issues related to data integrity, information privacy, and network accessibility. According to Baig et al. (2017), smart meters and IoT sensors are usually stored in insecure locations at their user's household, which make them easy to penetrate and hack. This is a very serious issue since it will put the entire smart gird at risk.

The second key in a typical smart city is Unmanned Aerial Vehicles (UAV's). It may be discussed that UAV's or drones are the most recent addition to concept of a smart city. New technologies have been used in the manufacturing of these drones which brought the price to as low as $250. Also, these drones have multiple features such as cameras and sensors. This makes drones very affordable and useful to individuals, who can use them is photography, recording videos, thermal sensing, and 3D interactive games. This also makes drones a very attractive option for a wide various of industrial applications. Drones may effectively be used in grocery delivery, packages and mail delivery, agriculture, and monitoring roads and coastlines. In the near future, it is expected to use drones for data collection in cities using IoT sensors. This data will then be communicated through a network to the city's database and information center. As mentioned by Baig et al. (2017), most drones nowadays use unsecured Wi-Fi connections which make them easier to interrupt and penetrate. Drones usually separated into two categories. The first being civilian-grade drones while the second is AR drone 2. Multiple studies Pleban et al. (2014) and Peacock (2014) shown the vulnerabilities in the two types of drones. Both drone types use unprotected connections between a smart device and the Linux system integrated in the drone. Finally, Pleban (2014) categorized drone vulnerabilities and weaknesses into two groups, communications risks, and device level risks.

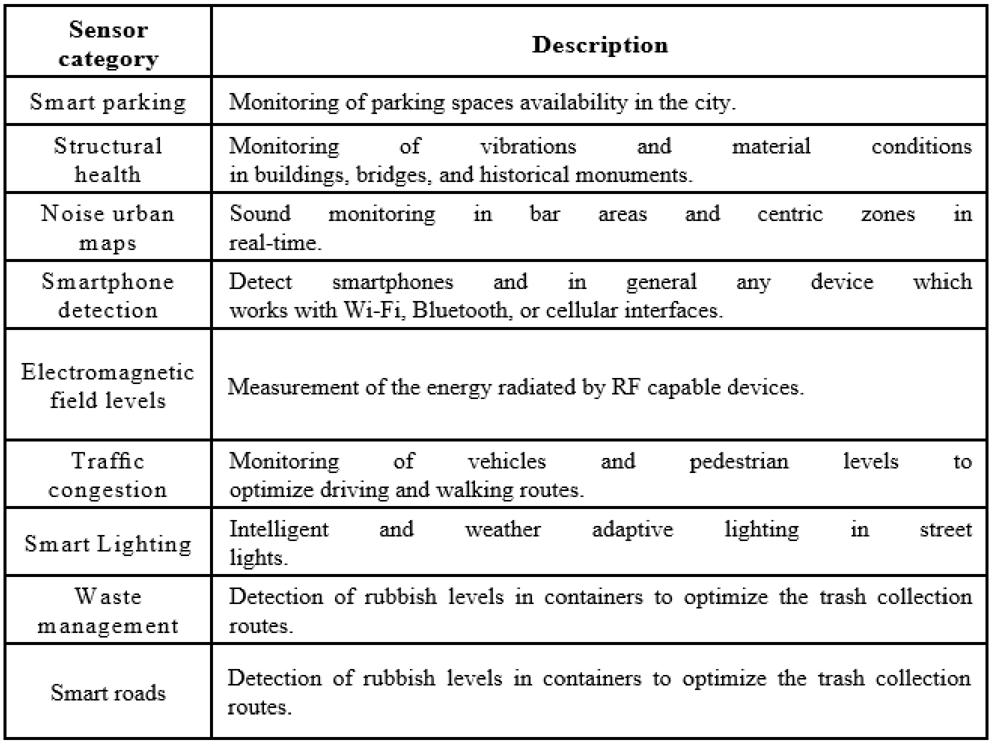
Moving on, smart buildings are a very critical part in smart cities, as a result, Building Automation Systems (BAS) are used. BAS accomplishes a very critical task, which is integrating all services inside a building (or multiple buildings) into a common network. Usually, the building services where BAS is used include lighting, elevators, water pumping, energy systems, surveillance cameras, and heating-ventilation air-conditioning (HVAC) systems. Connecting all these servers into a shared network provides efficient monitoring and control of all the building's systems at once. Nonetheless, this may lead to catastrophic results if this shared network is hacked. As highlighted by Baig et al. (2017), continuous handling of BAS would significantly help in preventing cyber-attacks.

After that, conventional vehicle networks nowadays already integrated GPS and other consumer-based devices in their network. This is due to the current development of the systems inside the car and due to the increase of entertainment systems inside the car. However, according to Lin and Sangiovanni-Vincentelli (2012), a fully smart vehicle must utilize a higher bandwidth protocol. Smart vehicles use developed systems such as OBD 2 and EDR to collect data and communicate them to stations located on the side of the road. This data is very useful to detect robbery as it occurs. Nonetheless, there is a main security issue with smart vehicles. Latest surveys show that more than 50% of risk assessment managers in different companies identified cyber-security of smart, self-driven vehicles as their number one concern. Other major threats that currently faces smart vehicles, and also might face them in future are also mentioned in Baig et al. (2017). These threats can be grouped into five groups.

1. Physical threats, such as using glitches to obtain unauthorized data from the vehicle, and using channels to leak information for illegal use.
2. Abuse threats, such as taking unauthorized control of the vehicle and using malicious firmware to get illegal access to the vehicle.
3. Interception threats, such as having a middleman to help gaining unlicensed data from the vehicle.
4. Data threats, such as lose of information from the vehicle as well as information leakage from the vehicle after selling it.
5. Malicious code, this is a very dangerous threat. It includes the execution of malicious code to run against the infotainment system to comprise all connected systems and devices to the vehicle.

Lastly, IoT refers to all smart devices, vehicles, and sensors connected to the server or to the network. Such devices have become crucial to smart cities in general. As Baig et al. (2017), they are usually maintained and used to monitor different phenomena and areas in smart cities. They can also be used to respond to different scenarios that might occur in the city's environment. Table 5 summarizes the most common IoT sensors in smart cities.

Table 5: Common IoT sensors in smart cities.



Sensor category	Description
Smart parking	Monitoring of parking spaces availability in the city.
Structural health	Monitoring of vibrations and material conditions in buildings, bridges, and historical monuments.
Noise urban maps	Sound monitoring in bar areas and centric zones in real-time.
Smartphone detection	Detect smartphones and in general any device which works with Wi-Fi, Bluetooth, or cellular interfaces.
Electromagnetic field levels	Measurement of the energy radiated by RF capable devices.
Traffic congestion	Monitoring of vehicles and pedestrian levels to optimize driving and walking routes.
Smart Lighting	Intelligent and weather adaptive lighting in street lights.
Waste management	Detection of rubbish levels in containers to optimize the trash collection routes.
Smart roads	Detection of rubbish levels in containers to optimize the trash collection routes.

Hamid et al. (2019) conducted a survey to determine the major security and privacy issues in smart cities concerning socio-economic, governance, and technological aspects. Talking about the socio-economic aspect, smart cities provide multiple services to enhance the citizen’s experience in the field of health care, banking, transportation, and communication. However, there are few challenges to be addressed in each of the previously mentioned fields. For example, in the healthcare sector, hospitals usually use a social network provided by a vendor. Some of these social networks have known weaknesses that might be exploited by hackers to get unauthorized and sensitive information about the patients. Moving on to the banking and financial aspect, it is extremely important to improve the banking experience for smart cities citizens because this allows more economic growth for the city itself. Nevertheless, this is also known as the most vulnerable aspect in a smart city, which of course provides an opportunity for thieves and invaders. In transportation, smart devices are used to control traffic and enhance the traffic flow around the city, but there might be severe consequences if such system is hacked, such as accidents, traffic jams, and stealing of vehicles. In a smart city, communication is considered a very important aspect, however, there are many common weaknesses in the networks, and connections. The second important aspect considered by Hamid et al. (2019) is the governance aspect. Cyber-security problems in this aspect can categorized into two groups, some may happen the management system and some may occur in collaborative & transparent governments. The main issue systems management is concerning the developers themselves; they tend to focus more on the tools and neglect the cyber-security part of it. On the other hand, in collaborative and transparent governments, the used systems are always at risk, because if hacked, disasters will happen. The third and final aspect discussed by Hamid et al. (2019) is the technological aspect. There are many technologies used in a smart city that are vulnerable to cyber-attacks, such as RFID systems, biometrics systems, smart networks, and smartphones. A cyber-attack on any of those systems will lead to many huge problems such as the leakage of private information.

Mohamed et al. (2020) investigated the benefits of smart cities over traditional cities while also discussing the advantages of using data-driven decision-making tools to identify challenges in smart cities. Mohamed et al. (2020) also discussed the challenges of applying data-driven decision-making approaches in identifying security problems in smart cities. The use of data-driven cyber security in smart cities will help in securing critical information related to the city’s applications. Any application in a smart city, no matter how small or how big, will consist of different components that are connected using a public or a special network. Ensuring that all components are safely protected from cyber-attacks is a necessity for a smooth operation of any smart city. Using data-driven cyber security in smart cities has a lot of benefits in the form of: (1) Fast security incident analysis, (2) Improving the security management processes, (3) Improving security protection mechanisms, and finally, (4) Using the collected data to create simulations and optimization models in order to enhance the defense mechanisms in smart cities. After that, Mohamed et al. (2020) mentioned that data-driven cyber security has multiple applications in smart cities, in which these applications are categorized into four groups, as follows:

1. Collaborative threat identification, usually such applications require monitoring and handling different security circumstances at once.
2. For enhancing the security systems management and structure. In this application, the data-driven cyber security is used to study the current management model and structure and optimize it.
3. For forecasting future cyber-attacks using the data from the past along with current data. This application depends heavily on using Artificial Intelligence (AI) and machine learning to create a reasonable forecast. This application can help a lot in reducing the damage from cyber-attacks and in some cases avoiding the cyber-attack.
4. For planning and enhancing security practices and systems in smart cities. The collected data is used to investigate the current security system will searching for weaknesses and opportunities of improvement.

3.2 Solutions to Security and Privacy Issues in Smart Cities

Many cities around the world opted to use Information and Communication Technologies (ICT) in their infrastructure. These cities are leading the transition from traditional cities into becoming smart cities. The objective of this transition is to make the citizen’s life easier by enhancing the quality of all services provided by the city, while this might be a noble goal, there are few obstacles standing in the way. A major issue is handling security and privacy issues that would arise from this transition. This section discusses few security and privacy solutions found in literature.

Smart cities usually contain several components, ensuring that all components are secured and protected necessary for the whole smart city to function efficiently. In the review of Khatoun and Zeadally (2017), security solutions in all smart city's components are discussed along with privacy protection protocols. According to Khatoun and Zeadally (2017) Industrial Control Systems (ICS's) are widely used in smart cities infrastructures. Some supervising tools are designed to work with ICS's, a popular one of them is SCADA. SCADA has several hardware components such as Programmable Logic Controllers (PLC), networks, Remote Terminal Units (RTU's), processors. These devices are controlled using specific protocols within SCADA, such as Distributed Network Protocol (DNP3), and Modbus. DNP3 is a very popular communication protocol certified by the IEEE for electric power systems, and Modbus is widely used communication tool in industries. The issue is security has not been taken into consideration when these protocols are initially designed. This opens the gap for cyber-attacks on SACDA systems, which lead to catastrophic outcomes. Lately, the DNP3 and Modbus protocols are updated by adding pre-processors to detect hackers and invades. Fovino et al. (2012) used the critical state distance, which is a measure of the distance between the current profile and the critical profile, to design a new fire-wall architecture for systems that use DNP3 and Modbus protocols.

Smart building is a very critical component in smart cities. Usually, different building's components such as elevators, lightning, water pumping, and heaters are interconnected into a single network. This allows easier management of the building, however, makes it easier to hack and disrupt. There are several communication protocols used in smart cities, such as BACnet, a communication protocol for control networks and building automation, and KNX, a communication protocol for smart buildings that is based on Open System Interconnection (OSI) network. Both of these protocols are ISO certified, nonetheless, both of them didn’t take cyber-security into consideration. To improve cyber-security in smart building there are four important characteristics to address, and they are as follows:

1. Technical aspect: using physical protection for security equipment, applying WPA2 protocol for any wireless network, securing remote accesses with VPN, deploying firewalls at every transition point, and using authentication, authorization, and accounting (AAA) servers such as RADIUS server. There are few standards that can be used to enhance cyber-security in this aspect such as ANSI/TIA-862, and ASHRAE standard.
2. Organizational aspect: manage and organize passwords, define rules and standards for citizens, create recovery plans, and allow feedback sessions for the citizens. The standards to follow to improve cyber-security in this aspect are: The five best practices to improve Building Management System (BMS), and IET standards for cyber security technologies in the built environment.
3. Human aspect: Alarm citizens whenever a crisis occurs, raise awareness about the importance of cyber-security, and use continuity plans.
4. Legal aspect: Use good ICT practices, use safety standards specified by the national cyber-security agencies, and respect legal aspects of security.

Khatoun and Zeadally (2017) specified e-governments as the third component in any smart city. It is all about using ICT tools to connect all government institutions together. According to the European report of the Science & Technology Options Assessment (STOA) project, new Eleven security policies were introduced in e-governments.

E-health is the fourth component in smart cities. It allows the country to face medical crises using information systems to monitor and make decisions. Networks such as the Wireless Body Area Networks (WBAN) are used to improve the security and privacy of patients. However, these networks have some difficulties dealing with hackers and intruders. One of the best solutions in terms of security is moving the data of all patients into a third-part cloud, however, this solution raises serious privacy questions. As a result, homomorphic encryption can be used since it allows modification of the encrypted data without decrypting it. Thus, homomorphic encryption sounds like the most suitable solution while taking security and privacy into consideration. This is because the data hosted by the third-party's cloud is impenetrable by the provider during data transmission or processing.

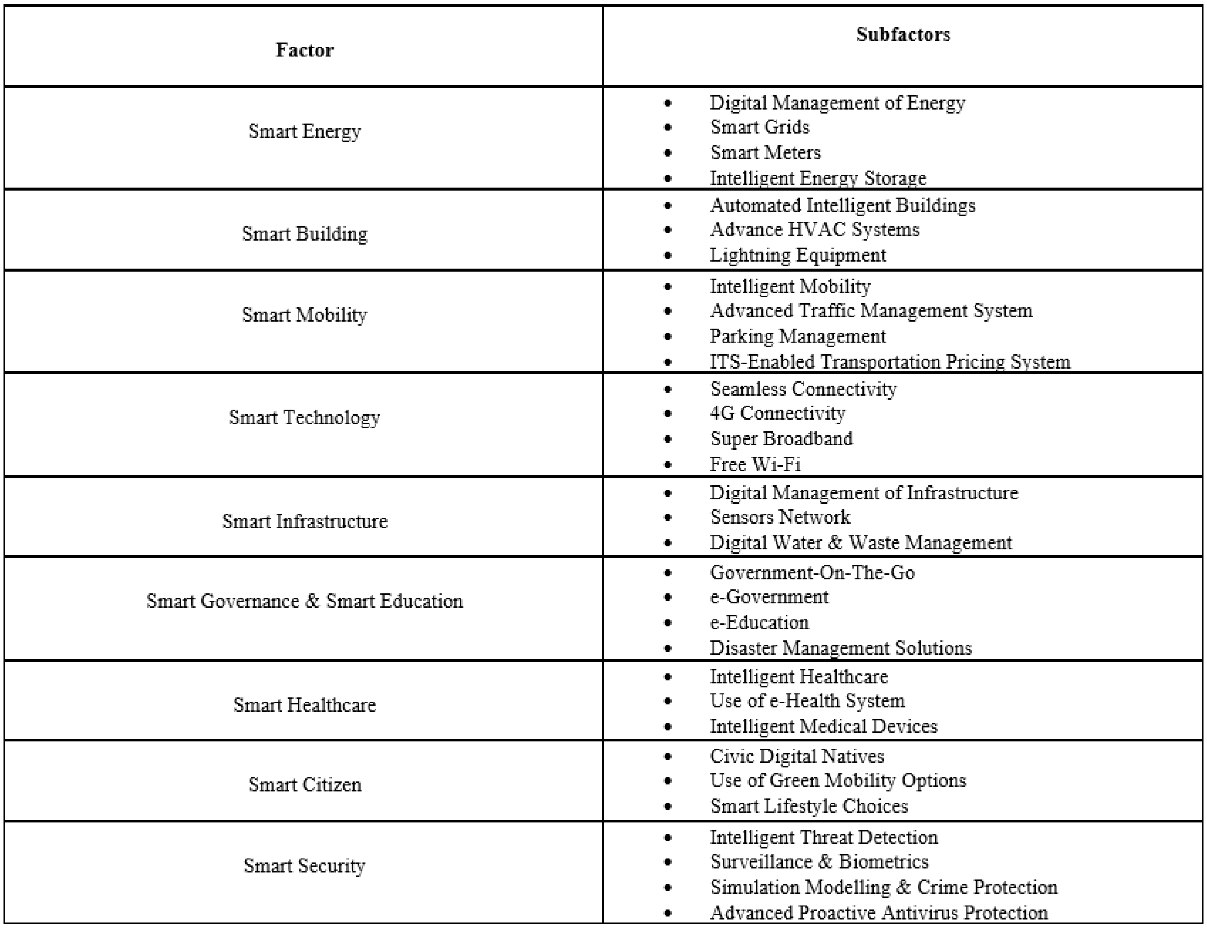
Khatoun and Zeadally (2017) also discussed privacy solutions in smart cities. Smart cities provide a lot of benefits to its citizens; however, privacy was and still always a problem. Citizens want their needs and rights always fulfilled and guaranteed. Most smart cities services are using ICT, as a result, users with less familiarity with such systems such as elderly are considered a perfect target for attacks and frauds. A major privacy issue in smart cities appears with the increase usage of smart vehicles. Such vehicles have a lot of devices and communication tools such as the GPS, RFID, Bluetooth, and electronic tolls systems, also the vehicle will be connected to many devices to track and record data about the driver's driving behavior. With such a huge amount of collected data, individuals start to ask questions about this data is being used. As Khatoun and Zeadally (2017) highlighted, there are three main operations in any information technology system, data transfer, data processing, and data storage. Privacy issues may arise in any of the three operations. Martinez and Solanas (2011) introduced the Where, Who, and What privacy model, which is called the 3W's model. This model is to be applied in location-based services. Spiekermann and Cranor

(2008) introduced a three-layer model that promotes building privacy and friendly systems. David et al. (2015) relied on linear algebra concepts such as matrix multiplications to obtain the correlation between distributed datasets from linear systems. This is a very efficient and secure solution; however, it can’t be used in large scale systems. The issue in all these solutions is that the privacy techniques used don’t consider few important constraints such as the reliability of the third-party cloud, and members circulation. Followed by that, Khatoun and Zeadally (2017) talked about how legislation is important to preserve privacy. The British parliament (2015) initiated a project in which smart services are allowed to get unlimited access to user’s data. This allows the police to hack any device, smartphone, or a computer if they needed to. However, big conglomerates such as Facebook, Twitter, and Microsoft disapproved the project.

3.3 A Framework for Assessing Cyber-Security Challenges in Smart Cities

As mentioned earlier, there are many factors and areas in a smart city. Each of these areas is affected by cyber-security issues in a different manner when compared to any of the other areas. Belgaum et al. (2018) gathered data from surveys and experts’ opinions about nine factors that are affected by cyber-security issues. After that, the data is analyzed using Fuzzy Analytical Hierarchy Process (FAHP) method to find the weight and rank of each factor. A factor with a higher weight indicates that it is more affected by cyber-security challenges than other factors with less weight. As per the novel model provided by Belgaum et al. (2018), there are nine main factors that are influenced by cyber-security issue, and each factor can be subcategorized into three to four subcategories. The nine factors and their subcategories are shown in Table 6.

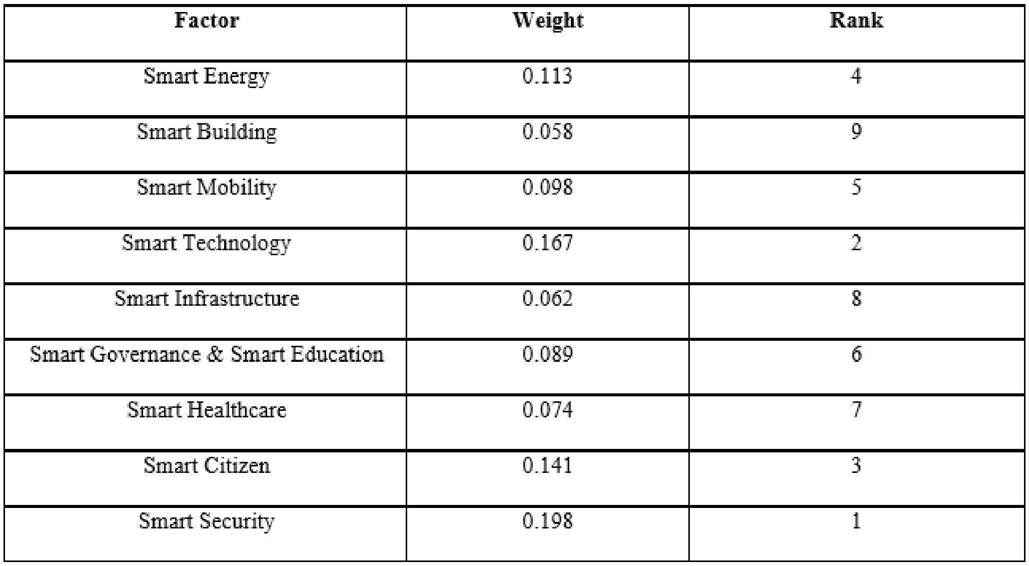
Table 6: The nine factors and their sub factors.



Factor	Subfactors
Smart Energy	• Digital Management of Energy • Smart Grids • Smart Meters • Intelligent Energy Storage
Smart Building	• Automated Intelligent Buildings • Advance HVAC Systems • Lightning Equipment
Smart Mobility	• Intelligent Mobility • Advanced Traffic Management System • Parking Management • ITS-Enabled Transportation Pricing System
Smart Technology	• Seamless Connectivity • 4G Connectivity • Super Broadband • Free Wi-Fi
Smart Infrastructure	• Digital Management of Infrastructure • Sensors Network • Digital Water & Waste Management
Smart Governance & Smart Education	• Government-On-The-Go • e-Government • e-Education • Disaster Management Solutions
Smart Healthcare	• Intelligent Healthcare • Use of e-Health System • Intelligent Medical Devices
Smart Citizen	• Civic Digital Natives • Use of Green Mobility Options • Smart Lifestyle Choices
Smart Security	• Intelligent Threat Detection • Surveillance & Biometrics • Simulation Modelling & Crime Protection • Advanced Proactive Antivirus Protection

After that, the FAHP approach is applied to obtain the weight of each factor and sub factor. The weight represents how the factor or sub factor is influenced by cyber-security challenges. Table 7 summarizes the weight and ranks of each main factor.

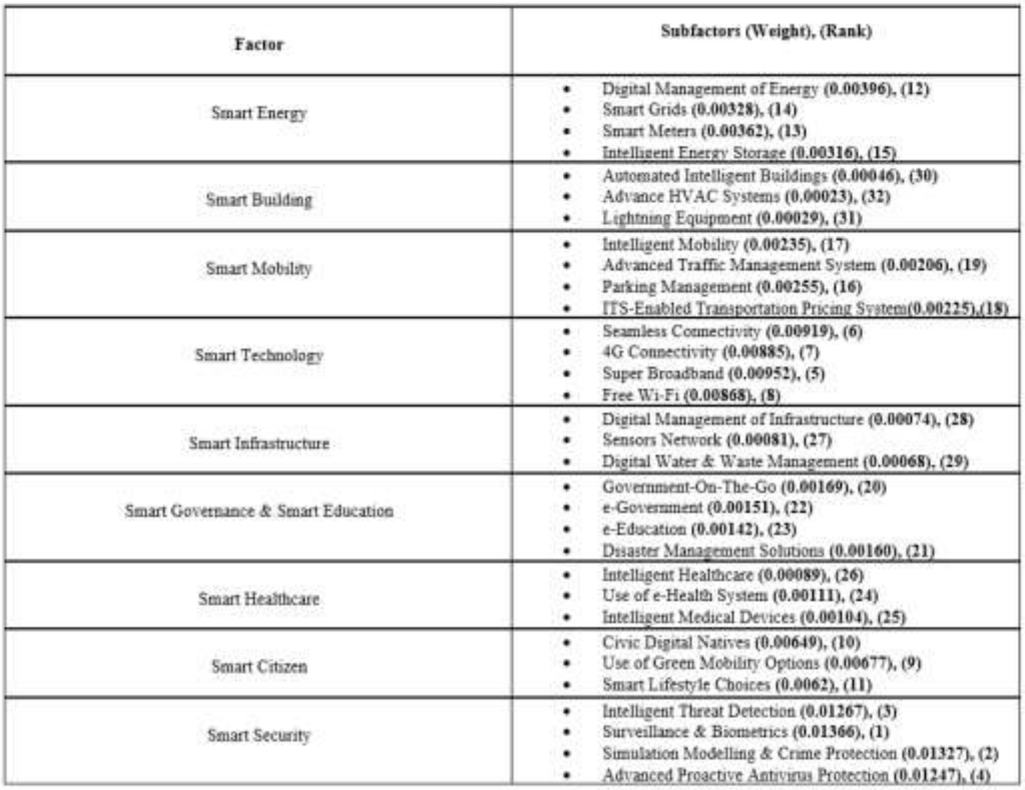
Table 7: The weight and rank of the nine factors.



Factor	Weight	Rank
Smart Energy	0.113	4
Smart Building	0.058	9
Smart Mobility	0.098	5
Smart Technology	0.167	2
Smart Infrastructure	0.062	8
Smart Governance & Smart Education	0.089	6
Smart Healthcare	0.074	7
Smart Citizen	0.141	3
Smart Security	0.198	1

Then, the weight of each of the sub factors presented in Table 3 is identified. This is needed to determine the sub factor responsible of the highest influence on the main factor in terms of getting affected by cyber-security issue. Table 8 represents the weight the rank of each of the sub factors.

Table 8: The weight and rank of all sub factors.



Factor	Subfactors (Weight), (Rank)
Smart Energy	• Digital Management of Energy **(0.00396), (12)** • Smart Grids **(0.00328), (14)** • Smart Meters **(0.00362), (13)** • Intelligent Energy Storage **(0.00316), (15)**
Smart Building	• Automated Intelligent Buildings **(0.00046), (30)** • Advance HVAC Systems **(0.00023), (32)** • Lightning Equipment **(0.00029), (31)**
Smart Mobility	• Intelligent Mobility **(0.00235), (17)** • Advanced Traffic Management System **(0.00206), (19)** • Parking Management **(0.00255), (16)** • ITS-Enabled Transportation Pricing System**(0.00225),(18)**
Smart Technology	• Seamless Connectivity **(0.00919), (6)** • 4G Connectivity **(0.00885), (7)** • Super Broadband **(0.00952), (5)** • Free Wi-Fi **(0.00868), (8)**
Smart Infrastructure	• Digital Management of Infrastructure **(0.00074), (28)** • Sensors Network **(0.00081), (27)** • Digital Water & Waste Management **(0.00068), (29)**
Smart Governance & Smart Education	• Government-On-The-Go **(0.00169), (20)** • e-Government **(0.00151), (22)** • e-Education **(0.00142), (23)** • Disaster Management Solutions **(0.00160), (21)**
Smart Healthcare	• Intelligent Healthcare **(0.00089), (26)** • Use of e-Health System **(0.00111), (24)** • Intelligent Medical Devices **(0.00104), (25)**
Smart Citizen	• Civic Digital Natives **(0.00649), (10)** • Use of Green Mobility Options **(0.00677), (9)** • Smart Lifestyle Choices **(0.0062), (11)**
Smart Security	• Intelligent Threat Detection **(0.01267), (3)** • Surveillance & Biometrics **(0.01366), (1)** • Simulation Modelling & Crime Protection **(0.01327), (2)** • Advanced Proactive Antivirus Protection **(0.01247), (4)**

3.4 A Case Study of Cyber Security in Smart Cities: Dubai

Efthymiopoulos (2016) provided a detailed study about how cyber-security is applied in the city of Dubai, in the United Ara Emirates (UAE). Dubai is leading city in terms of innovation, trading, technology, and management. Dubai is considered as a role model when it comes to modern and futuristic economical and socio-political structures. In 2014, His Highness Sheikh Mohammed Bin Rashid Al Maktoum, the Vice President and Prime Minister of the UAE and the ruler of Dubai, founded the Dubai center of e-Security. The center is aimed to provide technical support immediate response to all governmental entities in Dubai the center is also responsible for keeping all citizens, residents, and tourists in Dubai safe. This includes protecting their privacies and secure all their applications. The framework Dubai follows requires coordination and cooperation between governmental departments, and cyber-crime protection mechanisms. The framework also includes raising awareness and spreading knowledge about how serious cyber-security is in all educational levels. The center would create strategic plans and stand against any threat that might affect the smooth operation of the city. This happens by securing all governmental authorities, businesses, organizations, and institutions. This allows securing all grid networks whether it is a communication network or not. It can be noticed from the experience of Dubai that current and future challenges requires flexibility, agility, and accurate forecasting. Efthymiopoulos (2016) proposes that the e-Security center should work on providing a better e-Environment by enabling a complete protection of the city as a strategic plan using authorized and accredited approaches based on the recent decree. Anyhow, it is expected that smart cities, which they are 26 cities as in 2016, and Dubai is among them, are expected to become shareholders in a global revenue-sharing market. This global revenue-sharing market is expected to be valued at $3.3 trillion by 2025.

3.5 Research Gap

Smart cities rely on providing an easier, healthier, and more productive lifestyle to its citizens and residents. However, the concept of a smart city is relatively new, and face a lot of challenges still to be addressed. It is observed from the previous literature review that a lot of efforts are spent to determine the cyber-security and privacy challenges that face smart cities in all its components and areas. However, up to this day, not many solutions to these issues have been proposed. As a result, most smart cities in the world are still suffering from these issues. It is also noticed that studies that evaluate the security and privacy challenges in the GCC countries in general and in the UAE specifically are very minimal. This is a very obvious gap in literature. This thesis will assess the security and privacy issues in UAE. Table 9 provides a summary of the existing literature.

Table 9: Summarized literature review.

Existing Literature	Author(s)	Contribution
Current & Future Challenges Facing Smart Cities	Elmaghraby & Losavio (2013)	Studied security and privacy problems is smart cities, and developed a model to show the interaction between people and servers.
	AlDairi & Tawalbeh (2017)	Provided an overview about security and privacy challenges in smart cities, showed factors affecting information security in smart cities.
	Baig et al. (2017)	Studied the four keys of a smart city, and provided a security overview in smart cities while determining the threats.
	Hamdi et al. (2019)	Discussed core security and privacy issues in smart cities, and explained some weaknesses and vulnerabilities in smart cities while providing few recommendations.

	Mohamed at al. (2020)	Used data-driven cyber security methods to assess security issues in smart cities, and discussed few challenges in using data-driven cyber
Solutions to Security & Privacy Issues in Smart Cities	Spiekermann & Cranor (2008)	Introduced a three-layer model to promote building privacy and friendly systems.
	Martinez & Solanas (2013)	Developed the Who, Where, and What (3-W's) privacy model that depends on location-based services.
	David et al. (2015)	Used linear algebra concepts such as matrix multiplications to obtain the correlation between distributed datasets from linear systems.
	Khatoun & Zeadally (2017)	Discussed the concept of smart cities while explaining major security and privacy weaknesses, then provided multiple solutions for each aspect of the problem.
Framework For Assessing Cyber-Security Issues in Smart Cities	Belgaum et al. (2018)	Identified nine main factors to be affected by cyber security issues in smart cities, then used the Fuzzy Analytical Hierarchy Process (FAHP) to identify which of the nine factors is the most affected by security

		problem. Each factor has subfactors that were also studied by FAHP.
Case Study of Cyber-Security in Smart Cities: Dubai	Efthymiopoulos (2016)	Investigated how Dubai become a hub for innovation, strategic technology planning, and management, also discussed the strategic security elements that made Dubai a secured smart city while being a smart networked infrastructural service provider.

Chapter 4: Research Methodology

4.1 Study Design

Research is roughly interpreted as knowledge exploration. It is a systematic and scientific method to pursue information regarding a particular subject. Thus, it is an art of systematic investigation as its main objective is to obtain more information. Researchers have identified several types of approaches, these research approaches include descriptive, analytical, essential and applied research (Amrhein et al. 2019). Selecting the appropriate study design is the most significant decree to make while deciding the methodology of a certain study. This decision will determine the way of conducting the study, sampling and data analysis in particular (dos Santos Silva, 1999).

It is important to note that different study designs are categorized under either qualitative or quantitative research. However, for the focus of our study, the types of study design under quantitative research will be discussed, mainly, descriptive and analytical. The descriptive design of study is suitable for basically depicting the features or characteristics of the study sample. For example, a specific group of the study subjects exhibits a certain set of skills because of something in common, such as the level of education. This type of study design might also attempt to generalize the results to a targeted population from a representative sample, and only a solitary sample exists, without any comparison group. Meanwhile the analytical research compares two or more samples and follows the changes over a period of time (Omair, 2015). This type of study design focuses on cause and effect, as if the study is intended to look into why and how a specific characteristic has been exhibited by the samples that are being studied (McLeod et al. 2016). By referring the research questions, which are:

1- What are the main information security challenges that are faced by the organizations of Dubai and Abu Dhabi?

2- To what extent are the organizations of Dubai and Abu Dhabi prepared to detect, prevent or respond to information security threats?

3- Do we have the needed knowledge to protect ourselves enough?

Moreover, based on the gap presented in chapter 3, the quantitative method and the descriptive study design were selected, as this study is intended to answer what are the characteristics of the sample in this study. That are, the challenges of information security in the smart cities of the United Arab Emirates, the level of readiness in a case of a cyber-attack, whether the participants are equipped with the sufficient knowledge in cyber security and if a framework exists that could assist organizations/governments of smart cities to help reduce the risk of cyber-attacks.

4.2 Questionnaire Design and Data collection

The process of data collection begun with the design of the questionnaire, as well as the reviewing secondary resources. The questionnaire that was adopted for this study was proposed by Leach and Dana (2016). It has been modified to accommodate the situation of our study, and consists of twenty-two items about information security challenges and threats faced by residents and employees of smart cities, Breach readiness, risk management strategies, crisis communication and individuals' level of security in multiple areas such as e-mail security, cloud migration process, mobile computing etc. The questionnaire also contained several items to collect demographic data about the respondents, it was constructed using google forms (online survey), and it was sent to participants through social media platforms, a copy of the survey has been appended to the dissertation in the appendix section. The answers to the questionnaire items consisted of checkboxes, where there is a need to select more than one response, such as the case of types of security threats, multiple choice questions with a scaled response from 1 “inadequately prepared” to 5 “extremely well prepared”. In addition, the option “Not Applicable” was added since some areas of cyber-activities are not utilized by every organization. Furthermore, in addition to the reasons mentioned in section 4.1, the method of collecting data through a questionnaire was selected since it is time efficient, less expensive, more effective and easier to conduct. The process of data collection is the most critical part to any study as it forms its core and enables the researcher to draw the conclusion and contribute to the literature. By referring to the research questions and considering the nature of this study, two sources have been considered, primary data source, which is the data obtained from the respondents from the questionnaire, and a secondary source, which is the literature. The utilization of the literature is essential as it underpins the main theory of this study.

4.3 The Criteria’s of Choosing Participants

The participants to the study were chosen under the following criteria’s:

1- Participants are required to be residing in the United Arab Emirates.

2- Participants are required to be employed in either Dubai or Abu Dhabi, irrelative if they were employed in a public or private sector.

3- Participants are required to have relevant experience.

4.4 Study Community and Sample Size

The targeted population includes residents, employees, managers and executives of organizations of Dubai and Abu Dhabi. It is estimated that there are 2.5 million employees in Dubai and (Puri-

Mirza, 2020a) and 1.7 million in Abu Dhabi (Puri-Mirza, 2020b). According to Alsyouf (2021), the minimum sample size could be estimated utilizing equation (1).

$$n = \frac{N}{1 + N(e^2)} \qquad (1)$$

Where N is the size of population, n is the sample size and e is the error margin. Since the population size is estimated to be 4.2 million, and error margin is set to 10% for this study, the minimum sample size is calculated to be ~ 100 responses. Thus, the needed number of responses is required to be greater than or equal to hundered in order for this study to be representative of the targeted population.

4.5 Analyzing the Data

After receiving enough responses of the questionnaire, as mention in section 4.4, the data obtained from these responses are ought to be analyzed through software packages, the selected software for this purpose is IBM's SPSS version 26, and Minitab 19. Questions with "checkboxes" type of answers will be calculated and represented as a clustered bar graph to demonstrate the percentages of respondents' selected answers. These questions are question one, two, six, twelve, fourteen, eighteen, nineteen and twenty. Other types of the questionnaire's responses will be reflected on a Likert scale. These responses will be given weights ranging from 1 to 5, based on the least favorable outcome to most favorable outcome, respectively. For example, question four, seven, ten and eleven responses' range from "inadequately prepared" to "extremely well prepared". Regarding items with multiple answers, such as question three, will have a Likert scale that is based on the same criteria that has been mentioned earlier. The responses to question three are "No attacks at all in the past two years.", which is the most favorable outcome, will be given a score of 5, next response is “Fewer attacks than two years ago”, which will be given a score of 4. Next response is “Same number of attacks as two years ago”, which will be given a score of 3. Next response is “More data attacks than two years ago”, which will be given a score of 2, and lastly, “We are under constant attacks these days”, which will be given a score of 1 since it is the least favorable outcome. Hypothesis testing will be performed to validate whether organizations are prepared to detect, prevent and respond to cyberthreats, as well as whether individuals have enough cybersecurity awareness. Hypothesis testing will be performed on items 7, 10 and 11 to assess the originations’ preparedness to detect, prevent and respond to several cyber-threats. Additionally, hypothesis testing will be performed on item 9 to evaluate the level of cyber-security awareness among participants.

4.6 Research Protocol

The current study is willing to investigate the information security management for cyber-security challenges in smart cities, Dubai and Abu Dhabi in particular. It is critical to identify the risks associated with the move towards a smart city and implementing its underpinning technologies. Therefore, this study attempts to call attention to the main cyber-security threats, in addition to the extent of readiness of detection, preventing and responding to such threats, as well as measuring the security awareness among the people of Dubai and Abu Dhabi. With the focus on developing an understanding of the previously mentioned parameters, a sample of at least 100 responses will be selected for analytical analysis. The survey targets people who are currently employed in Dubai and Abu Dhabi, from both of the private and public sector. All of the questions presented in the questionnaire will be close-ended and the data is planned to be collected within a span of one month.

4.7 Research Ethics

It is of paramount importance to consider research ethics while performing the study because it is concerned with the participant’s privacy. The participants are ought to be informed about the study’s techniques and how their data will be processed, as well as any risk that could be accompanied with the process of gathering/processing the data. The questionnaire designed for this study states at the beginning that the data will solely be used for research purposes, and their data will indefinitely remain confidential. The participants are reassured that their data is stored in a password protected electronic format, and the questionnaire will not contain any information that will personally identify the respondents. The participation to this questionnaire is voluntary and it is up to the respondents to participate in the study, and the participant has the right to withdraw at any time.

Chapter 5: Results

A total of 103 valid responses were collected over the span of three weeks, after which, no further responses were received. As mentioned earlier in this research, this questionnaire consisted of 29 items, seven of which were concerned with demographics. The other 22 items were concerned with the subject of the study, which is cybersecurity challenges in smart cities.

5.1 Demographics

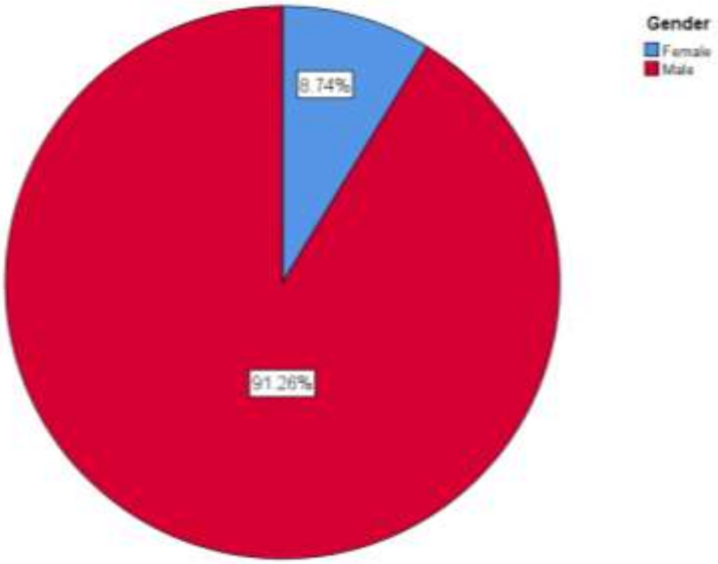


Figure 5: Gender distribution.

Figure 5 demonstrates the distribution of the respondents based on their gender, the questionnaire revealed that 91.26% of the respondents were males and 8.74% were females. It is worth noting that the number of female respondents was too low to perform gender based comparison among the study's main focal points.

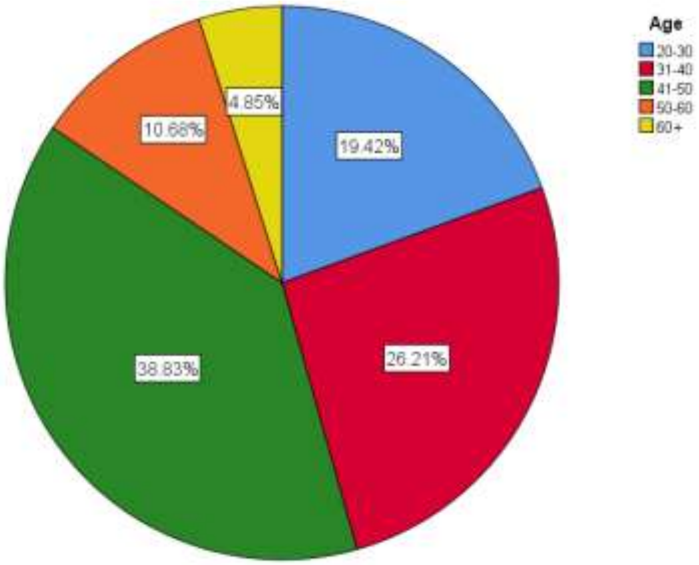


Figure 6: Age distribution

Figure 6 illustrates the age distribution among the respondents, it shows that 40 (38.8%) respondents are between the ages of 41 to 50 years old, 27 respondents (26.2%) are between 31 to 40 years old, 20 respondents (19.4%) are 20 to 30 years old, 11 respondents (10.7%) are between the ages of 51 to 60 years old and 5 (4.9%) are above the age of 60.

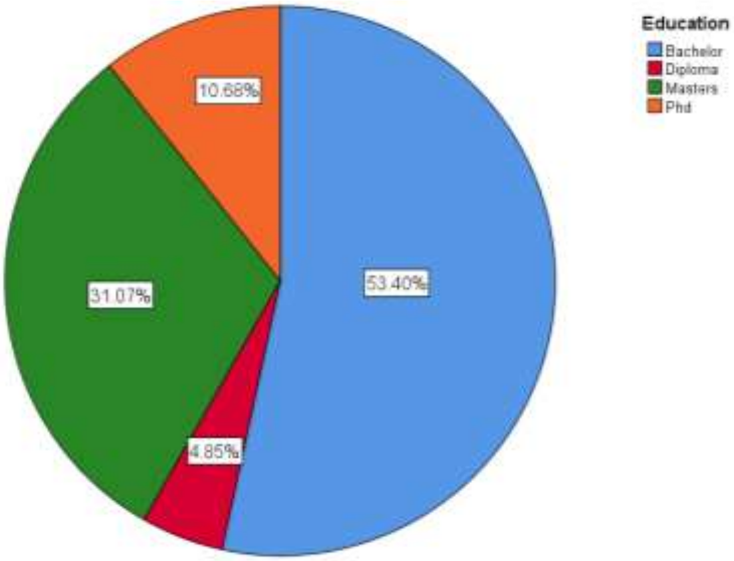


Figure 7: Education distribution.

Figure 7 is concerned with education distribution, it is prominent from the chart that 55 (53.4%) respondents got a Bachelor degree, 32 (31.07%) of the sample got a master's degree, 11 respondents (10.68%) got a PhD degree and 5 (4.9%) got a diploma degree.

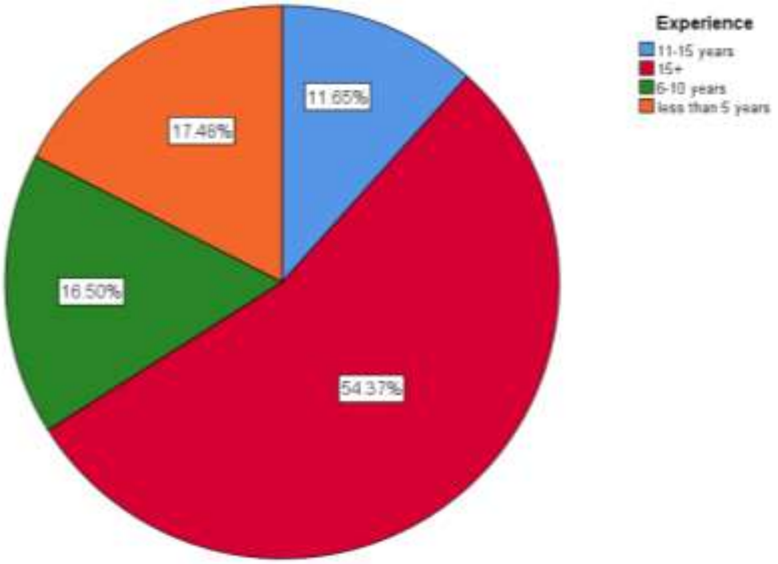


Figure 8: Experience distribution.

Figure 8 shows the years of experience of the respondents, it shows that 56 respondents (54.37%) have an experience above 15 years, 18 respondents (17.46%) got an experience between 0 to 5 years, 17 respondents (16.5%) have 6 to 10 years of experience and 12 respondents (11.7%) have between 11 and 15 years of experience.

Table 10: Specialization distribution

Specialization

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Accounting	1	1.0	1.0	1.0
	Allied health professional	1	1.0	1.0	1.9
	Artificial intelligence or machine learning	5	4.9	4.9	6.8

Big data	5	4.9	4.9	11.7
Blockchain technology	1	1.0	1.0	12.6
Construction	7	6.8	6.8	19.4
Designer tools and surveys	1	1.0	1.0	20.4
Document management solutions	1	1.0	1.0	21.4
◌́Energy	1	1.0	1.0	22.3
Engineering	1	1.0	1.0	23.3
Engineering Design	1	1.0	1.0	24.3
Factory work	1	1.0	1.0	25.2
Finance	1	1.0	1.0	26.2
General trading products	1	1.0	1.0	27.2
Home automation	1	1.0	1.0	28.2
Information Security (IS)	4	3.9	3.9	32.0
Information Technology (IT)	22	21.4	21.4	53.4
Internet of Things (IoT)	2	1.9	1.9	55.3
Manufacturing	2	1.9	1.9	57.3
Mechanical engineer	1	1.0	1.0	58.3
Mechanical engineering	1	1.0	1.0	59.2
Nuclear Engineering	1	1.0	1.0	60.2
Project Engineer	11	10.7	10.7	70.9
Project Manager	22	21.4	21.4	92.2
Retail and wholesale	1	1.0	1.0	93.2
Software development	1	1.0	1.0	94.2
Software engineering	1	1.0	1.0	95.1
Sustainability and renewable energy	3	2.9	2.9	98.1
Training and consultations	1	1.0	1.0	99.0
Transportation	1	1.0	1.0	100.0
Total	103	100.0	100.0	

Table 10 is concerned with the area of expertise of the respondents. It is evident from the table that the most dominant area of expertise were information technology (21.4%) and project management

(21.4%), followed by project engineers (10.7%), construction (6.8%), artificial intelligence (4.9%), big data (4.9%), information security (3.9%) and other specializations with 1% each.

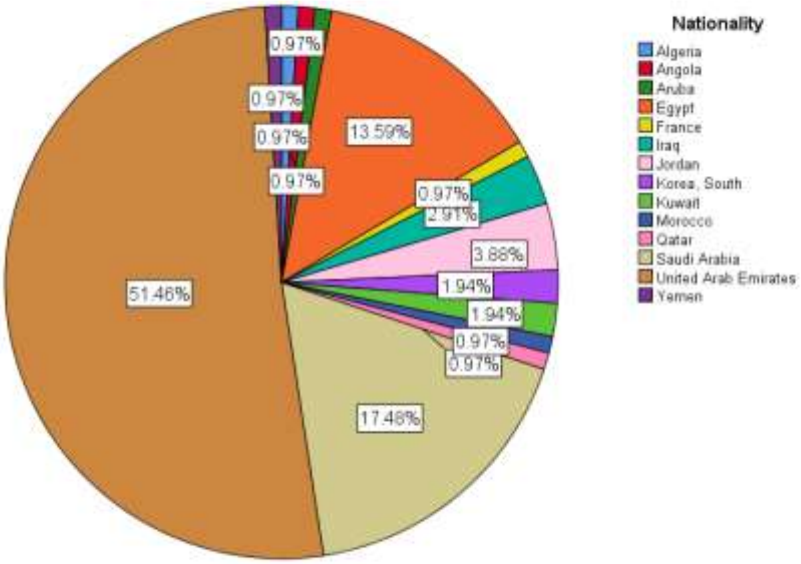


Figure 9: Nationality distribution.

Figure 9 demonstrates the respondent's nationalities, a total of 14 different nationalities were involved in the study, and it shows that more than half of the participants (51.46%) were from United Arab Emirates, followed by Saudi Arabia (17.48%) and Egypt (13.59%).

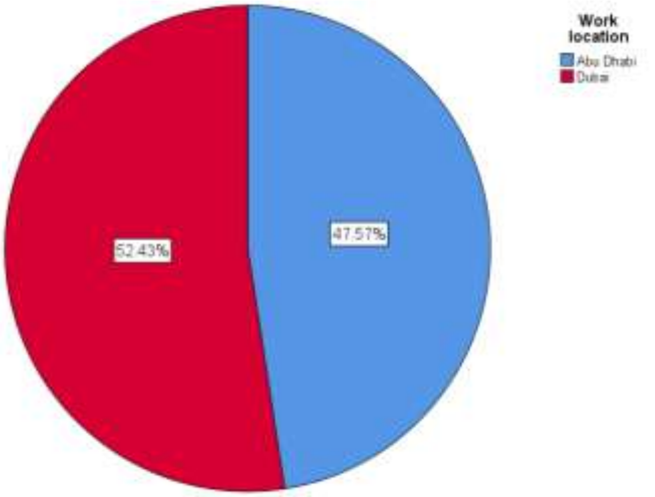


Figure 10: Work location distribution.

5.2 Statistical Analysis

This section of the study analyzes the results obtained from the questionnaire, and provides a brief explanatory discussion of each response to the questionnaire items.

5.2.1 Descriptive statistics

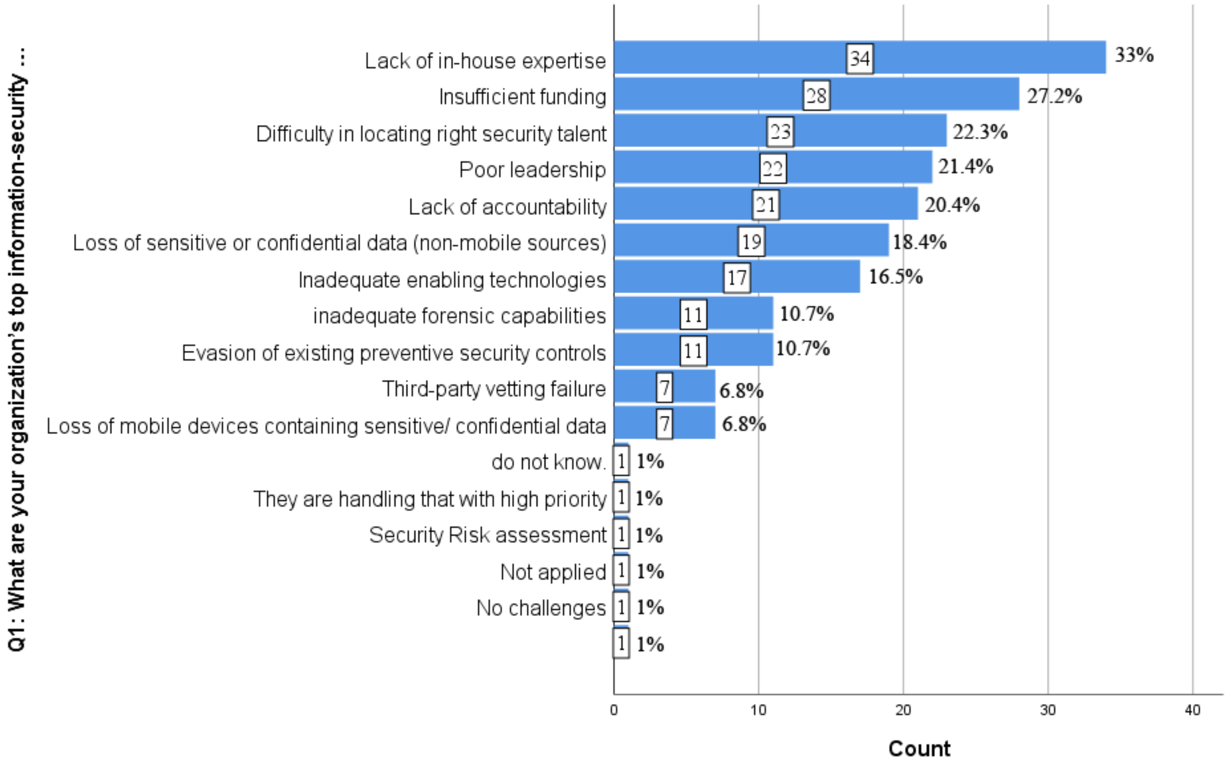


Figure 11: organization's top information-security challenges.

Responses to question 1 of the questionnaire reveals that the top three information security challenges are lack of in-house expertise, insufficient funding and difficulty in locating right security talent. Due to the incorporation of new technologies, well developed competition and unsettling governing, cyber-security has become the top priority. One of the highest concerns of Dubai's and Abu Dhabi's organization is recruiting and retaining cyber-security professionals. Insufficient funding is also a prominent issue while managing cyber-security across organizations, responses to question 22 indicates that 38.84% of organizations in Dubai and Abu Dhabi allocate less than 10% of their IT budget for cyber-security, which is an alarming percentage.

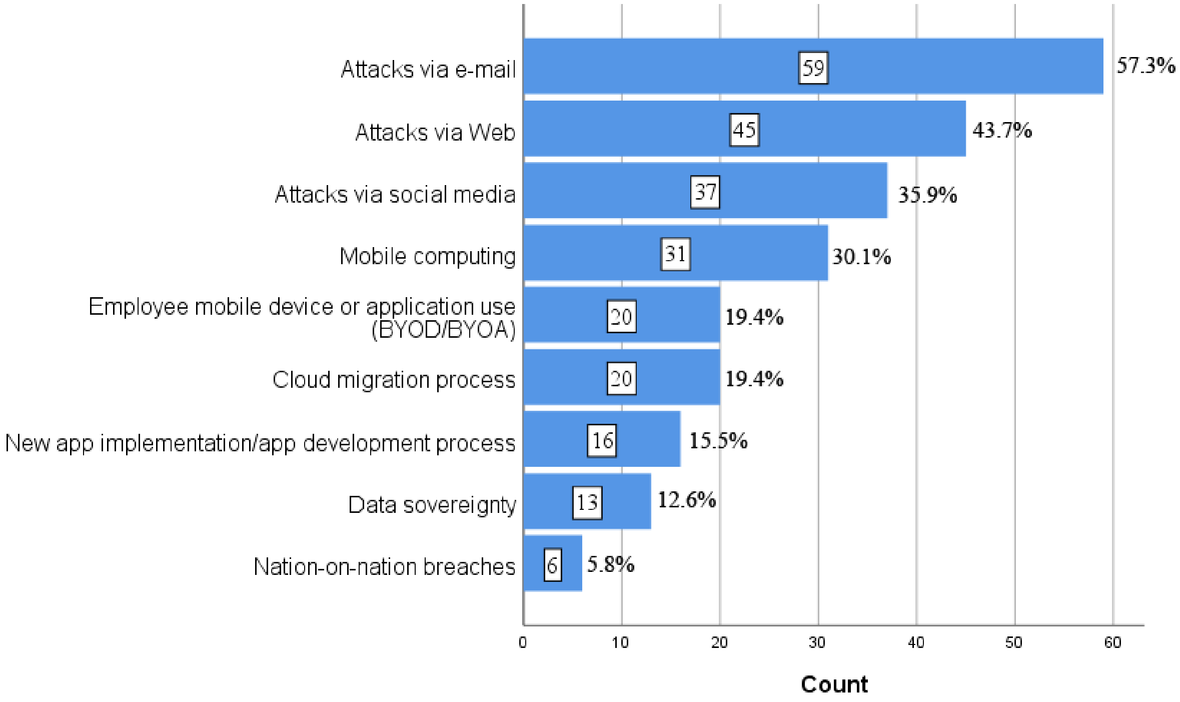


Figure 12: Most growth in security threats.

57.3% of the respondents agree that attacks via e-mails are the most prominent potential security threat, followed by attacks via web, which ranks the second most potential cybersecurity threat with 43.7% of total responses. Furthermore, attacks via social media ranked the third with 35.9% of total responses. Given the ease of access and simplicity of email spoofing with simple online tools, sending a fake email that has an official organization’s representative could be easily mistaken for a real one, tricking the employees to fall for it and clicking on any malicious links or files that has been attached to the e-mail, compromising the whole IT structure of the organization. Web attacks have also seen a growth in the past few years, a recent study According to Ilic (2019), the cross-site scripting (XSS) attack is the most common type of cyber-attack. Nevertheless, it’s not very sophisticated and most of these attacks are carried out by amateurs utilizing scripts which were created by others. Another highly ranked area of cyber-attacks growth is regarding social media, this type of attack could take several forms, such as fake profiles, malicious links and social engineering.

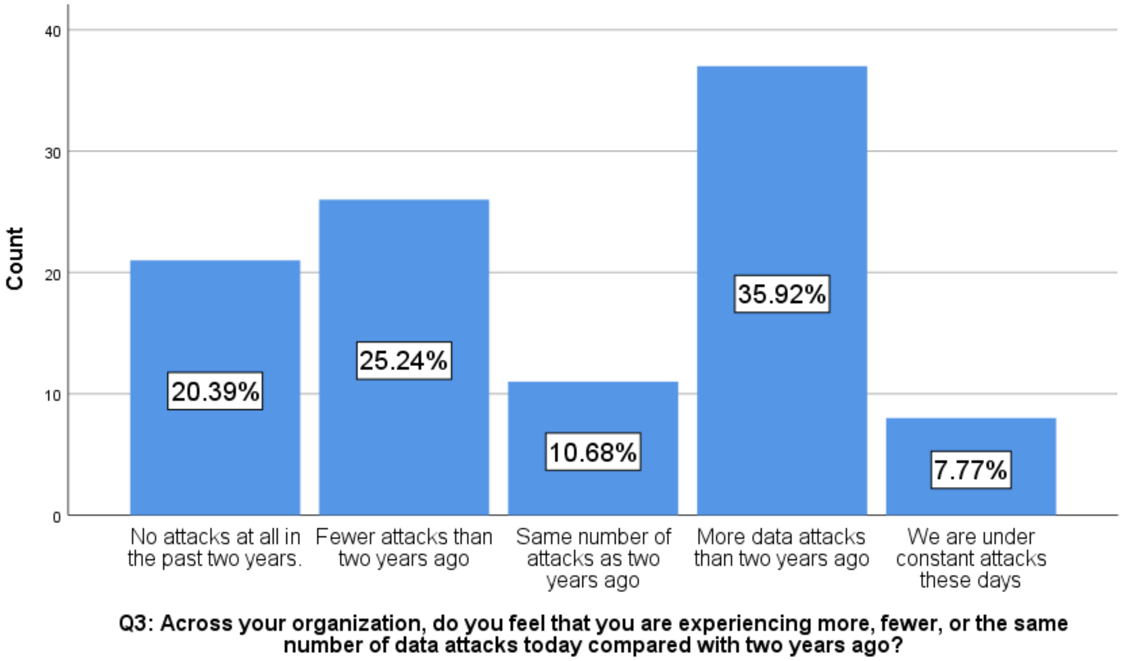


Figure 13: Frequency of data attacks.

Figure 13 demonstrates the distribution of frequency of cyber-attacks across the organizations of Dubai and Abu Dhabi, where 35.92% of the respondents indicated that their organizations have experienced more data attacks than the last two years, while 25.24% stated that their organizations have experienced less attacks than the past two years. A respectively high percentage of the responses (20.39%) indicate that there were no attacks in the past two years.

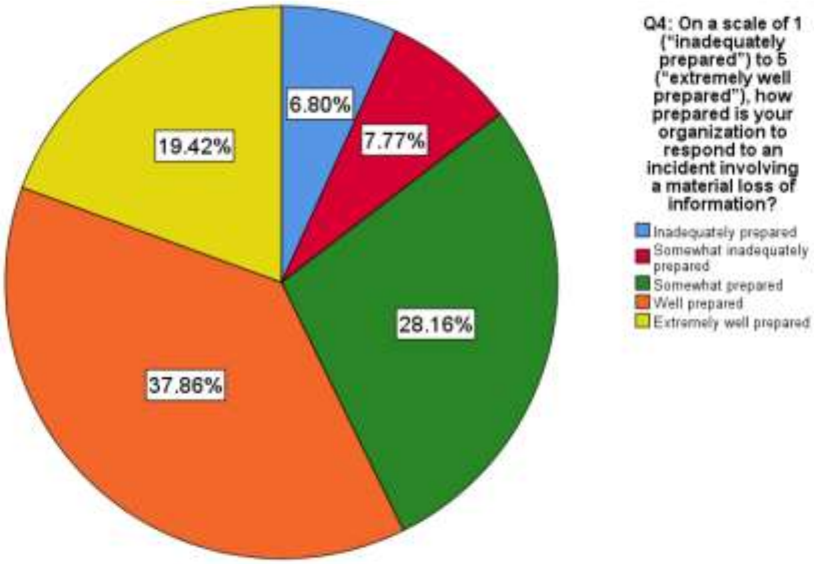


Figure 14: Organization's preparedness to respond to an incident involving a material loss of information.

Figure 14 is concerned with the distribution of organizations who are ready to respond to a cyber-security incident involving data loss, 37.86% of the respondents are confident that their organizations are well prepared to respond to such incident, while 19.42% believe that their organizations are extremely well prepared. a concerning 33.99% of the respondents believe that their organizations are either somewhat prepared, somewhat inadequately prepared or inadequately prepared. Being in such position in today’s active cyber-criminal activities, it is considered as not acceptable for an organization’s management to be unprepared to respond to cyber-security incident, since it is a matter of when, instead of if, an organization is deemed to experience such incidents.

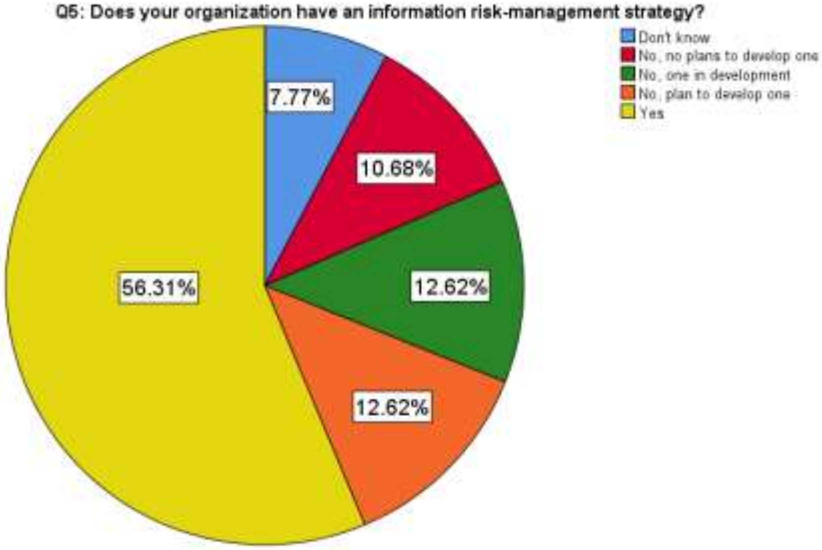


Figure 15: Organization's information risk-management strategy.

Responses to question 5 of the survey is represented by figure 15, which is concerned with the presence of an information risk-management strategy, were 56.31% of the respondents stated that their organizations indeed have such strategy, 25.24% stated that their organizations are either developing a strategy, or planning to develop one. The process of uncertainties management is a difficult task, inadequate resources and dynamic nature of cyber-attacks and threats have deemed it impossible to mitigate all vulnerabilities. Hence the IT team is required to have a plan to support them in communicating a generally comprehended view with the top management about the implications of cyber-security incident on the business.

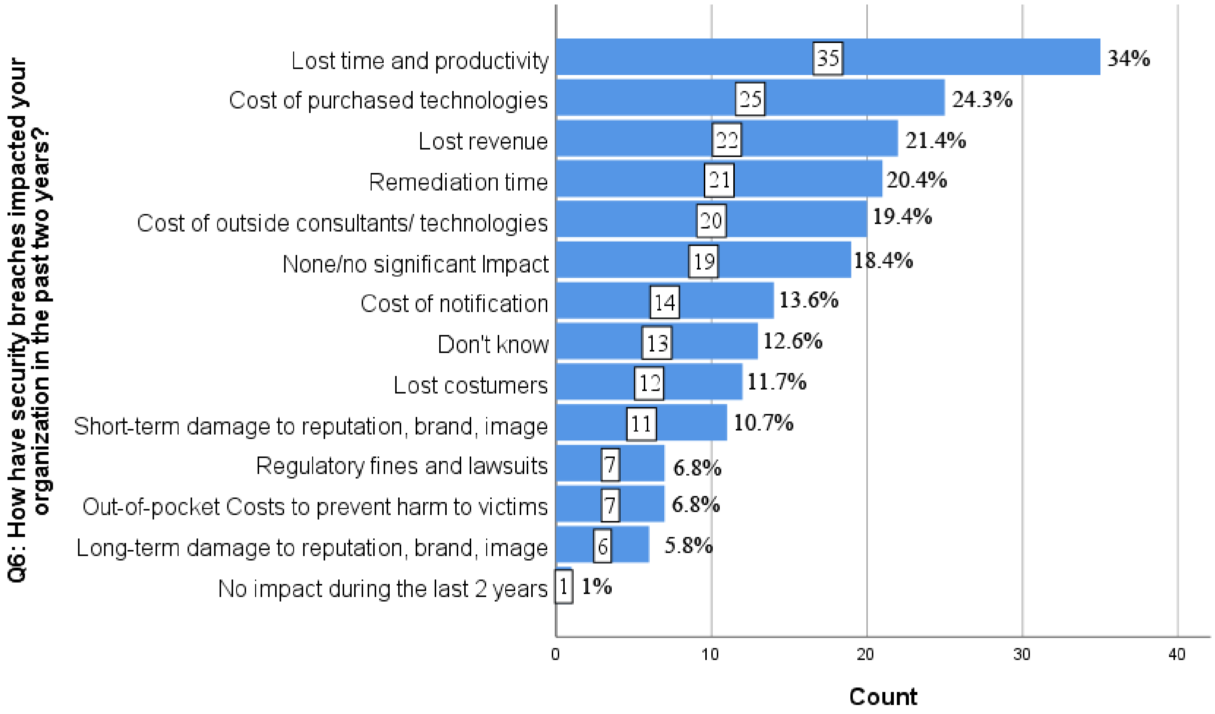


Figure 16: The impact of security breaches on the organization.

Question 6 responses are represented in figure 16, where 34% of the respondents agreed that lost time and productivity was the highest impact to security breaches in the past two years, followed by cost of purchased technologies (24.3%), lost revenue (21.4%) and remediation time (20.4%). A destructive data breach is considered one of the most disruptive events to the business, its impact will usually have a long-term effect on the reputation and customers' perception, as well as risk posture. Furthermore, remediation time could significantly negatively affect the productivity of the whole organization, if the IT structure is compromised, leading to loss in revenue, as well as the cost of replacing the affected technologies.

Table 11: Organization's preparedness in detecting security threats.

	Extremely well prepared	Well prepared	Somewhat prepared	Somewhat inadequately prepared	Inadequately prepared	N/A
Migration to cloud-based applications	18.4%	19.4%	17.5%	11.7%	25.2%	7.8%
Insider attack	15.5%	23.3%	17.5%	19.4%	19.4%	4.9%
Advanced Persistent Threats (APT) attack	13.6%	23.3%	19.4%	19.4%	19.4%	4.9%
Internet of things related threats	13.6%	17.5%	19.4%	22.3%	16.5%	10.7%
Process control logic (PCL) and supervisory control and data acquisition (SCADA) threats	14.6%	15.5%	20.4%	14.6%	22.3%	12.6%
Hacktivist threats	16.5%	18.4%	19.4%	15.5%	23.3%	6.8%
Cybercriminal threats	17.5%	20.4%	15.5%	18.4%	20.4%	7.8%

Table 11 demonstrates the perceived organizations' preparedness to detect security threats, the data in this table were ran through a non-parametric 1-sample sign test to draw an overall conclusion about the situation of preparedness of detecting threats. Further details are discussed in section 5.2.2. The result indicate that organizations are somewhat in adequately prepared to detect cyber-threats, which indicates an alarming potential of failing to detect an attack. The best defense against hackers and cybercriminals is detection. Although it is not possible to prevent all attacks, it is the only way to keep an eye on suspicious activity. Many companies are reluctant to admit that they are good at spotting potential threats due to the number of attacks that are happening.

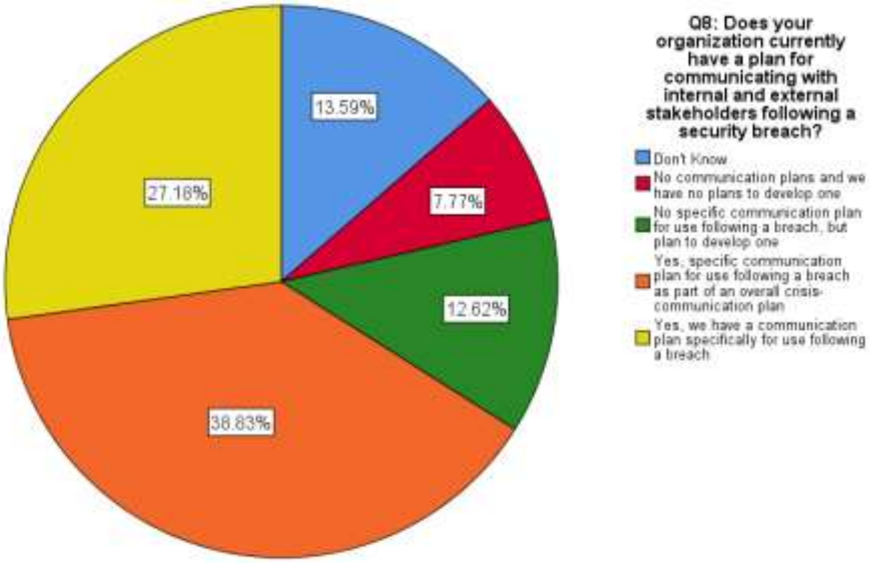


Figure 17: The existence of a communication plan following a security breach.

Figure 18 is concerned with the distribution of respondents in regards to having a communication plan in case of a security breach. 38.83% of the respondents stated that a communication plan exists as a part of an overall crisis – communication plan, while 27.18% stated that there exists a communication plan specifically for use following a security breach. After a breach has been detected, it's important to notify the various stakeholder groups within an instant. These include the board of directors, the C-suite executives, the media and the public.

Table 12: Respondent's rating of their own level of security in different areas.

	Extremely Secure	Secure	Somewhat Secure	Somewhat inadequately secure	Inadequately secure
Mobile computing	9.7%	28.2%	15.5%	20.4%	26.2%
Employee mobile-device or application use (BYOD/BYOA))	7.8%	23.3%	23.3%	20.4%	25.2%
New application implementation/application development process	10.7%	27.2%	20.4%	21.4%	20.4%
E-mail security	16.5%	27.2%	18.4%	14.6%	23.3%
Cloud-migration process	15.5%	26.2%	19.4%	15.5%	23.3%

Data sovereignty/Data security	17.5%	29.1%	15.5%	18.4%	19.4%

Responses to question 9 are represented in table 3. Here, the data have been put through a non-parametric 1-sample sign test and compared to a target value of 4 to draw an overall conclusion about the situation of the respondents' self-rating of security awareness. Further details have been discussed in section 5.2.2. the results of the test indicate that the respondents are somewhat inadequately secure. As cyber attackers become more focused on humans, organizations should start focusing on the people who can most effectively defend themselves from attacks.

Table 13: Organizations preparedness in preventing several security threats.

	Extremely well prepared	**Well prepared**	**Somewhat prepared**	**Somewhat inadequately prepared**	**Inadequately prepared**	**N/A**
Migration to cloud-based applications	18.4%	19.4%	12.6%	19.4%	23.3%	6.8%
Insider attack	16.5%	23.3%	20.4%	18.4%	19.4%	1.9%
Advanced Persistent Threats (APT) attack	18.4%	24.3%	17.5%	20.4%	16.5%	2.9%
Executive breach response	20.4%	21.4%	22.3%	12.6%	22.3%	1%
Internet of things related threats	15.5%	21.4%	15.5%	21.4%	17.5%	8.7%
Process control logic (PCL) and supervisory control and data acquisition (SCADA) threats	17.5%	21.4%	17.5%	18.4%	18.4%	6.8%
Hacktivist threats	17.5%	25.2%	19.4%	14.6%	20.4%	2.9%
Cybercriminal threats	14.6%	25.2%	17.5%	17.5%	20.4%	4.9%

Table 13 illustrates the distribution of responses to question 10, similar to question 7 and 9, the data were tested using non-parametric 1-sample sign test to draw an overall conclusion about the situation of organizations' preparedness to prevent security threats, more details are discussed in section 5.2.2. the results indicate that organizations are somewhat inadequately prepared to prevent several cyber-security threats, which calls for immediate actions and corrective measures to enhance the organizations' ability to prevent such attacks. Being aware of the various types of tools and techniques used by criminals can help prevent a cyber-attack. This ensures that the organization has the necessary tools and resources to safeguard itself.

Table 14: Organizations preparedness in responding to several security threats.

	Extremely well prepared	Well prepared	Somewhat prepared	Somewhat inadequately prepared	Inadequately prepared	N/A
Migration to cloud-based applications	16.5%	21.4%	14.6%	19.4%	22.3%	5.8%
Insider attack	13.6%	27.2%	19.4%	22.3%	17.5%	0%
Advanced Persistent Threats (APT) attack	16.5%	21.4%	18.4%	23.3%	17.5%	2.9%
Executive breach response	15.5%	23.3%	23.3%	17.5%	19.4%	1%
Internet of things related threats	17.5%	16.5%	19.4%	20.4%	19.4%	6.8%
Process control logic (PCL) and supervisory control and data acquisition (SCADA) threats	15.5%	21.4%	16.5%	24.3%	16.5%	5.8%
Hacktivist threats	18.4%	19.4%	22.3%	20.4%	17.5%	1.9%

Cybercriminal threats	16.5%	20.4%	22.3%	21.4%	16.5%	2.9%

Responses to question 11 are represented in table 14, the results obtained from the respondents were further analyzed through non-parametric 1-sample sign test, which indicate that organizations are somewhat inadequately prepared to respond to several cyber-security threats. Even for small businesses, an insignificant security breach could have a significant influence on their operation. Immediate action following a cyber-attack will empower the organization to a better containment or decrease the influence of a cyber-attack.

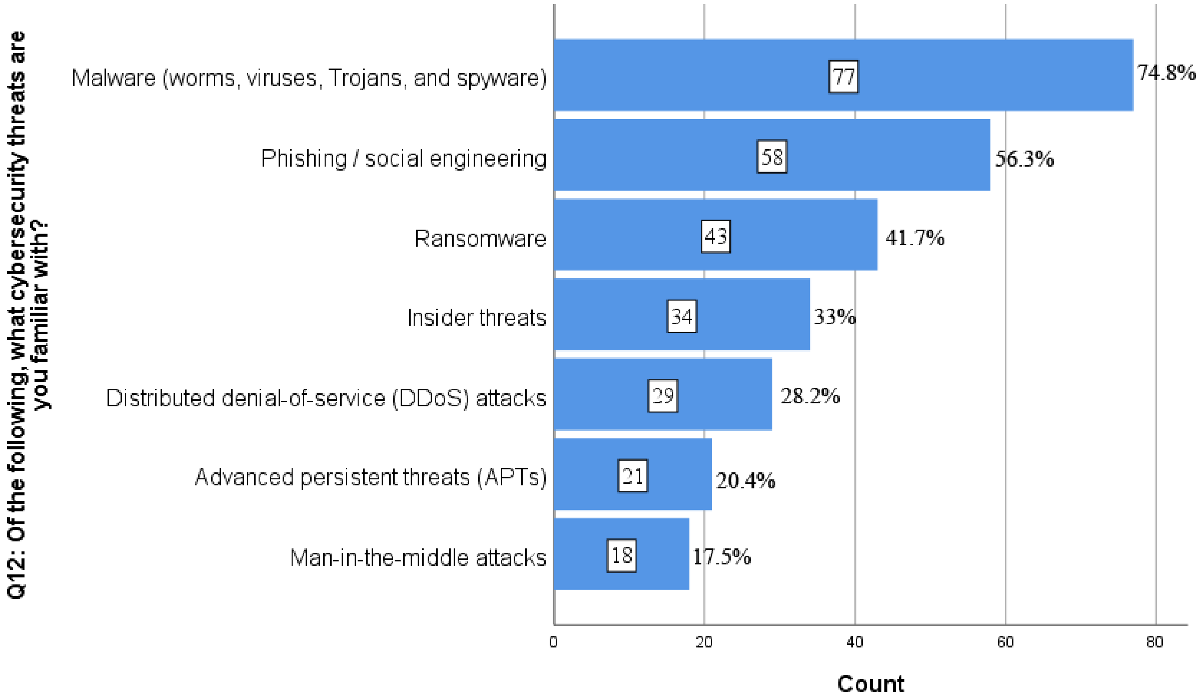


Figure 18: Respondent's familiarity with different cybersecurity threats.

Question 12 responses are represented by figure 18, where it shows that the most familiar type of threat is malware (worms, viruses, trojans and spyware) with a portion of 74.8%. followed by phishing / social engineering with 56.3%%, ransomware with 41.7% and insider threat with 33%. It is quite surprising that a very low percentage of the respondents are aware of ransomware, since this is one of the most dangerous cyber-attacks that could lead to a substantial business loss. Even the mitigation of ransomware attacks could still lead to business loss, since the organization may not be up to date with their backups, and recovering data from an old restore point could result in a serious amount of lost business due to lost transactions with customers. Furthermore, some of the encrypted data could end up not recoverable, which also leads to significant data loss.

Table 15: Level of difficulty to protect, detect and respond to threats compared to two years ago.

	More difficult	**Easier**	**No Significant changes**	**Don't know**
Protect against security breaches	29.1%	50.5%	14.6%	5.8%
Detect security breaches	21.4%	53.4%	20.4%	4.9%
Respond to security breaches	25.2%	51.5%	16.5%	6.8%

Table 15 is concerned with the responses to question 13, where the respondents were asked about the level of difficulty to protect, detect and respond to security breaches. The responses were test through a non-parametric 1-sample sign test and were compared to a target mean of 3. It is evident that no significant changes when it comes to protect, detect and respond to security breaches.

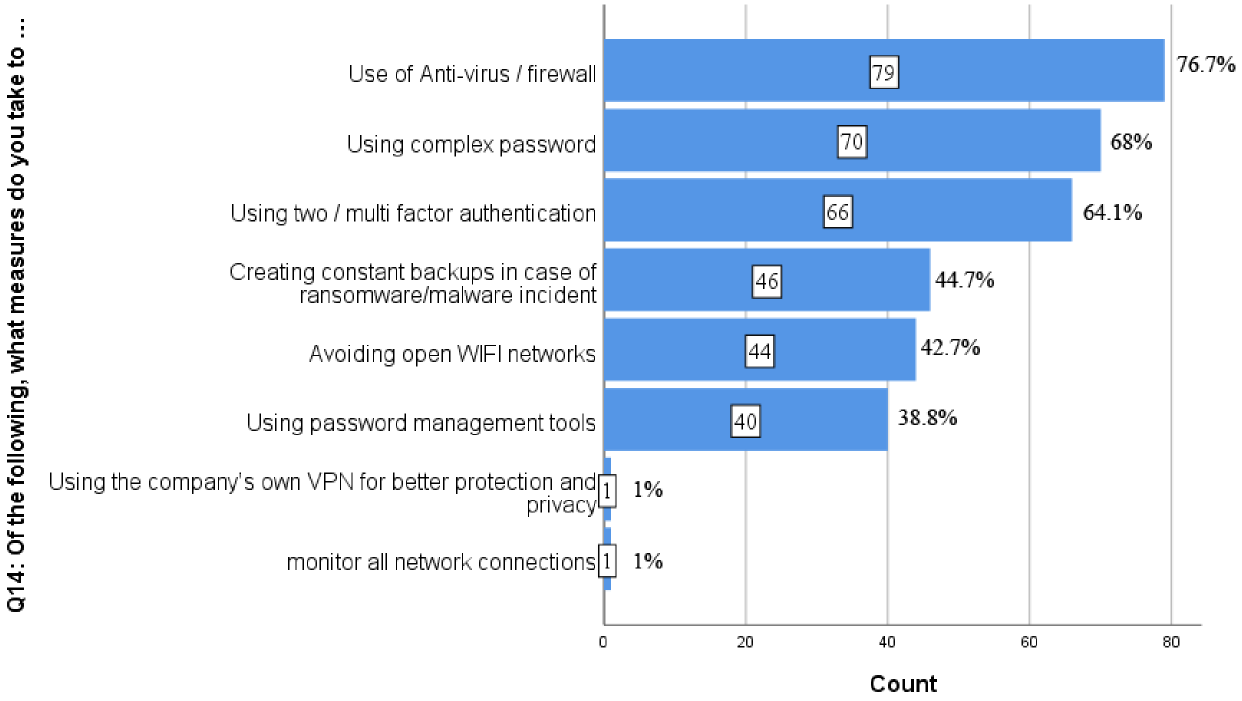


Figure 19: Measures taken by respondents to protect themselves online.

Question 14 responses are represented in figure 19, where the respondents showcase the measures they take in order to protect themselves in an online world. Most of the respondents utilize antivirus software (76.7%), followed by using complex passwords (68%), Using two/ multifactor authentication (64.1%) and creating constant backups in case of ransomware / malware incident (44.7%). The use of antivirus software is very convenient in the present day due to the ease of access to such software, cheap prices and huge variety in the market. Using complex passwords is an excellent strategy to make it near impossible to hack into their accounts, nonetheless, there is always a chance that their passwords might get leaked through an attack on some websites that are not well protected, exploiting their passwords to hackers. Which in terms leads to the second most important strategy in online protection, which is the utilization of two / multifactor authentication.

No matter what passwords the hacker may obtain, it will be impossible to login without an authentication from the owner of the account. It is quite alarming that a low percentage of respondents actually create constant backups to mitigate the effects of a ransomware attack, as such type of attacks is mostly devastating and could lead to huge data loss.

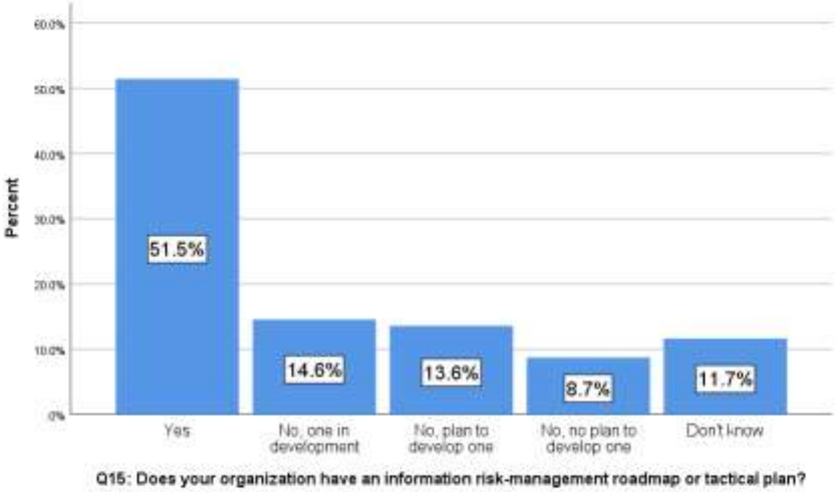


Figure 20: Existence of organization's information risk-management roadmap.

Figure 20 demonstrates the distribution of responses to question 15, where 50.5% of the respondents stated that their organizations do indeed have an information risk-management roadmap, while 14.6 % stated that a roadmap does not exit, but the organization is developing one. 13.6% stated that the organization is planning to develop a roadmap and 8.7% stated that the organization is not developing a roadmap.

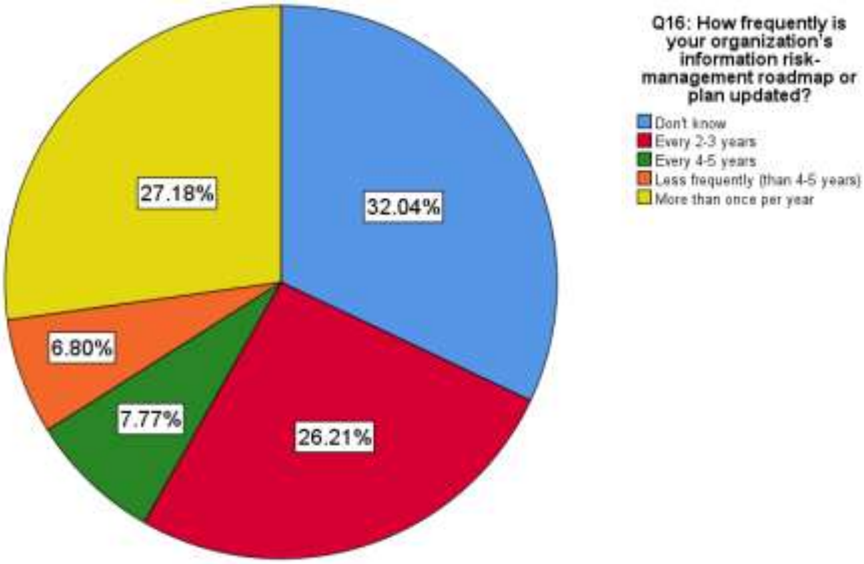


Figure 21: Frequency of organizations information risk-management plan update.

Question 16 responses are represented by figure 21, where the respondents were asked about the frequency of information risk-management roadmap update, 32.04% of the respondents stated that they do not know how frequent it is updated, while 27.18% responded with more than once per year, followed by a 26.21% of the respondents stating that it is updated once every 2-3 years, and 7.77% said that it is updated once every 4-5 years. The organization needs to constantly test, assess and update their risk management plan as risks are constantly changing. Regularly reviewing risk-management roadmap is crucial for recognizing new risks and surveilling the effectiveness of the current risk-management roadmap.

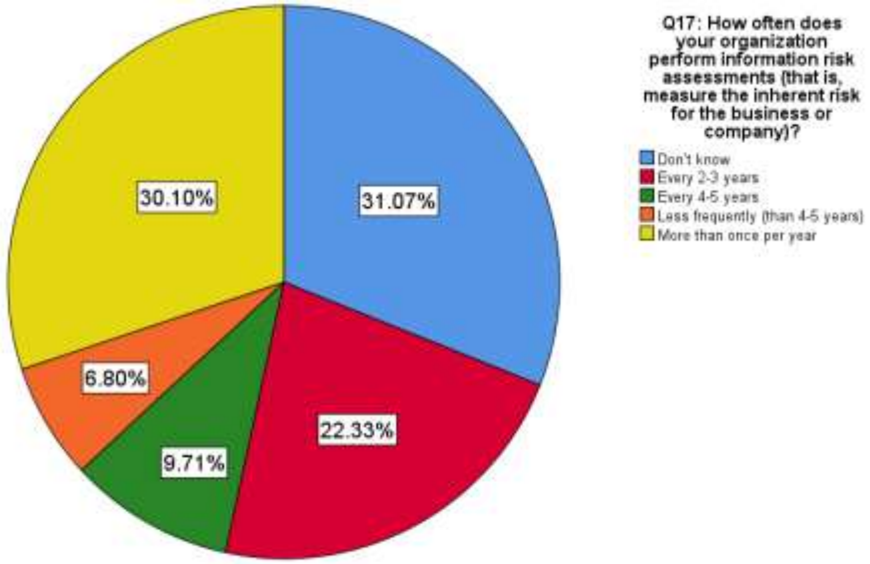


Figure 22: Frequency of information risk assessments across organizations.

Figure 22 illustrates the distribution of responses to question 17, where 31.07% of the respondents stated that they do not know how often does their organizations perform information risk assessments, while 30.1% said that it is carried out more than once per year. Furthermore, 22.33% stated that the assessment is done every 2-3 years, 9.71% stated that the assessment is carried out every 4-5 years. Risk assessments are usually focused on identifying and assessing risks associated with the use and operation of information systems. They are usually conducted for business reasons. After identifying the areas where the company can improve its information technology infrastructure, it's important to think about how this can reduce the risk of a financial loss.

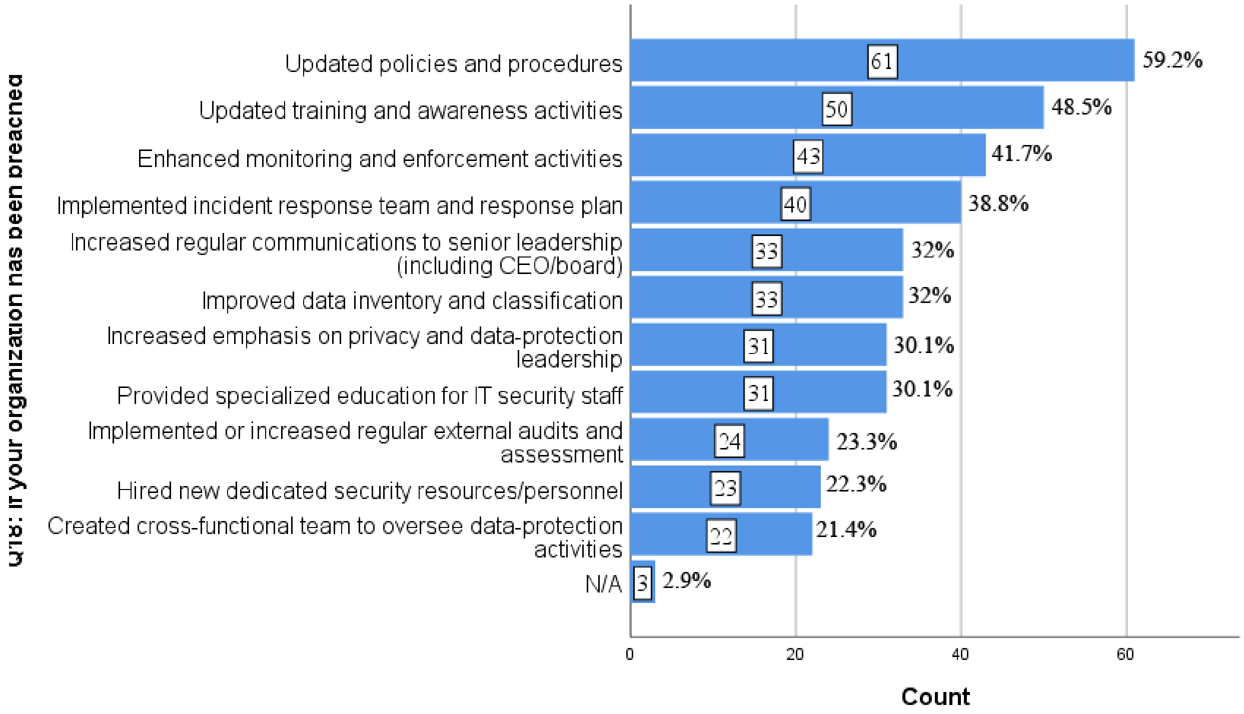


Figure 23: Measures taken by organizations to detect/prevent future attacks.

Question 18 responses are represented in Figure 23, where the respondents were asked what changes to operation and other actions were taken to assist in preventing and detecting future breaches. 59.2% of the respondents stated that the organization have updated their policies and procedures, 48.5% said that their organizations have updated training and awareness activities, while 41.7% reported that their organizations have enhanced monitoring and enforcement activities and 38.8% stated that the organization has implemented incident response team and response plan. Taking protective actions and procedures can significantly reduce the risk of a cyber-attack incident, as new policies may prohibit some unwanted actions by the employees, as well as implement new safeguards and security protocols, which enhances the overall cyber-security system of the organization.

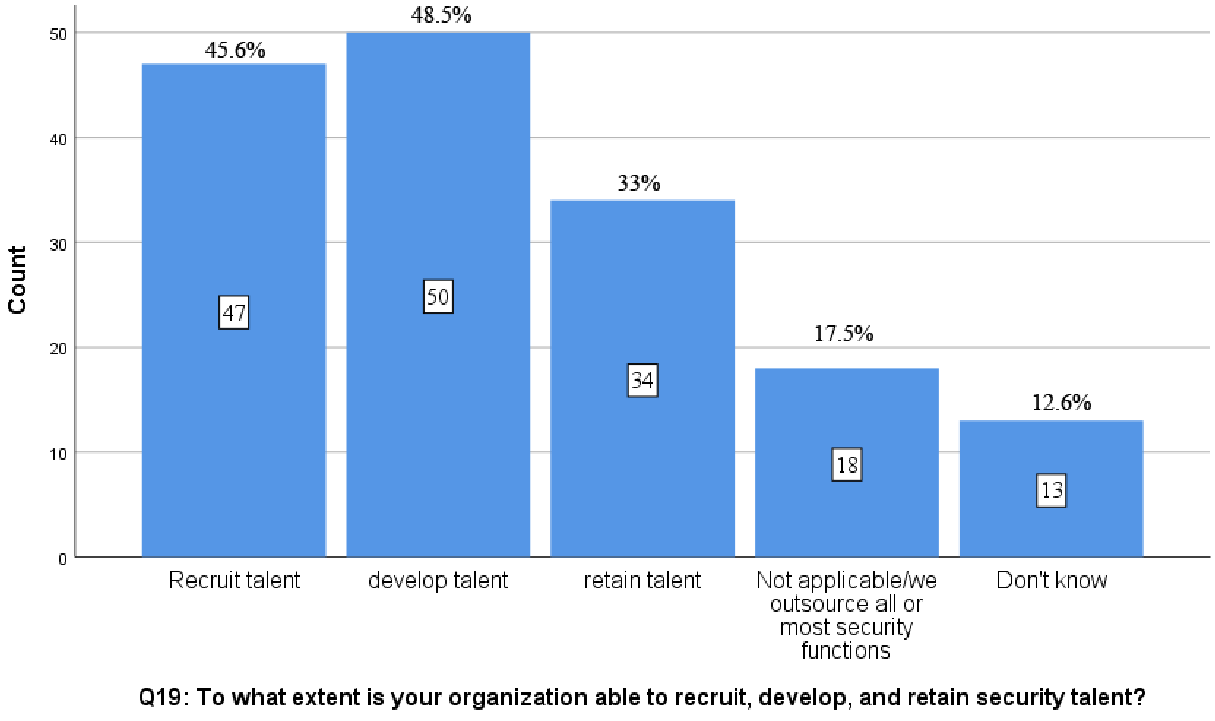


Figure 24: Organization's talent recruitment/development/retaining.

Figure 24 illustrates the distribution of responses to question 19, the respondents were asked to demonstrate to what extent do their organizations recruit, develop and retain security talents. 48.5% of the respondents stated that their companies develop talents, while 45.6% said that their organizations recruit talents, while only 33% stated that their organization retain talent and 17.5% of the respondents stated that most of their security functions are outsourced. While recruiting and developing security talents have their advantages, outsourcing security certainly has its benefits that may outweigh recruiting, developing and retaining talents. Cyber-security should be the organization's top priority, and in a rapid developing business some companies may not pay enough attention to security, therefore not allocating the necessary staff to implement security procedures. Therefore, it could be more convenient for some organizations to outsource their security functions to cyber-security firms where specialists in the field will handle one of the most important aspect of their business. One of the most eminent benefits of outsourcing cyber security functions is the experience that the firm has gained through its work. This ensures that the company doesn't have to recruit a whole team of experienced professionals.

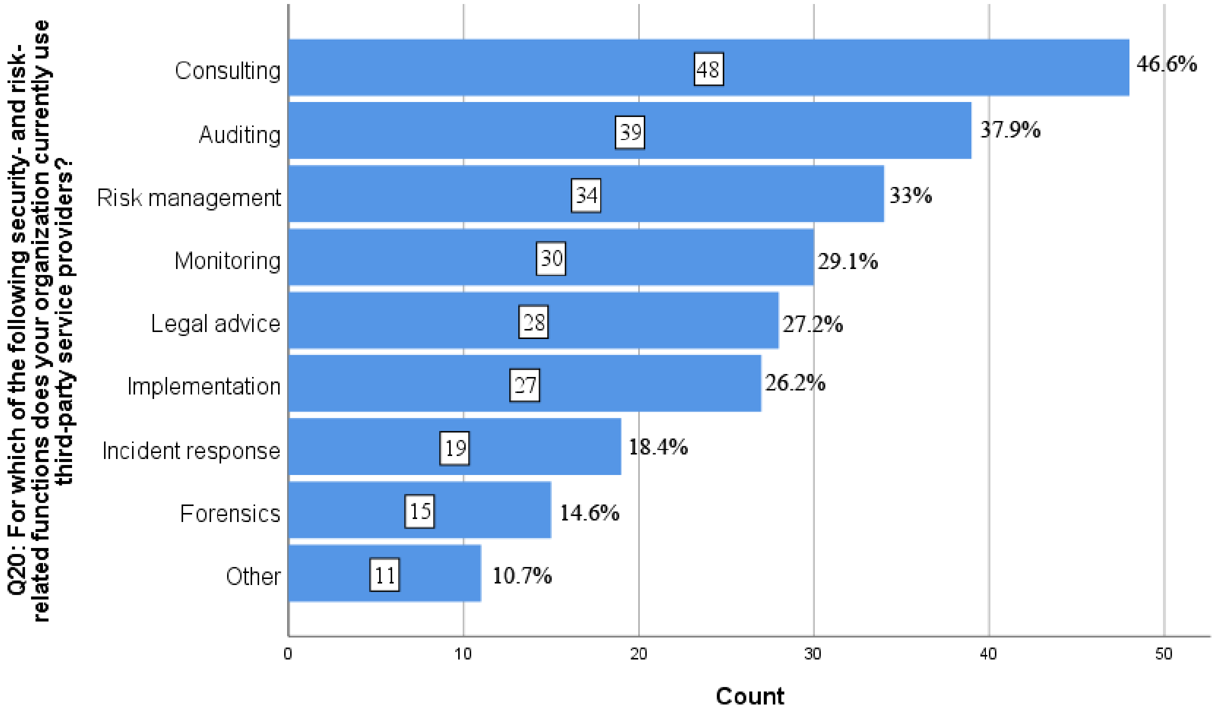


Figure 25: Third party utilization for multiple risk/security functions by the organizations.

Responses to question 20 are represented in figure 25, where the respondents were asked to choose what security and related functions do their organizations currently rely on third-party services with. 46.6% of the respondents stated that their organizations consult third party organizations, 37.9% hire third-party service providers for auditing, while 33% allocate risk management for third-party service provider, 29.1% outsource monitoring their activities and 27.2% get their legal advices from third-party service providers. As mention earlier, outsourcing some of the security functions is usually beneficial for the company and allows their teams to focus on business activities to be able to generate more revenue.

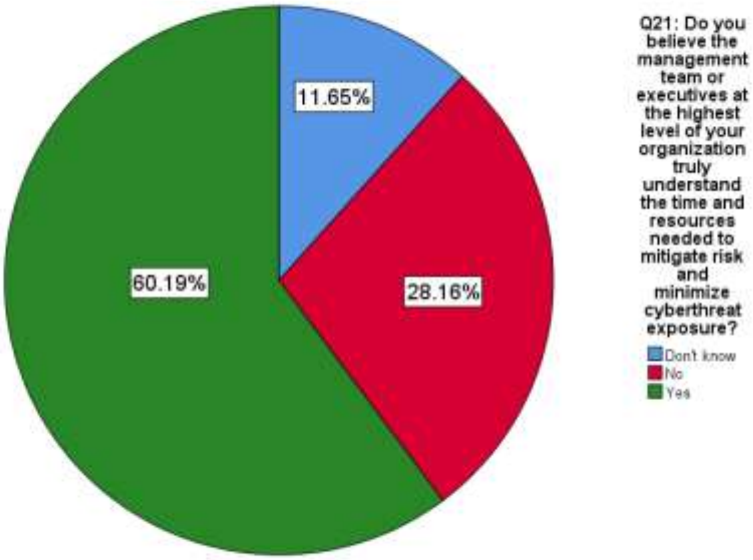


Figure 26: The importance of executives understanding the resources to mitigate risk and cybersecurity exposure.

Figure 26 demonstrates the distribution of responses to question 21, the respondents were asked if they believe that their organizations' top management and executives truly understand the resources needed to mitigate risk and minimize the exposure to cyber-threats. 60.19% of the respondents believe that their supervisors and executives actually understand what it takes to minimize the exposure to cyber-threats, while an alarming 28.16% stated that they do not think that the top management have an understanding of the importance of time and resources allocation for cybersecurity. This is a crucial part of the information security system in the organization as the top management play an important role in achieving a high security state. A good information security culture is created when the top management of an organization is sensitive to the importance of protecting its information. This can be achieved through the development of an effective information security policy.

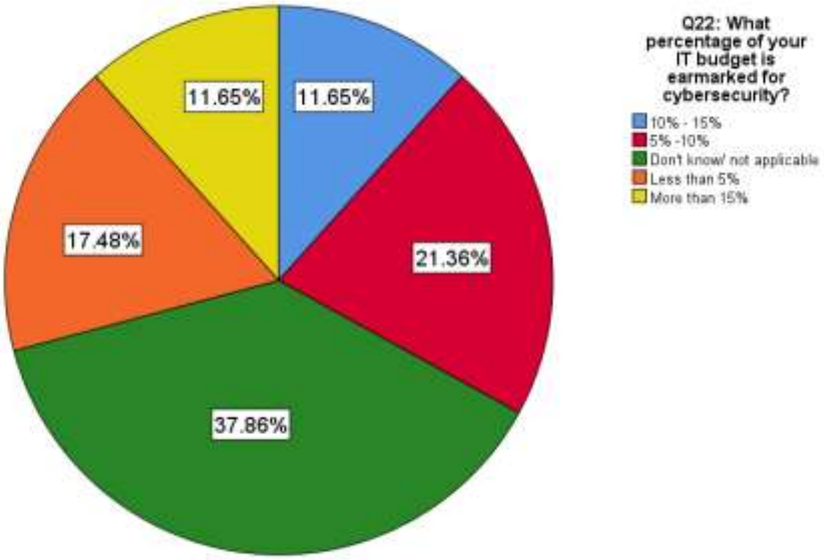


Figure 27: Cybersecurity budget allocated by organizations.

Responses to question 22 is represented in figure 27. The respondents were asked what percentage of the IT budget was allocated to cybersecurity. 37.86% of the respondents were not able to provide such an information, 21.36% stated that the organization allocates 5% to 10% of their IT budget for cybersecurity, 17.48% said that the allocation was less than 5%, 11.65% stated that the allocation was between 10% to 15% and 11.65% said that more than 15% was allocated for cyber-security. Setting an adequate budget will ensure that all security functions, whether in-house or outsourced, are effectively deployed and running. Although it's cheaper to prevent a cyber-attack than to fix the damage caused by it, it's still important to realize that financial losses can still occur due to breaches and other types of attacks. One of the most damaging effects of these attacks is the loss of customers' confidence in the company.

5.2.2 Hypothesis testing

This section of the study will include hypothesis testing to multiple aspects of the cybersecurity situation based on the data collected from the questionnaire. Non-parametric 1-sample sign test was used to perform the hypothesis testing with different target values for the medians to be compared to. This type of test was selected for hypothesis testing because Likert scale items produce a discrete dataset, in addition, all datasets were tested for normality and it was concluded that they do not follow a normal distribution. “N/A” responses were considered missing data and therefore were discarded from the test.

Hypothesis 1a (H1a): Organizations are well prepared to detect cyber-threats.

Table 16: Results of H1a.

Null hypothesis H_0: $\eta = 4$
Alternative hypothesis H_1: $\eta < 4$

Sample	Number < 4	Number = 4	Number > 4	P-Value
Q7	409	142	113	0.000

Hypothesis 1b (H1b): Organizations are somewhat prepared to detect cyber-threats.

Table 17: Results of H1b.

Null hypothesis H_0: $\eta = 3$
Alternative hypothesis H_1: $\eta < 3$

Sample	Number < 3	Number = 3	Number > 3	P-Value
Q7	276	133	255	0.193

Table 16 and 17 demonstrate the results of non-parametric 1 sample sign test for question 7, which revealed that the p-value is less than $\alpha = 0.05$ when compared to a median of 4, which means that the null hypothesis should be rejected and conclude that the median is less than 4. Furthermore, the p-value was greater than $\alpha = 0.05$ when the median was compared to 3, which implies that we the null hypothesis should be accepted and conclude that the median is equal to 3. This result indicate that organizations are somewhat prepared to detect a cyber-threat.

Hypothesis 2a (H2a): Organizations are well prepared to prevent cyber-threats.

Table 18: Results of H2a.

Null hypothesis	$H_0: \eta = 4$			
Alternative hypothesis	$H_1: \eta < 4$			
Sample	**Number < 4**	**Number = 4**	**Number > 4**	**P-Value**
Q10	457	187	143	0.000

Hypothesis 2b (H2b): Organizations are somewhat prepared to prevent cyber-threats.

Table 19: Results of H2b.

Null hypothesis	$H_0: \eta = 3$			
Alternative hypothesis	$H_1: \eta < 3$			
Sample	**Number < 3**	**Number = 3**	**Number > 3**	**P-Value**
Q10	310	147	330	0.797

Table 18 and 19 demonstrates the results of non-parametric 1 sample sign test for question 10, it was revealed that the p-value is less than $\alpha = 0.05$ when compared to a median of 4, which means that the null hypothesis should be rejected and conclude that the median is less than 4. Furthermore, the p-value was greater than $\alpha = 0.05$ when the median was compared to 3, which implies that we null hypothesis should be accepted and conclude that the median is equal to 3. This result indicate that organizations are somewhat prepared to prevent a cyber-threat.

Hypothesis 3a (H3a): Organizations are well prepared to respond to cyber-threats.

Table 20: Results of H3a.

Null hypothesis	$H_0: \eta = 4$			
Alternative hypothesis	$H_1: \eta < 4$			
Sample	**Number < 4**	**Number = 4**	**Number > 4**	**P-Value**
Q11	486	176	134	0.000

Hypothesis 3b (H3b): Organizations are somewhat prepared to respond to cyber-threats.

Table 21: results of H3b.

Null hypothesis H_0: $\eta = 3$
Alternative hypothesis H_1: $\eta < 3$

Sample	Number < 3	Number = 3	Number > 3	P-Value
Q11	325	161	310	0.289

Table 20 and 21 demonstrates the results of non-parametric 1 sample sign test for question 11, it was revealed that the p-value is less than $\alpha = 0.05$ when compared to a median of 4, which means that the null hypothesis should be rejected and conclude that the median is less than 4. Furthermore, the p-value was greater than $\alpha = 0.05$ when the median was compared to 3, which implies that we the null hypothesis should be accepted and conclude that the median is equal to 3. This result indicate that organizations are somewhat prepared to respond to a cyber-threat.

Hypothesis 4 (H4a): respondents have high level of cyber-security awareness.

Table 22: Results of H4a.

Null hypothesis H_0: $\eta = 4$
Alternative hypothesis H_1: $\eta < 4$

Sample	Number < 4	Number = 4	Number > 4	P-Value
Q9	372	166	80	0.000

Hypothesis 4 (H4b): respondents have mediocre level of cyber-security awareness.

Table 23: Results of H4b.

Null hypothesis H_0: $\eta = 3$
Alternative hypothesis H_1: $\eta < 3$

Sample	Number < 3	Number = 3	Number > 3	P-Value
Q9	256	116	246	0.344

Table 22 and 23 demonstrates the results of non-parametric 1 sample sign test for question 9, it was revealed that the p-value is less than $\alpha = 0.05$ when compared to a median of 4, which means that the null hypothesis should be rejected and conclude that the median is less than 4. Furthermore, the p-value was greater than $\alpha = 0.05$ when the median was compared to 3, which implies that we should accept the null hypothesis and conclude that the median is equal to 3. This result indicate that individuals have mediocre security awareness against various types of cyber-threats.

5.3 Findings

Upon the completion of this study, it was discovered that:

- The top information security challenges are lack of in-house expertise, insufficient funding, difficulty in locating right security talent, poor leadership and lack of accountability.
- The p-value of (H1a) is equal to 0.000, This value is less than α = 0.05 (significance level), therefore the null hypothesis should be rejected, and the p-value of (H1b) was 0.193, This value is greater than α = 0.05, therefore we should accept the null hypothesis and conclude that the organizations are *somewhat prepared* to detect cyber-threats.
- The p-value of (H2a) is equal to 0.000, this value is less than α = 0.05, therefore the null hypothesis should be rejected, and the p-value of (H2b) was 0.797, this value is greater than α = 0.05, therefore we the null hypothesis should be accepted and conclude that the organizations are *somewhat prepared* to prevent cyber-threats.
- The p-value of (H3a) is equal to 0.000, this value is less than the α = 0.05, therefore the null hypothesis should be rejected, and the p-value of (H3b) was 0.289, this value is greater than α = 0.05, therefore the null hypothesis should be accepted and conclude that the organizations are *somewhat prepared* to respond cyber-threats.
- The p-value of (H4a) is equal to 0.000, this value is less than α = 0.05, therefore the null hypothesis should be rejected, and the p-value of (H3b) was 0.344, this value is greater than

$\alpha = 0.05$, therefore the null hypothesis should be accepted and conclude that people have mediocre level of security awareness.

Chapter 6: Discussion

The main objective of this study was to identify the main cyber-security challenges that are concerning the organizations established in the smart cities of the United Arab Emirates, Dubai and Abu Dhabi. Furthermore, this study aimed to investigate the preparedness of organizations to detect, prevent and respond to cyber-threats, as well as measure the level of awareness of individuals of smart cities. It was revealed that the main challenges that were face by organizations were lack of in-house expertise, insufficient funding, difficulty in locating right security talent, poor leadership and lack of accountability. Such challenges could really put the organization at high risk if corrective measures are not taken. Regarding lack of in-house expertise, it was revealed by the responses of question 19 that less than 50% of the organizations recruit and develop security talents, and only a third of the organizations have retained their security talent, while 17% had their security functions outsourced. Hiring an in-house security talent has its advantages, Due to the sensitive nature of an information security specialist's job, it's natural for an organization's top management to hire a permanent employee for this position. This ensures that the company has the right candidate for the job. However, the extremely limited qualified candidates (Christiansen & Piekarz, 2018) makes it extremely hard for organizations to hire security talents, which may motivate the organization to outsource their security functions. In addition, to address the skills shortage in the industry, many companies turn to their partners for help in managing their security operations. This ensures that the company has the proper resources to effectively protect its critical assets.

Insufficient funding was also found to be a major cyber-security challenge for organizations in smart cities, as it as revealed by question 22, 38.84% of the organizations of smart cities in the

UAE allocate less than 10% of their IT budget towards cyber-security. Allocating the right budget for cybersecurity is often hard and troublesome (Moore et al. 2015), because there in not enough data since threat moves too quickly, preventing security firms from accumulating data fast enough. Nonetheless, a security officer could justify the cyber-security budget by knowing the frequency of cyber-attacks, how many data breaches or how many of the employees were victims to email phishing. Afterwards, the need of cybersecurity budget could be explained based on the collected data. Poor leadership is also a major challenge that may hurdle a smooth cyber-security operation. The work of Masrek et al. (2019) indicates that a good information security culture is created when the top management of an organization is sensitive to the importance of protecting its information. This can be achieved through the development of an effective information security policy. Due to the evolution of attack methods and techniques, it's also important to note that cyber-attacks are becoming more sophisticated. Unlike the past, where attackers would typically try to cripple a website to prevent business transactions, today's attackers are focused on going unnoticed. Instead of focusing on perimeter protection, it's important for top management to adopt a strategy that focuses on detecting hidden threats. This strategy can help protect their critical data and prevent unauthorized access.

Furthermore, the results of hypothesis testing indicated that organizations are somewhat prepared to detect, prevent and respond to cyber-threats. These are core functions of any cybersecurity system and organizations should implement meticulously to insure smooth business operation. One of the most important steps that a company can take to identify and address a weakness is to quickly identify the root cause of the issue. This will allow them to close the gap and prevent further damage. Some methods which may assist in the process of detecting a cyber-threat is to identify mysterious emails, identify suspicious pop-ups note, uncommon password activity, penetration testing and keeping software updated. The first two strategies are especially important, since the results of question 2 revealed that these are the top two growing cyber-threats. Top management and IT department should constantly raise awareness across the whole organization to avoid suspicious emails and avoid all web pop-up windows, as unknown pop-ups could be infected with malware and malicious emails could lead to ransomware attack through attachments and download links. Lokuketagoda et al. (2020) have proposed a three-level ransomware detection and prevention mechanism that uses virtual machine and browser extension to scan any files the users intends to download from the internet. It is a common occurance that individuals tend to rely exclusively on antivirus software since it gives them a peace of mind that their devices are secured, however, it might not be enough for protection, as cybersecurity awareness plays a very important role in protecting the users and organizations.

Chapter 7: Conclusion

Cyber-security remains to be one of the top challenges that faces the transformation into a smart city (Baker et al. 2017; Lu & Da Xu, 2018; Ejaz and anpalagan, 2019). In this study, the major cyber-security challenges were identified and exposed to practitioners and researchers. In a rapidly growing world, governments are working around the clock to find solutions to the increased populations and considering the transformation into a smart city a feasible solution. However, this solution imposes a number of challenges since it requires extensive implementation of IoT and information and communication technologies (ICTs). As mentioned earlier, cyber-security is a major concern, as the infrastructure of smart city could be comprised in an event of a cyber-attack, which could expose sensitive data that belongs both to individuals and governments. Therefore, it is there is a persistent need for continuous development, monitoring, controlling and evaluation of cybersecurity procedures and protocols. This study has also provided an insight into the preparedness of the organizations to detect, prevent and respond to cyber-attacks. It was revealed that companies are somewhat prepared to deploy the cyber-security functions. With the massive number of cyber-attacks faced by the industry every day, early detection of such attacks could prevent massive data loss and business interruption. If for any reason the detection mechanism fails to perform its job, then the organization should immediately start the prevention and response functions. The quicker a company can recognize the root cause and respond to the vulnerability, the quicker it is for the company to address and close the gap. Such quick response to incidents enables the organization to resume its business in the shortest amount of time, minimize the losses and retain customers and stakeholder confidence in the rigidity and robustness of the organization's business operation. Furthermore, this study revealed that individual's cyber-security awareness level is mediocre, which worsens the situation even more. The work presented in this study could assist practitioners and researchers in understanding the current situation of organizations found in our region, which calls for corrective measures and enhancement to the cybersecurity system. Future studies may consider digging deeper in the specific weaknesses in the functions of cyber-security, as this study provided an overall insight about the current implantation of security functions: detect, prevent and respond. More specifically, within each function there are security threats that could be further investigated.

References

Abraham, S., & Chengalur-Smith, I. (2019). Evaluating the effectiveness of learner controlled information security training. *Computers & Security*, *87*, 101586.

Ahmad, K., Maabreh, M., Ghaly, M., Khan, K., Qadir, J., & Al-Fuqaha, A. (2022). Developing future human-centered smart cities: Critical analysis of smart city security, Data management, and Ethical challenges. *Computer Science Review*, *43*, 100452.

Al Sharif, R., & Pokharel, S. (2021). Smart City Dimensions and Associated Risks: Review of literature. *Sustainable Cities and Society*, 103542.

Alansari, Z., Soomro, S., Belgaum, M. R., & Shahaboddin, S. (2016). A new conceptual model for BYOD organizational adoption. *Asian J. Sci. Res*, *10*, 400-405.

AlDairi, A. (2017). Cyber security attacks on smart cities and associated mobile technologies. *Procedia Computer Science*, *109*, 1086-1091.

Aljazeera net (2019). Digital transformation and smart cities.. the end of QITCOM. [Online] Available at: https://www.aljazeera.net/news/scienceandtechnology [Accessed Nov. 05, 2021].

Al-Karaki, J. N., Gawanmeh, A., & El-Yassami, S. (2020). GoSafe: on the practical characterization of the overall security posture of an organization information system using smart auditing and ranking. *Journal of King Saud University-Computer and Information Sciences*.

Alsyouf, I., Alsuwaidi, M., Hamdan, S., & Shamsuzzaman, M. (2021). Impact of ISO 55000 on organisational performance: evidence from certified UAE firms. *Total Quality Management & Business Excellence*, *32*(1-2), 134-152.

Amoroso, E. 2006. *Cyber Security*. New Jersey: Silicon Press.

Amrhein, V., Trafimow, D., & Greenland, S. (2019). Inferential statistics as descriptive statistics: There is no replication crisis if we don't expect replication. *The American Statistician*, *73*(sup1), 262-270.

Anderson, J. M. (2003). Why we need a new definition of information security. *Computers & Security*, *22*(4), 308-313.

Anderson, R., & Moore, T. (2006). The economics of information security. *science*, *314*(5799), 610-613.

At least 3 of Sans Top 20 critical controls require addressing SSH key based access & SSH key management to know who can access what & enforce boundary. At least 3 of SANS top 20 Critical Controls require addressing SSH key based access & SSH key management to know who can access what & enforce boundary. (2021, April 23). Retrieved December 4, 2021, from https://www.ssh.com/academy/compliance/sans-top-20

Bagloee, S. A., Heshmati, M., Dia, H., Ghaderi, H., Pettit, C., & Asadi, M. (2021). Blockchain: The operating system of smart cities. *Cities*, *112*, 103104.

Baig, Z. A., Szewczyk, P., Valli, C., Rabadia, P., Hannay, P., Chernyshev, M., ... & Peacock, M. (2017). Future challenges for smart cities: Cyber-security and digital forensics. *Digital Investigation*, *22*, 3-13.

Baker, S. B., Xiang, W., & Atkinson, I. (2017). Internet of things for smart healthcare: Technologies, challenges, and opportunities. *IEEE Access*, *5*, 26521-26544.

Belgaum, M. R., Alansari, Z., Jain, R., & Alshaer, J. (2018, April). A framework for evaluation of cyber security challenges in smart cities. In *Smart Cities Symposium 2018* (pp. 1-6). IET.

Benevolo, C., Dameri, R. P., & D'auria, B. (2016). Smart mobility in smart city. In *Empowering organizations* (pp. 13-28). Springer, Cham.

Biryukov, D. N., Lomako, A. G., & Rostovtsev Yu, G. The appearance of anti-cyber systems to prevent the risks of cyber-threat [Proc. SPIIRAN]. 2015, V. 39. *DOI: http://dx. doi. org/10.15622/sp*, *39*, 5-25.

Breslow, H. (2021). The smart city and the containment of informality: The case of Dubai. *Urban Studies*, *58*(3), 471-486.

Chang, S. H., Chiang, R. D., Wu, S. J., & Chang, W. T. (2016). A context-aware, interactive M-health system for diabetics. *IT professional*, *18*(3), 14-22.

Chen, J., Ramanathan, L., & Alazab, M. (2021). Holistic big data integrated artificial intelligent modeling to improve privacy and security in data management of smart cities. *Microprocessors and Microsystems*, *81*, 103722.

Choeum, D., & Choi, D. H. (2021). Trilevel smart meter hardening strategy for mitigating cyber attacks against Volt/VAR optimization in smart power distribution systems. *Applied Energy*, *304*, 117710.

Chourabi, H., Nam, T., Walker, S., Gil-Garcia, J. R., Mellouli, S., Nahon, K., ... & Scholl, H. J. (2012, January). Understanding smart cities: An integrative framework. In *2012 45th Hawaii international conference on system sciences* (pp. 2289-2297). IEEE.

Christiansen, B., & Piekarz, A. (Eds.). (2018). *Global cyber security labor shortage and international business risk*. IGI Global.

Cohen, B. (2006). Urbanization in developing countries: Current trends, future projections, and key challenges for sustainability. *Technology in society*, *28*(1-2), 63-80.

Committee on National Security Systems (CNSS). (2010) . National Information Assurance Glossary. Committee on National Security Systems (CNSS) Instruction No 4009 http://www.ncix.gov/publications/policy/docs/CNSSI_4009.pdf

Craigen, D., Diakun-Thibault, N., & Purse, R. (2014). Defining cybersecurity. *Technology Innovation Management Review*, *4*(10).

David, B., Dowsley, R., van de Graaf, J., Marques, D., Nascimento, A. C., & Pinto, A. C. (2015). Unconditionally secure, universally composable privacy preserving linear algebra. *IEEE Transactions on Information Forensics and Security*, *11*(1), 59-73.

Delahunty, S. (2009). State of enterprise storage. *Paper presented by Byte & Switch. InformationWeek Analytics. com, Manhassett, NY*.

Donta, P. K., Srirama, S. N., Amgoth, T., & Annavarapu, C. S. R. (2021). Survey on recent advances in IoT application layer protocols and machine learning scope for research directions. *Digital Communications and Networks*.

dos Santos Silva, I. (1999). Overview of study designs. *Cancer epidemiology: principles and methods. Lyon: International Agency for Research on Cancer*, 83-101.

Draft Investigatory Powers Bill, Nov. 2015

Dubrawsky, I., & Faircloth, J. (2007). *Security+ Study Guide*. Syngress.

Efthymiopoulos, M. P. (2016). Cyber-security in smart cities: the case of Dubai. *Journal of Innovation and Entrepreneurship*, *5*(1), 1-16.

Ejaz, W., & Anpalagan, A. (2019). Internet of things for smart cities: overview and key challenges. *Internet of Things for Smart Cities*, 1-15.

Elmaghraby, A. S., & Losavio, M. M. (2014). Cyber security challenges in Smart Cities: Safety, security and privacy. *Journal of advanced research*, *5*(4), 491-497.

Flick, T., & Morehouse, J. (2010). *Securing the smart grid: next generation power grid security*. Elsevier.

Fovino, I. N., Coletta, A., Carcano, A., & Masera, M. (2011). Critical state-based filtering system for securing SCADA network protocols. *IEEE Transactions on industrial electronics*, *59*(10), 3943-3950.

Fu, Y., O'Neill, Z., Yang, Z., Adetola, V., Wen, J., Ren, L., ... & Wu, T. (2021). Modeling and evaluation of cyber-attacks on grid-interactive efficient buildings. *Applied Energy*, *303*, 117639.

Gai, K., Qiu, L., Zhao, H., & Qiu, M. (2016). Cost-aware multimedia data allocation for heterogeneous memory using genetic algorithm in cloud computing. *IEEE transactions on cloud computing*, *8*(4), 1212-1222.

Gantz, S. D. (2014). *The basics of it audit: Purposes, processes, and practical information*. Elsevier.

Gardner, B., & Thomas, V. (2014). *Building an information security awareness program: Defending against social engineering and technical threats*. Elsevier.

Garg, P., & Singh, D. K. (2021). Analysis of cryptographic encryption algorithm design to Secure IoT Devices: A review. Materials Today: Proceedings.

Ghafir, I., & Prenosil, V. (2014). Advanced persistent threat attack detection: an overview. *Int J Adv Comput Netw Secur, 4*(4), 5054.

Gil-Garcia, J. R., Zhang, J., & Puron-Cid, G. (2016). Conceptualizing smartness in government: An integrative and multi-dimensional view. *Government Information Quarterly, 33*(3), 524-534.

Gillis, A. S. (2021, June 2). *What is a security audit?* SearchCIO. Retrieved December 8, 2021, from https://www.techtarget.com/searchcio/definition/security-audit

Goodman, S. E., & Lin, H. S. (2007). Committee on Improving Cybersecurity Research in the United States Computer Science and Telecommunications Board Division on Engineering and Physical Sciences.

Gope, P., & Hwang, T. (2015). BSN-Care: A secure IoT-based modern healthcare system using body sensor network. *IEEE sensors journal*, *16*(5), 1368-1376.

Gordon, L. A., & Loeb, M. P. (2002). The economics of information security investment. *ACM Transactions on Information and System Security (TISSEC), 5*(4), 438-457.

Hall, R. E., Bowerman, B., Braverman, J., Taylor, J., Todosow, H., & Von Wimmersperg, U. (2000). *The vision of a smart city* (No. BNL-67902; 04042). Brookhaven National Lab., Upton, NY (US).

Hamdoun, H., & Sagheer, A. (2020). Information security through controlled quantum teleportation networks. *Digital Communications and Networks*, *6*(4), 463-470.

Hamid, B., Jhanjhi, N. Z., Humayun, M., Khan, A., & Alsayat, A. (2019, December). Cyber Security Issues and Challenges for Smart Cities: A survey. In *2019 13th International Conference on Mathematics, Actuarial Science, Computer Science and Statistics (MACS)* (pp. 1-7). IEEE.

Han, S. M., Lee, C., Chae, Y. H., & Seong, P. H. (2021). A study on classification of the security controls for the effective implementation to nuclear power plant. *Nuclear Engineering and Technology*.

Hanson, J. (2021, December 20). *How will the Cybersecurity Industry Evolve in 2022?* Help Net Security. Retrieved December 29, 2021, from https://www.helpnetsecurity.com/2021/12/28/cybersecurity-industry-2022/?web_view=true

Heaton, J., & Parlikad, A. K. (2019). A conceptual framework for the alignment of infrastructure assets to citizen requirements within a Smart Cities framework. *Cities*, *90*, 32-41.

Hu, Y., Zhu, P., Xun, P., Liu, B., Kang, W., Xiong, Y., & Shi, W. (2021). CPMTD: Cyber-physical moving target defense for hardening the security of power system against false data injected attack. *Computers & Security*, *111*, 102465.

Ijaz, S., Shah, M. A., Khan, A., & Ahmed, M. (2016). Smart cities: A survey on security concerns. *International Journal of Advanced Computer Science and Applications*, *7*(2), 612-625.

Ilic, J. (2019, December 23). *Cross-site scripting (XSS) makes nearly 40% of all cyber attacks in 2019*. PreciseSecurity.com. Retrieved March 22, 2022, from https://www.precisesecurity.com/articles/cross-site-scripting-xss-makes-nearly-40-of-all-cyber-attacks-in-2019/

International Telecommunications Union (ITU) (2008). ITU-TX.1205: series X: data networks, open system communications and security: telecommunication security: overview of cybersecurity.

Jang-Jaccard, J., & Nepal, S. (2014). A survey of emerging threats in cybersecurity. *Journal of Computer and System Sciences*, *80*(5), 973-993.

Kalinin, M., Krundyshev, V., & Zegzhda, P. (2021). Cybersecurity risk assessment in smart city infrastructures. *Machines*, *9*(4), 78.

Kankanhalli, A., Charalabidis, Y., & Mellouli, S. (2019). IoT and AI for smart government: A research agenda.

Kawyitri, N., & Shekhar, A. (2021). Assessing vulnerability and capacity of Bhubaneswar as a progressive smart-city: An empirical case study of Fani cyclone impact on the city. *International Journal of Disaster Risk Reduction*, *56*, 101986.

Khatoun, R., & Zeadally, S. (2017). Cybersecurity and privacy solutions in smart cities. *IEEE Communications Magazine*, *55*(3), 51-59.

Kitchin, R. (2016). Getting smarter about smart cities: Improving data privacy and data security.

Kodali, R. K., Jain, V., Bose, S., & Boppana, L. (2016, April). IoT based smart security and home automation system. In *2016 international conference on computing, communication and automation (ICCCA)* (pp. 1286-1289). IEEE.

Kosutic, D. (2021a, June 3). *ISO 27001/ISO 27005 risk assessment/treatment: 6-Step Guide*. 27001Academy. Retrieved December 4, 2021, from https://advisera.com/27001academy/knowledgebase/iso-27001-risk-assessment-treatment-6-basic-steps/

Kosutic, D. (2021b, June 3). *ISO 27001/ISO 27005 risk assessment/treatment: 6-Step Guide*. 27001Academy. Retrieved December 4, 2021, from https://advisera.com/27001academy/knowledgebase/iso-27001-risk-assessment-treatment-6-basic-steps/

Kosutic, D. (2022, January 24). *What is ISO 27001? A beginner's guide*. 27001Academy. Retrieved January 10, 2022, from https://advisera.com/27001academy/what-is-iso-27001/

KOSUTIC, D. E. J. A. N. (2017a). *Iso 27001 risk management in plain english;a step-by-step handbook for information security practitioners in small businesses*. ADVISERA EXPERT SOLUTIONS.

KOSUTIC, D. E. J. A. N. (2017b). *Secure & Simple - a small-business guide to implementing Iso 27001 on your own;the plain English, step-by-step handbook for information*. ADVISERA

EXPERT SOLUTIONS.

Kuhl, M. E., Sudit, M., Kistner, J., & Costantini, K. (2007, December). Cyber attack modeling and simulation for network security analysis. In *2007 Winter Simulation Conference* (pp. 1180-1188). IEEE.

Kumar, A. (2021, October 29). *Abu Dhabi, Dubai top smart city index 2021 in Middle East*. Khaleej Times. Retrieved November 19, 2021, from https://www.khaleejtimes.com/uae/abu-dhabi-dubai-top-smart-city-index-2021-in-middle-east.

Kumar, H., Singh, M. K., Gupta, M. P., & Madaan, J. (2020). Moving towards smart cities: Solutions that lead to the Smart City Transformation Framework. *Technological forecasting and social change*, *153*, 119281.

Kumar, P., Khare, M., Harrison, R. M., Bloss, W. J., Lewis, A., Coe, H., & Morawska, L. (2015). New directions: air pollution challenges for developing megacities like Delhi. *Atmospheric Environment*, *122*, 657-661.

Larsen, A. (1999). Global security survey: Virus attack. *Information Week*, (743), 42-4.

Leach, C., & Dana, J. (2016, July 21). Cybersecurity challenges, risks, trends and impacts: Key survey insights. Retrieved October 7, 2021, from https://www2.fireeye.com/MITTR-Cybersecurity-Challenges.html?utm_source=webinar&utm_medium=FEwebportal&utm_campaign=MITTRE.

Leal, R. (2021, August 7). *ISO 31010: Alternative methods for ISO 27001 risk assessment*. 27001Academy. Retrieved December 2, 2021, from https://advisera.com/27001academy/blog/2016/04/04/iso-31010-what-to-use-instead-of-the-asset-based-approach-for-iso-27001-risk-identification/

Lewis, J. A. (2006). Cybersecurity and critical infrastructure protection. *Center for Strategic and International Studies*, *9*.

Li, E., Endter-Wada, J., & Li, S. (2015). Characterizing and contextualizing the water challenges of megacities. *JAWRA Journal of the American Water Resources Association*, *51*(3), 589-613.

Li, D., Ma, J., Cheng, T., van Genderen, J. L., & Shao, Z. (2018). Challenges and opportunities for the development of megacities. International Journal of Digital Earth.

Li, Z., & Liao, Q. (2018). Economic solutions to improve cybersecurity of governments and smart cities via vulnerability markets. *Government Information Quarterly*, *35*(1), 151-160.

Lin, C. W., & Sangiovanni-Vincentelli, A. (2012, December). Cyber-security for the controller area network (CAN) communication protocol. In *2012 International Conference on Cyber Security* (pp. 1-7). IEEE.

Liu, X., Zhang, J., Zhu, P., Tan, Q., & Yin, W. (2021). Quantitative cyber-physical security analysis methodology for industrial control systems based on incomplete information Bayesian game. *Computers & Security*, *102*, 102138.

Lokuketagoda, B., Weerakoon, M. P., Kuruppu, U. M., Senarathne, A. N., & Abeywardena, K. Y. (2018, August). R-Killer: An email based ransomware protection tool. In *2018 13th International Conference on Computer Science & Education (ICCSE)* (pp. 1-7). IEEE.

Lu, Y., & Da Xu, L. (2018). Internet of Things (IoT) cybersecurity research: A review of current research topics. *IEEE Internet of Things Journal*, *6*(2), 2103-2115.

Lueth, K. L. (2022, January 11). *IOT 2021 in review: The 10 most relevant IOT developments of the year*. IoT Analytics. Retrieved March 13, 2022, from https://iot-analytics.com/iot-2021-in-review/

Ma, C. (2021). Smart city and cyber-security; technologies used, leading challenges and future recommendations. *Energy Reports*, *7*, 7999-8012.

Marks, J. (2021, September 21). *Analysis | more secure election machines won't be ready until 2024*. The Washington Post. Retrieved December 30, 2021, from https://www.washingtonpost.com/politics/2021/09/09/cybersecurity-202-more-secure-election-machines-wont-be-widely-used-until-2026/

Masrek, M. N., Harun, Q. N., Ramli, I., & Prasetyo, H. (2019, June). The Role of Top Management in Information Security Practices. In *The 6th International Conference on Education, Social Sciences and Humanities, Istanbul, Turkey* (pp. 24-26).

Maymí, F., & Harris, S. (2021). *CISSP All-in-One Exam Guide* (8th ed.). McGraw Hill.

McLeod, M. S., Payne, G. T., & Evert, R. E. (2016). Organizational ethics research: A systematic review of methods and analytical techniques. *Journal of Business Ethics*, *134*(3), 429-443.

Mellouli, S., Luna-Reyes, L. F., & Zhang, J. (2014). Smart government, citizen participation and open data. *Information Polity*, *19*(1, 2), 1-4.

Merriam-Webster. (n.d.). *Cybersecurity*. Merriam-Webster. Retrieved October 23, 2021, from https://www.merriam-webster.com/dictionary/cybersecurity.

Miller, T., Staves, A., Maesschalck, S., Sturdee, M., & Green, B. (2021). Looking back to look forward: Lessons learnt from cyber-attacks on Industrial Control Systems. *International Journal of Critical Infrastructure Protection*, *35*, 100464.

Miloslavskaya, N. (2021). Network Protection Tools for Network Security Intelligence Centers. *Procedia Computer Science, 190*, 597-603.

Mohamed, N., Al-Jaroodi, J., & Jawhar, I. (2020, July). Opportunities and Challenges of Data-Driven Cybersecurity for Smart Cities. In 2020 IEEE Systems Security Symposium (SSS) (pp. 1-7). IEEE.

Mohammadpourfard, M., Khalili, A., Genc, I., & Konstantinou, C. (2021). Cyber-Resilient Smart Cities: Detection of Malicious Attacks in Smart Grids. *Sustainable Cities and Society, 75*, 103116.

Moore, T., Dynes, S., & Chang, F. R. (2015). Identifying how firms manage cybersecurity investment. *Available: Southern Methodist University. Available at: http://blog. smu. edu/research/files/2015/10/SMU-IBM. pdf (Accessed 2015-12-14)*, *32*.

Morvaj, B., Lugaric, L., & Krajcar, S. (2011, July). Demonstrating smart buildings and smart grid features in a smart energy city. In *Proceedings of the 2011 3rd international youth conference on energetics (IYCE)* (pp. 1-8). IEEE.

Nahar, N. (2021, September 22). *10 importance of information security audit*. ZEVENET. Retrieved December 6, 2021, from https://www.zevenet.com/blog/10-importance-of-information-security-audit/

Nam, T., & Pardo, T. A. (2011, September). Smart city as urban innovation: Focusing on management, policy, and context. In *Proceedings of the 5th international conference on theory and practice of electronic governance* (pp. 185-194).

Neirotti, P., De Marco, A., Cagliano, A. C., Mangano, G., & Scorrano, F. (2014). Current trends in Smart City initiatives: Some stylised facts. *Cities*, *38*, 25-36.

Neumann, P. G. (1994). *Computer-related risks*. Addison-Wesley Professional.

Olga, V., Ruslana, Z., Yuriy, F., & Joanna, N. (2021). Big Data Analysis Methods Based on Machine Learning to Ensure Information Security. *Procedia Computer Science*, *192*, 2633-2640.

Omair, A. (2015). Selecting the appropriate study design for your research: Descriptive study designs. *Journal of Health Specialties*, *3*(3), 153.

Omar, A., Alijani, D., & Mason, R. (2011). Information technology disaster recovery plan: Case study. *Academy of Strategic Management Journal*, *10*(2), 127.

Omar, S. (2021, October 3). *How can governments safeguard smart cities against cybersecurity threats?* EY US - Home. Retrieved December 13, 2021, from https://www.ey.com/en_sy/government-public-sector/how-can-governments-safeguard-smart-cities-against-cybersecurity

Ota, K., Kumrai, T., Dong, M., Kishigami, J., & Guo, M. (2017). Smart infrastructure design for smart cities. *IT Professional*, *19*(5), 42-49.

Ouchani, S. (2021). A security policy hardening framework for Socio-Cyber-Physical Systems. *Journal of Systems Architecture*, *119*, 102259.

Peacock, M. (2014). Detection and control of small civilian UAVs.

Pérez-Martínez, P. A., & Solanas, A. (2011, May). W3-privacy: the three dimensions of user privacy in LBS. In *12th ACM Int'l. Symp. Mobile Ad Hoc Networking and Computing*.

Petrenko, S. A., & Makoveichuk, K. A. (2017). Big data technologies for cybersecurity. In CEUR workshop (pp. 107-111).

Pleban, J. S., Band, R., & Creutzburg, R. (2014, February). Hacking and securing the AR. Drone 2.0 quadcopter: investigations for improving the security of a toy. In *Mobile*

Devices and Multimedia: Enabling Technologies, Algorithms, and Applications 2014 (Vol. 9030, p. 90300L). International Society for Optics and Photonics.

Power, R. (2001). CSI/FBI computer crime and security survey. *Computer Security Journal*, *17*(2), 20-51.

Priester, R., Kenworthy, J., & Wulfhorst, G. (2013). The diversity of megacities worldwide: Challenges for the future of mobility. In *Megacity mobility culture* (pp. 23-54). Springer, Berlin, Heidelberg.

Puri-Mirza, A. (2020a, August 28). *UAE: Number of employed persons in Dubai 2017*. Statista. Retrieved November 20, 2021, from https://www.statista.com/statistics/638359/uae-total-number-of-workforce-in-dubai/.

Puri-Mirza, A. (2020b, August 28). *UAE: Number of employed persons in Abu Dhabi 2017*. Statista. Retrieved November 20, 2021, from https://www.statista.com/statistics/638409/uae-total-number-of-workforce-in-abu-dhabi/.

Raghuvanshi, A., & Singh, U. K. (2020). Internet of Things for smart cities-security issues and challenges. *Materials Today: Proceedings*.

Ramaprasad, A., Sánchez-Ortiz, A., & Syn, T. (2017, September). A unified definition of a smart city. In *International Conference on Electronic Government* (pp. 13-24). Springer, Cham.

Rambabu, K., & Venkatram, N. (2021). Ensemble classification using traffic flow metrics to predict distributed denial of service scope in the Internet of Things (IoT) networks. *Computers & Electrical Engineering*, *96*, 107444.

Saifuzzaman, M., Khan, A. H., Moon, N. N., & Nur, F. N. (2017). Smart Security for an Organization based on IoT. *International Journal of Computer Applications*, *165*(10), 33-38.

Sarker, I. H. (2021). CyberLearning: Effectiveness analysis of machine learning security modeling to detect cyber-anomalies and multi-attacks. *Internet of Things*, *14*, 100393.

Semerci, M., Cemgil, A. T., & Sankur, B. (2018). An intelligent cyber security system against DDoS attacks in SIP networks. *Computer Networks*, *136*, 137-154.

Shrestha, M., Johansen, C., Noll, J., & Roverso, D. (2020). A methodology for security classification applied to smart grid infrastructures. *International Journal of Critical Infrastructure Protection*, *28*, 100342.

Singh, S., Sharma, P. K., Yoon, B., Shojafar, M., Cho, G. H., & Ra, I. H. (2020). Convergence of blockchain and artificial intelligence in IoT network for the sustainable smart city. *Sustainable Cities and Society*, *63*, 102364.

Skatkov, A. V., & Shevchenko, V. I. (2015). Expansion of the Reference Model of the Cloud Computing Environment in the Concept of Large-Scale Scientific Research. *Trudy Instituta sistemnogo programmirovaniia RAN*, *27*(6), 285-306.

Spiekermann, S., & Cranor, L. F. (2008). Engineering privacy. *IEEE Transactions on software engineering*, *35*(1), 67-82.

Staricco, L. (2013). Smart Mobility: opportunità e condizioni. *TeMA-Journal of Land Use, Mobility and Environment*, *6*(3), 342-354.

Stytz, M. R. (2003). Security in computing, [Book Review]. *IEEE Security & Privacy*, *1*(04), 14-14.

Tankard, C. (2016). What the GDPR means for businesses. *Network Security*, *2016*(6), 5-8.

Tariq, M. I. (2019). Agent based information security framework for hybrid cloud computing. *KSII Transactions on Internet and Information Systems (TIIS)*, *13*(1), 406-434.

Ten, C. W., Manimaran, G., & Liu, C. C. (2010). Cybersecurity for critical infrastructures: Attack and defense modeling. *IEEE Transactions on Systems, Man, and Cybernetics-Part A: Systems and Humans*, *40*(4), 853-865.

Thomas, J. (2018). Individual cyber security: Empowering employees to resist spear phishing to prevent identity theft and ransomware attacks. *Thomas, JE (2018). Individual cyber security: Empowering employees to resist spear phishing to prevent identity theft and ransomware attacks. International Journal of Business Management*, *12*(3), 1-23.

Tragos, E. Z., Angelakis, V., Fragkiadakis, A., Gundlegard, D., Nechifor, C. S., Oikonomou, G., ... & Gavras, A. (2014, March). Enabling reliable and secure IoT-based smart city applications. In *2014 IEEE International Conference on Pervasive Computing and Communication Workshops (PERCOM WORKSHOPS)* (pp. 111-116). IEEE.

Trang, S., & Nastjuk, I. (2021). Examining the role of stress and information security policy design in information security compliance behaviour: An experimental study of in-task behaviour. *Computers & Security*, *104*, 102222.

United Nations (UN). (2016). The world's cities in 2016.

Usmonov, B., Evsutin, O., Iskhakov, A., Shelupanov, A., Iskhakova, A., & Meshcheryakov, R. (2017, November). The cybersecurity in development of IoT embedded technologies. In 2017 International Conference on Information Science and Communications Technologies (ICISCT) (pp. 1-4). IEEE.

Vaidya, G., Nambi, A., Prabhakar, T. V., & Sudhakara, S. (2021). Towards generating a reliable device-specific identifier for IoT devices. Pervasive and Mobile Computing, 76, 101445.

Vignoli, F. (2021, May 24). *Securing a smart city approach: The Ecosystem of Cybersecurity*. WORKTECH Academy. Retrieved December 13, 2021, from https://www.worktechacademy.com/securing-a-smart-city-approach-the-ecosystem-of-cybersecurity/

Von Solms, R., & Van Niekerk, J. (2013). From information security to cyber security. *computers & security*, *38*, 97-102.

Wataya, E., & Shaw, R. (2019). Measuring the value and the role of soft assets in smart city development. *Cities*, *94*, 106-115.

Watson, D. L., & Jones, A. (2013). *Digital forensics processing and procedures: Meeting the requirements of ISO 17020, ISO 17025, ISO 27001 and best practice requirements*. Newnes.

Whitman, M. E., & Mattord, H. J. (2013). *Management of information security, Fourth edition*. Cengage Learning.

Whitman, M. E., & Mattord, H. J. (2018). *Principles of information security, sixth edition*. Cengage learning.

Wiles, J., Claypoole, T., Drake, P., Henry, P. A., Johnson, L. J., Lowther, S., ... & Windle, J. H. (2008). *Techno Security's Guide to Securing SCADA: A Comprehensive Handbook On Protecting The Critical Infrastructure*. Syngress.

Wright, C. S. (2008). Assessing security awareness and knowledge of policy. *The IT regulatory and standards compliance handbook: how to survive information systems audit and assessments. Syngress*, 161-94.

Xu, J., Wang, X., & Yan, L. (2021). The moderating effect of abusive supervision on information security policy compliance: Evidence from the hospitality industry. *Computers & Security*, *111*, 102455.

Yamin, M. M., Katt, B., & Nowostawski, M. (2021). Serious games as a tool to model attack and defense scenarios for cyber-security exercises. *Computers & Security*, *110*, 102450.

Zhang, R., & Hu, Z. (2021). Access control method of network security authentication information based on fuzzy reasoning algorithm. *Measurement*, *185*, 110103.

Zhu, N., Diethe, T., Camplani, M., Tao, L., Burrows, A., Twomey, N., ... & Craddock, I. (2015). Bridging e-health and the internet of things: The sphere project. *IEEE Intelligent Systems*, *30*(4), 39-46.

Zissis, D., & Lekkas, D. (2012). Addressing cloud computing security issues. *Future Generation computer systems*, *28*(3), 583-592.

Appendix

Cybersecurity challenges in smart cities – questions	
(1)	What are your organization's top information-security challenges?
(2)	Where do you see the most growth in security threats?
(3)	Across your organization, do you feel that you are experiencing more, fewer, or the same number of data attacks today compared with two years ago?
(4)	On a scale of 1 ("inadequately prepared") to 5 ("extremely well prepared"), how prepared is your organization to respond to an incident involving a material loss of information?
(5)	Does your organization have an information risk-management strategy?
(6)	How have security breaches impacted your organization in the past two years?
(7)	How prepared is your organization to detect each of the following kinds of security threats?
(8)	Does your organization currently have a plan for communicating with internal and external stakeholders following a security breach?
(9)	How do you rate your level of security in each of the following areas?
(10)	How prepared is your organization to prevent each of the following kinds of security threats?
(11)	How prepared is your organization to respond to each of the following kinds of security threats?
(12)	Of the following, what cybersecurity threats are you familiar with?
(13)	Compared to a few years ago, do you feel that it's easier or more difficult to do the following?
(14)	Of the following, what measures do you take to protect yourself online?
(15)	Does your organization have an information risk-management roadmap or tactical plan?
(16)	How frequently is your organization's information risk-management roadmap or plan updated?
(17)	How often does your organization perform information risk assessments (that is, measure the inherent risk for the business or company)?

(18)	If your organization has been breached, what changes to operations, compliance processes, and other activities did it make to help prevent and/or detect future breaches?
(19)	To what extent is your organization able to recruit, develop, and retain security talent?
(20)	For which of the following security- and risk-related functions does your organization currently use third-party service providers?
(21)	Do you believe the management team or executives at the highest level of your organization truly understand the time and resources needed to mitigate risk and minimize cyberthreat exposure?
(22)	What percentage of your IT budget is earmarked for cybersecurity?