حكومة دبي
GOVERNMENT OF DUBAI

مركز دبي للأمن الإلكتروني
DUBAI ELECTRONIC SECURITY CENTER

DUBAI CYBER SECURITY STRATEGY

Establishing Dubai as a global leader
in innovation, safety and security

DUBAI CYBER SECURITY STRATEGY

Version 1.0
by Dubai Electronic Security Center

His Highness Sheikh Mohammed bin Rashid Al Maktoum

Vice President and Prime Minister
of the UAE and Ruler of Dubai

Challenges have never prevented us from pursuing our ambitions, and they never will. We are determined to transform challenges into opportunities for creativity and innovation, and explore new ideas and initiatives that can help us achieve our aspirations.

The Dubai Cyber Security Strategy, which adds to the government's numerous achievements, gives further impetus to our journey of excellence in cyber space.

On the occasion of the launch of this Strategy, I would like to thank all those who contributed to its development and call on them to recommit to the highest excellence and leadership and forge ahead with our goals so that we can create even more happiness and prosperity for our people.

We have great confidence in the ability of the government and private sectors in the UAE to successfully implement the Dubai Cyber Security Strategy. Let us double our efforts and work diligently to make the UAE one of world's digitally safest countries.

— His Highness Sheikh Mohammed bin Rashid Al Maktoum

His Highness Sheikh Hamdan bin Mohammed bin Rashid Al Maktoum

Crown Prince of Dubai and Chairman
of the Executive Council

“A new history of Dubai is being created and signed by Mohammed bin Rashid Al Maktoum.”

— His Highness Sheikh Hamdan
bin Mohammed bin Rashid Al Maktoum

FOREWORD

Thanks to the technological leadership, which constitutes one of the major pillars of the city, Dubai is now a leading international hub and an attractive investment destination for national, regional and international institutions. Also, the huge technological advancements happening across the region have contributed in attracting the countries attention around the world to Dubai.

The goals of technological development will never be met in the absence of supportive frameworks that promote the security and safety of information systems. Therefore, establishing a reliable and safe cyber space is essential to continuing the development march and facing future challenges.

In line with the vision of Vice President and Prime Minister and Ruler of Dubai, His Highness Sheikh Mohammed bin Rashid Al Maktoum to place Dubai among the most secure cities electronically in the world, we have launched the Dubai Cyber Security Strategy, which defines Dubai's vision and objectives in this regard. The plan provides rules protecting the data and electronic services from threats and attacks, as well as protects companies, individual users or any information technology-related activities.

The path to become a smart city is full of challenges, however, this will not prevent us from achieving our goals. We will continue the hard work with the determination and perseverance we have learned from our role models and leaders in the UAE in order to make Dubai one of the most secure cities electronically worldwide – just as His Highness Sheikh Mohammed bin Rashid Al Maktoum envisions.

Raising the awareness of cyber security is a key element of promoting the success of the strategy. The goal is to build a more secure information society that is perfectly aware of cyber security risks. One of the key objectives of this strategy is to address any risks, threats or attacks, as well as allowing user access to various aspects of information technology so as to promote the success of the strategy in the future.

Achieving these objectives depends upon the participation and cooperation of all the governmental and non-governmental sectors in the city. Let us all work as one team, as per the directives of His Highness Sheikh Mohammed bin Rashid, in order to lay a solid basis for a free and secure cyber world that fosters scientific research and innovation.

– H.E. Yousuf Al Shaibani
DESC Executive Director

1 INTRODUCTION

The growth of the internet and cyber space has had a tremendous impact on all parts of society, ranging from the public and private sectors to the individual. Our daily lives, social interactions and economies depend on information and communication technologies working reliably, seamlessly and securely. An open and free cyber space provides value by reducing barriers to trade, as well as barriers between countries, communities and citizens, and allowing information sharing across the globe. It is important to protect this value against the risks of malicious activities and disruptions — only a secure cyber space can provide trust and confidence for the individuals, businesses and the public sector.

Dubai is a major target for malicious actors using the cyber space for their attacks. This can affect Dubai's public and private sectors, as well as individuals in many different ways. Statistics show that these problems are rapidly increasing, and the methods employed in malicious attacks are becoming even more sophisticated.

The Dubai Plan 2021 describes the future of Dubai through holistic and complementary perspectives, starting with the people and the society. The plan addresses the urban environment including both natural and built assets. It looks at the living experience of the people of Dubai and its visitors as a result of their interaction with this environment and the economic and social services provided. Several goals of the Dubai Plan 2021 are supported by this strategy, particularly the following statement:

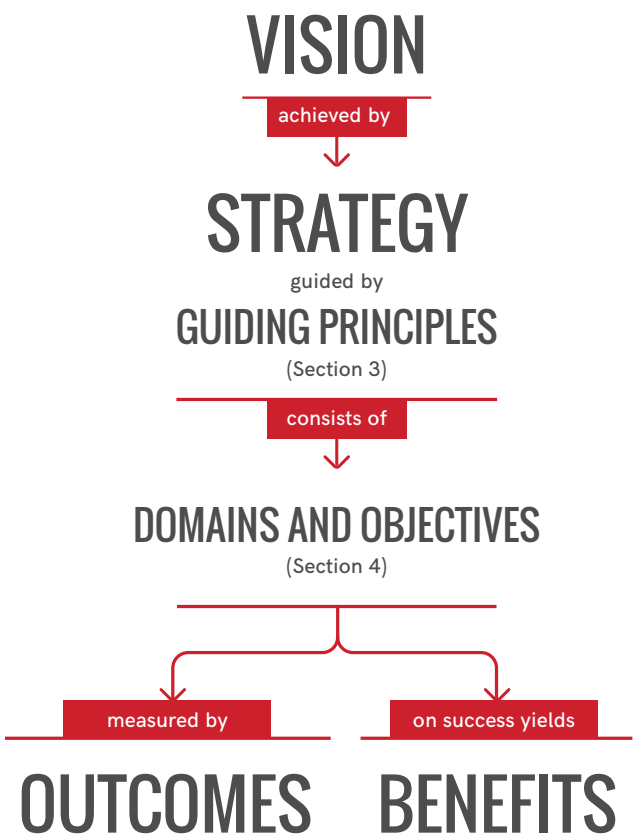
> "The Most Secure Place: A feeling among residents and workers living in Dubai and tourists visiting Dubai, that the city is a safe and secure place and that any personal security concerns are dealt with efficiently and transparently by law enforcement authorities."▲

▲ See Dubai Plan 2021, "The Experience", Aim 3

The Dubai Electronic Security Center (DESC) was founded pursuant to Law No. 11 in 2014 with the aim to develop and implement information security practices and set good-practice criteria for cyber security, across the Emirate. DESC's strategic plan includes initiatives to combat threats, cyber attacks, and cyber crime.

DESC has created this strategy to help protect Dubai from cyber security risks with the aim of supporting the growth and innovation of Dubai and its economy. This strategy describes the actions required to reduce risks and secure the benefits of a trusted cyber space for organizations and individuals in Dubai. It details what organizations and individuals can do to contribute to a safe and secure cyber space, thereby supporting Dubai's future success. The timeline for the implementation of this strategy is five years.

The following picture illustrates how the different elements of this strategy relate to each other.



2 WHY THIS STRATEGY?

This section describes the opportunities for growth and innovation existing in the cyber space and the associated cyber security risks in more detail.

2.1 GLOBAL CONNECTIONS

In December 2016, more than 91% of the UAE population used the internet. The internet-based economy continues to grow at a fast rate. New developments such as cloud, internet of things and smart cities all make use of the interconnectivity provided by the cyber space. Therefore, the UAE population's exposure to cyber space is likely to increase. Public and private sectors are also benefiting from improved online and mobile technologies, for example by the creation of products and services tailored and delivered according to individual needs.

Along with the increased connectivity, physical objects and people in real world become interconnected without physical constraints. This leads to an "interconnected information society" where physical space and cyber space are more integrated through the free flow of information and communications. This will enable Dubai and its citizens to create innovative products and services, thereby generating new value exponentially.

However, such value may only be realized if the use of the cyber space is secure. People need to be confident that the networks which support private and business activities, and economic prosperity are safe and resilient. DESC has created this cyber security strategy to protect Dubai's public and private sectors and individuals from these cyber crimes and other cyber risks. As such, the implementation of this strategy is one of its highest priorities.

▲ http://www.internetworldstats.com/me/ae.htm

2.2 THREATS AND RISKS OF CYBER SPACE

The cyber space attacks lead to a variety of threats, such as:

- FRAUD
- ESPIONAGE
- TERRORISM
- VIOLATION OF PRIVACY
- DEFAMATION

These threats already affect the public and private sectors, and the individuals in Dubai using the cyber space. The UAE is a large target for attackers; in 2016, 5.14 billion dirhams were lost through cyber crime.▲

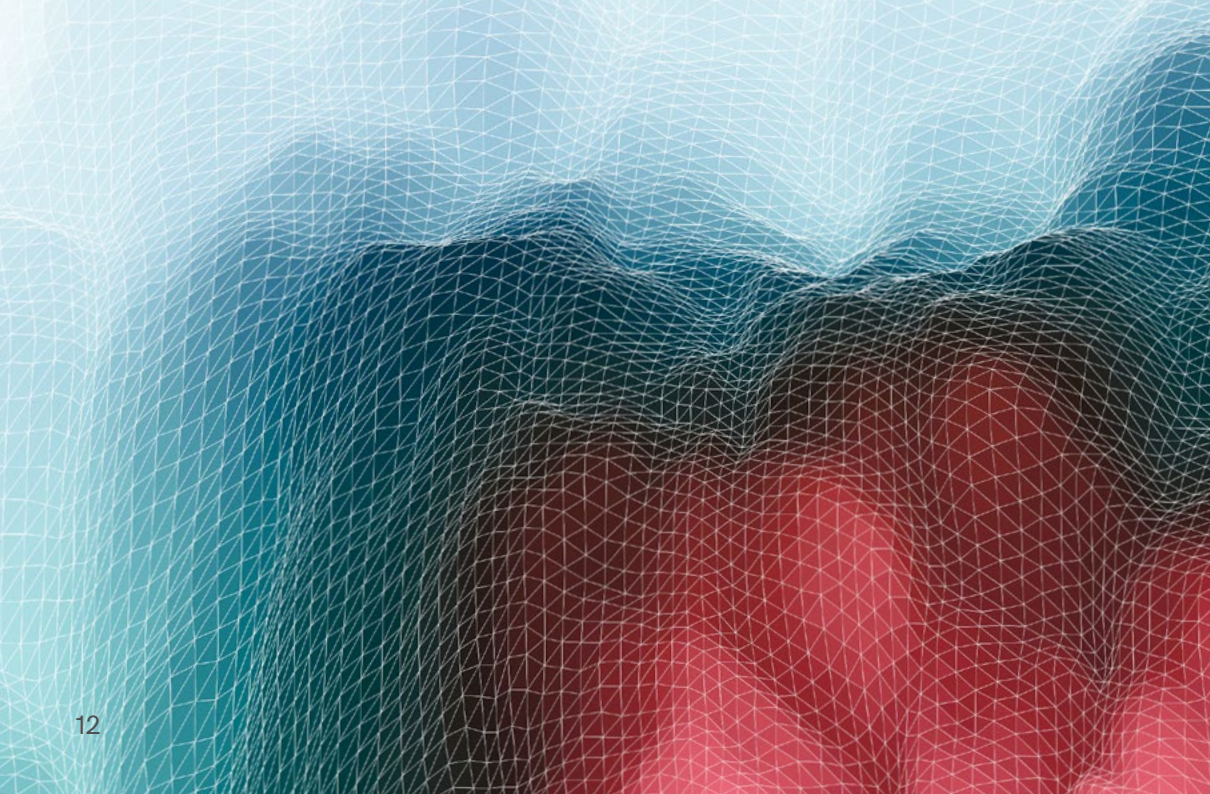
Published figures show the continuous rise of cyber crime in the UAE.◆ According to Dubai Police, around one in five residents in the UAE were victims of cyber crime in 2015, and reports of cyber crime increased by 23% in 2015 alone. It is expected that these rates will grow even faster at least until the year 2020.

The Dubai Electronic Security Center■ in Dubai has been set up according to the law of its establishment to protect against cyber crime and hacking and develop both technical and non-technical solutions to keep up with this situation.

▲ http://gulfnews.com/business/sectors/technology/cybercrime-cost-uae-dh5-14b-this-year-1.1933736

◆ http://www.arabianbusiness.com/dubai-cybercrime-rises-23-percent--621167.html

■ http://gulfnews.com/news/uae/government/cyber-security-centre-established-in-dubai-1.1346144



3 GUIDING PRINCIPLES

There are some underlying guiding principles that need consideration to achieve the objective of this strategy:

3.1 FREE FLOW OF INFORMATION

Everyone should have the ability and right to access the cyber space in terms of skills, technology and opportunity. The cyber space needs to remain open to innovation and free flow of ideas, information, and expression. This requires security and reliability of the information used. Information should not be altered without any legitimate reason, and shall be delivered to intended recipients.

There is a need to respect individual rights of privacy and provide proper protection to intellectual property. In this sense, due consideration should be made to maintain the proper balance between open technology and the individual rights of privacy. Overall, the cyber space should be a competitive environment which ensures a fair return on investment in infrastructure, services and content.

In Dubai, the free flow of information across the public and private sectors, investors, residents and visitors is supported by the Dubai Data Manual, led by the Dubai Data Establishment.

> "Our aim is not to have the most data, but to unleash the greatest value from data, creating new opportunities and improved experiences for all."
>
> — His Highness Sheikh Mohammed bin Rashid Al Maktoum

The Dubai Data Manual sets out the guidance to be followed by Dubai Government entities to manage their data, in alignment with the Dubai Government's commitment to agile development of user-centric and data-driven services.

Dubai's vision is contingent upon the free flow of information where the public sector has embarked upon a programme to transform Dubai into the smartest, happiest city in the world. Data and information will be the "new currency" by which the public and private sectors, citizens and residents will exchange value and develop new, innovative ways to live, learn and do business in a culture of secure data sharing.

3.2 CONSIDERATION OF RISK

It is important for individuals using the cyber space to understand that absolute security cannot be achieved. Public and private sector organizations, as well as individuals using the cyber space should be fully aware of the risks they could be facing. This all-pervasive awareness contributes more to cyber security than any single organization can.

The proactive risk assessment is a core component of Dubai's Information Security Regulations (ISR). The implementation of the ISR is already mandatory for Dubai's public sector, and it is highly recommended for the private sector to also apply ISR, or similar standards (based on their business requirements), such as ISO/IEC 27001 or the National Electronic Security Authority (NESA) Information Assurance Standard (IAS). It is important to note that all the above standards place similar emphasis on undertaking information security risk assessments. Additionally, their approach to risk assessments are compatible, and can be used in combination with each other. Although individual citizens will not perform a risk assessment, the Cyber Security Strategy will address the risks faced through its Cyber Smart Society domain.

3.3 COLLABORATION

The cyber space interconnects in multiple dimensions and cannot be addressed by Dubai's public sector alone, nor managed by just one country or city. Dubai's public sector needs to work hand in hand with the private sector and individuals. All cyber space stakeholders, including the Critical Information Infrastructure (CII), should share a common vision of cyber security and fulfill their responsibilities for cyber security and cyber resilience. It is important that all organizations and individuals understand their responsibilities in achieving a secure cyber space (this is also further addressed in National and International Collaboration domain later in the document).

Similarly, the risks of the cyber space is transnational. Therefore, Dubai needs to seek partnerships with other regional and international cities, countries, initiatives; the risks cannot be managed through Dubai's defense alone.

Countries can protect against threats through better cooperation between Computer Emergency Response Teams (CERTs) and concerted efforts at international diplomacy. Such interaction can be supported by the use of international standards, such as ISO/IEC 27001, which interface well with Dubai's Information Security Regulations. International collaboration should also seek harmonization in the legal field.

> "I believe that if the vision is clear then the objectives can be easily achieved."
>
> — His Highness Sheikh Mohammed bin Rashid Al Maktoum

3.4 COMPLIANCE WITH REGULATIONS

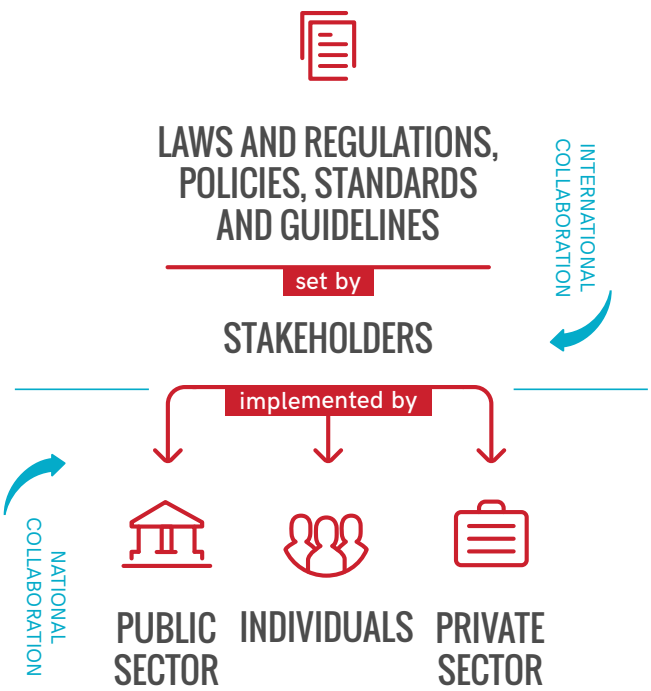
All applicable laws and regulations should be applied to the cyber space in order to achieve cyber security and enhance awareness of all society about the importance of compliance with legislation. Legislation taken into consideration when developing this strategy includes:

- Federal Law No. (7) of 2002 on Intellectual Property
- Federal Law No. (1) of 2006 on Electronic Commerce and Transactions
- Federal Law No. (5) of 2012 on Cyber crime Prevention
- Law No. (4) of 2016 on Dubai Economic Security Center
- The Executive Council of Dubai Government Resolution No. (13) of 2012 for Information Security Regulation in Dubai Government

It is required to establish international rules and norms in conformity with universal values as cyber space is not restricted to Dubai.

3.5 CYBER SECURITY ARCHITECTURE

Different stakeholders need to work together to implement the cyber security strategy and provide Dubai's public and private sectors, and individuals with a safer cyber space. The cyber security architecture depicted below illustrates the different responsibilities in the overall cyber security programme:



4 STRATEGY DOMAINS AND OBJECTIVES

The Cyber Security Strategy has a set of main domains, which, together with the guiding principles listed in Section 3, will be established and implemented to achieve cyber security.

CYBER SMART SOCIETY

Achieving awareness, skills and capabilities to manage cyber security risks for Dubai's public and private sectors, and individuals

INNOVATION

Promoting research and development for cyber security, and establishing a free, fair and secure cyber space in Dubai

CYBER SECURITY

Putting controls in place to protect confidentiality, integrity and availability, as well as data privacy for Dubai's public and private sectors, and individuals

CYBER RESILIENCE

Ensuring the continuity of IT systems and their availability in the cyber space

NATIONAL AND INTERNATIONAL COLLABORATION

Establishing national and international collaboration to manage cyber risks

The Cyber Security Strategy is implemented by different stakeholders, that all need to achieve their objectives and work together to create a secure cyber Dubai. These objectives are outlined in the sections later in the document.

CYBER SMART SOCIETY

The aim of the Cyber Smart Society domain is to ensure that all people in Dubai have sufficient knowledge, understanding and awareness of cyber security, and their related responsibilities. This includes training for employees of the public and private sectors in Dubai, as well as awareness programmes for children, students and other individuals. Another objective of this domain is to establish programmes for students, professionals and experts to increase their knowledge on cyber security.

> **"The future belongs to those who can imagine it, design it, and execute it."**
>
> — His Highness Sheikh Mohammed bin Rashid Al Maktoum

1 Availability of knowledgeable, experienced and trained personnel specialized in cyber security for public and private sector organizations

Organizations (public and private sectors) should be encouraged to build a well educated workforce with sufficient cyber security knowledge, as required for their roles and responsibilities. It is important to have such workforce in place to be able to manage incidents and protect the organization, as well as to be proactive (not reactive) to cyber security threats. Building such workforce should be supported by trainings, conferences and workshops. The results should be continuously monitored and measured.

2 Cyber security awareness should be provided to public and private sectors' employees

Organizations (public and private sectors) should provide awareness of cyber security threats, risks, and the required protection measures taken to their employees.

This should include the employees' responsibilities for information security, why their support is needed, and what happens if cyber security policies and procedures are violated.

Organizations should implement a holistic and continuously developing awareness programme, addressing the different target groups of employees, including newcomers.

3 Provision of cyber security awareness to individuals

More people have been subject to cyber attacks in the last years, and this number is rapidly increasing. This trend is expected to continue rising especially with new technologies that will take more part in our lives.

Schools, universities and other entities need to develop awareness campaigns and provide awareness to individuals about cyber security, and the possibilities of threats and risks in the cyberspace. The campaigns should be oriented to target groups using different forms of delivery to raise the awareness for cyber security. The campaigns should also use the offers made by DESC and other entities to learn more about cyber security.

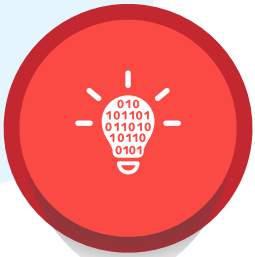
4 Raising the skills of cyber security experts

Dubai public sector, schools and universities should work together to increase the number of cyber security experts. This development needs strategic planning, and schools and universities should include cyber security in their curricula, by adding study subjects covering cyber specific topics.

Universities and industry should work together to establish a plan for cyber security to raise the number of security experts, and motivate people towards this subject.

There should also be training programmes for individuals to increase their cyber security knowledge, e.g. people working in organizations with a job that includes cyber security responsibilities. A certification scheme for cyber security professional might also be developed, e.g. using ISO/IEC 27021.

Collaboration with other institutions should also be sought to develop security products and services that will be included in educational activities within the schools and/or universities, for example as guest lecturers.



INNOVATION

The aim of the Innovation domain is to support research and development (R&D) activities, develop new technologies, and innovate new certification schemes for products or people to support the inclusion of cyber security in relevant innovations.

> **"Innovation is continuous and does not stop at any limits or borders."**
>
> — His Highness Sheikh Mohammed bin Rashid Al Maktoum

1 Promotion of research and development activities that support a secure cyber space

The threats and risks in the cyber space will become more sophisticated as technology develops. Therefore, research and development (R&D) is needed to protect successfully against the cyberattacks to come.

Dubai's public and private sectors need to promote productive R&D. This should include the following initiatives:

- Adoption of laws and regulations, where necessary
- Inclusion of security in products and services in the design stage
- Promotion of interdisciplinary research
- More advanced monitoring and detection measures
- Using new technologies, such as artificial intelligence (AI), to increase the defense capabilities
- Using national and international collaboration (refer also to National and International Collaboration domain)

2 Adoption of cyber security in new technologies

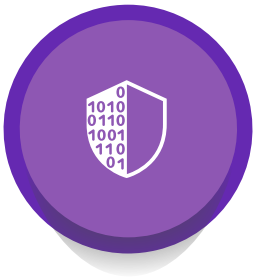
New technologies, such as the internet of things (IoT) or smart cities provide huge opportunities for Dubai, but can also pose risks as attackers might use these technologies to their advantage.

It is therefore important to create secure systems and include security as an inherent part of their design, for the production of IoT devices as well as when designing smart cities.

This should be supported by an incentive scheme that rewards organizations addressing cyber security in their products.

3 Introduction of new certification schemes for cyber security

Dubai's public sector should introduce new certification schemes that address security in new technologies (more granular schemes might be required for different technologies) and consider technology requirements for secure devices, as well as the use of sector-specific management system certification, e.g. for cloud service providers. The standard(s) for this scheme and the associated certifications need to be developed and should be based on international best practices.



CYBER SECURITY

The aim of the Cyber Security domain is to ensure that organizations in the public and private sectors, particularly all those involved in the CII, implement information security management system standards. It is crucial that senior executives of organizations understand the importance of information security.

In addition, a set of baseline security controls for individuals will be developed and the support will be provided for their implementation. Information and cyber security standards and guidelines will also be developed to further support the implementation of cyber security.

> "A new history of Dubai is being created and signed by Mohammed bin Rashid Al Maktoum."
>
> — His Highness Sheikh Hamdan bin Mohammed bin Rashid Al Maktoum

1 Senior executive management needs to understand the importance of cyber security

Senior executive management of an organization needs to understand that cyber security is an important asset, which allows organizations to grow and achieve their business objectives and promote cyber security controls as an "investment" for more progressive management.

2 Implementation of an information security management system (ISMS) standard

There are different standards that organizations in Dubai can benefit from. These standards will help achieve a common baseline for protection across the different organizations of Dubai. The Information Security Regulations (ISR) is mandatory for Dubai's public and semi-public sectors. The private sector should also consider implementing ISR, or other applicable standards, such as ISO/IEC 27001 and/or NESA UAE IAS for their information security management system. This is particularly important for organizations that are part of the CII. Other standards that can be considered are ISO/IEC 27035 (for incident management), ISO/IEC 27031 (ICT readiness for business continuity), or ISO 22301 and/or NCEMA 7000 (both for business continuity). The implementation of such standards has a number of important cornerstones:

Responsibilities for cyber security need to be assigned. In addition to the necessary knowledge, expertise and training that people responsible for cyber security should have, it is a fundamental prerogative for the success of this role that there is access to senior executive management. This is particularly needed for proper decision making.

Each organization needs to understand their exposure to cyber security risks. A method should be defined to carry out a risk assessment (refer also to the guiding principle "Consideration of Risk") and the appropriate level of detail that provides enough information to decide on solutions.

Based on the understanding of their individual risks, organizations need to develop and implement appropriate solutions. This can be done using either internationally or locally accepted standards as listed above. This solution design should take into account any existing security controls and set ownership, responsibilities or timelines for actions.

3 Establishment of a set of baseline controls for cyber security, and support of their implementation

A lot of cyber attacks are successfully exploiting vulnerabilities of the systems targeted. Whilst attacks on specific aims (banks, public sector, etc.) become increasingly sophisticated, the attacks at individuals are still often simple (e.g. phishing attacks or password cracking). Raising the bar of protection of individual systems can therefore help to counter the attacks.

A set of baseline controls should be established, maintained and supported by Dubai individuals in their implementation. Such protection may include:

- Protection against malicious software
- Good password selection and management (including for IoT devices)
- Use of appropriate firewall and network security tools
- Applying system updates in a timely manner
- Careful use of social media
- Maintaining physical security of computers and devices in public
- Responsible public Wi-Fi use, and securing your own Wi-Fi network

Encouragement to apply and maintain such protections should be supported by the aforementioned rewards programme and by the provision of tools to check parts of the security status of a system.

4 Continuous development of information and cyber security services standards and guidelines

DESC has developed the Information Security Regulations (ISR), which is mandatory for Dubai's public and semi-public sectors. DESC also provides an auditing function to verify that the standard has been implemented correctly.

DESC has also developed this Cyber Security Strategy and is specialized to develop further standards and guidelines, including future service providers.

DESC will also collaborate with competent authorities to set further standards, guidelines and tools that can help Dubai's public sector, private sector and individuals to increase their cyber security capabilities.

CYBER RESILIENCE

The aim of the Cyber Resilience domain is to ensure that organizations of Dubai's public and private sectors, particularly organizations in the CII are resilient to cyber attacks and can continue their important business operations even in cases of problems.

A key element to delivering such resilience is the establishment of a facility that provides support for the management of cyber security incidents, threat intelligence and a platform for information sharing.

To achieve sufficient cyber resilience, it is necessary that organizations in the public and private sectors, particularly all those involved in the CII, implement standards to support IT system continuity, disaster recovery and wider business continuity.

> "We offer the world a new and unique model of developing cities which is always in need of different ideas and innovative creations."
>
> — His Highness Sheikh Mohammed bin Rashid Al Maktoum

1 Incidents should be reported, and information about cyber security risks should be shared

Organizations should share information about cyber security risks and incidents, and use the centralized infrastructure for incident management, which helps to:

- Prevent incident spread
- Allow for reporting of incidents
- Set an overall scheme for reporting, analyzing and projecting the future

As the service providers are at the forefront of cyber security attacks, incidents and events, their collaboration and reporting is particularly important to allow for the well-functioning of cyber security services.

2 Establishment, maintenance and improvement of defined cyber security and cyber resilience capabilities

The cyber space includes telecom, internet service providers, organizations developing software, digital devices, etc., and organizations that provide services over the internet. All organizations playing an important role in Dubai's cyber space should follow a set of rules to ensure that the cyber space is sufficiently secure. This is particularly the case for those organizations forming part of Dubai's CII.

It is important that these organizations establish a framework that supports effective maintenance and continuous improvement of their cyber security capabilities, e.g. through the implementation of ISR.

3 Provision of support for incident management, threat intelligence, and a platform for information sharing

DESC will provide the following functionalities for Dubai's public and semi-public entities:

- Incident monitoring, management and handling
- Information about trends, issues, and new threats in the cyber space
- Threat intelligence by linking different sources and using the information and technical capabilities available in DESC to form an integrated picture
- A platform for information sharing in relation to cyber Dubai, its possibilities, strength and risks

4 Compliance with cyber resilience standards

Provisions should be made to ensure continuation of all functions that are critical to the cyber space. Standards related to business continuity and ICT readiness (ISO/IEC 27031 (ICT readiness for business continuity), ISO 22301 and/or NCEMA 7000 (business continuity)) can be helpful to achieve this.

Service providers, both present and future, operating within Dubai (e.g. cloud service providers), or internet communication services (such as communication as a platform) should be required to comply with a set of rules defined by DESC to ensure they are not compromising the security of the cyber space in Dubai.

Organizations in the private sector, particularly those in the CII, should also consider to implement such standards.

NATIONAL AND INTERNATIONAL COLLABORATION

The aim of this domain is to facilitate all national and international collaboration necessary to make Dubai's cyber space secure and resilient.

The national collaboration addresses the identification of organizations forming the CII of Dubai, and the establishment of a scheme that allows for secure information exchange, communication and collaboration and motivates private organizations not in the CII to join collaborative efforts. The international collaboration focuses on common regulations and global threats.

Where necessary, new legislation or regulations should be established to facilitate cyber Dubai.

> "We have a clear goal; we want Dubai to be the smartest city in the world."
>
> — His Higness Sheikh Hamdan bin Mohammed bin Rashid Al Maktoum

1 Establishment of international collaboration

Cyber space is a shared space where communications and information exchange take place on the global level. Therefore, international collaboration is necessary to address the global issues related to cyber security. International collaboration will be established to:

- Combat cyber threats and risks
- Develop legislation, regulations and standards
- Identify particular nations for collaboration/research

DESC and other law enforcement agencies are currently building many international collaborations to combat cyber crimes and secure the cyber space within Dubai.

2 Collaboration between organizations forming part of the CII and establishment of partnerships with public and private sectors

Dubai public sector needs to build a national initiative for the collaboration organizations forming part of Dubai's CII and make them work together to establish Cyber Dubai. This collaboration includes several activities:

- Establishment of a scheme to exchange information between CII organizations
- Collaboration and communication between CII organizations (this can benefit from the requirements and guidance provided in ISO/IEC 27010)
- Provision of support from Dubai's public sector
- Establishment of an incentive scheme to encourage the private sector (not part of the CII) to participate in cyber security

In addition, Dubai's public sector needs to collaborate with federal organizations addressing cyber security in the UAE and its CII.

3 Establishment of cyber security legislation and regulations

Cyber crime can take many different forms, ranging from harmful digital communications of a criminal nature (cyberbullying), to violation of intellectual property given the broad scope of cyber crime and the range of organizations threatened, this particular area needs more detailed legal action to address cyber crime.

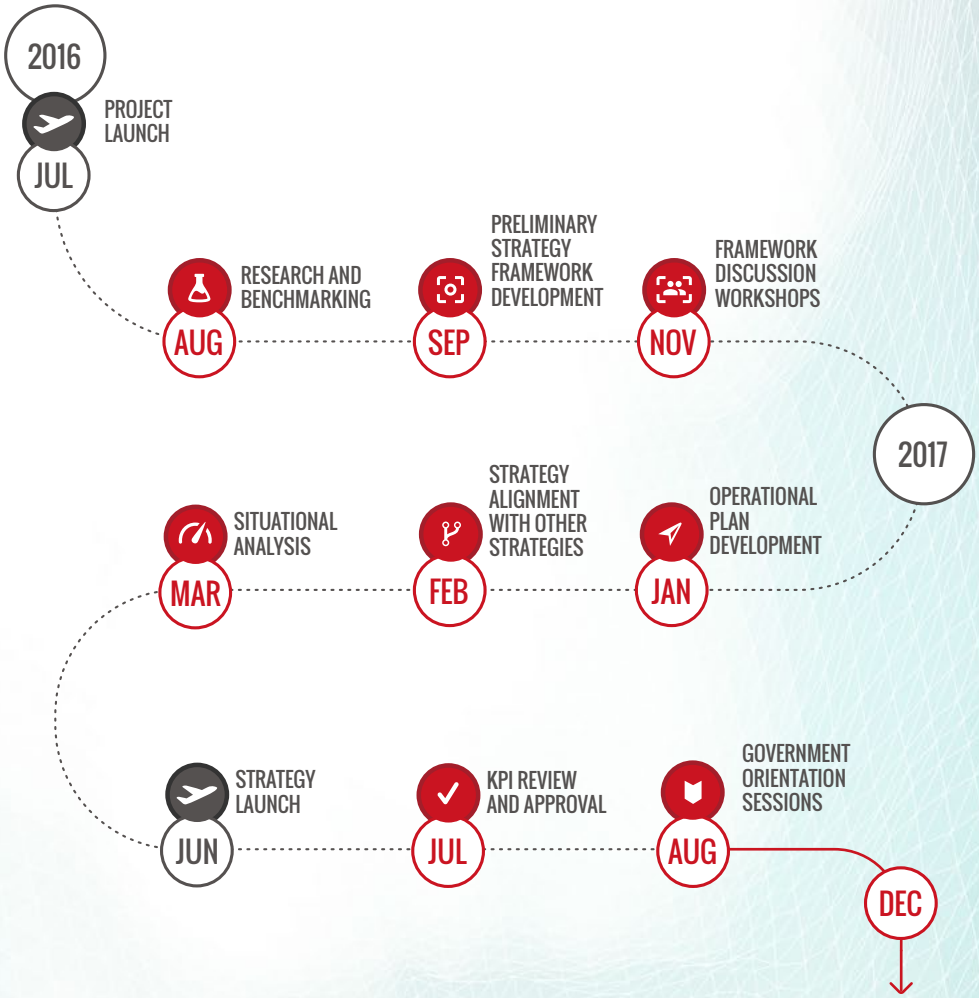
Establishment of cyber security legislation and regulations requires the involvement from both the public and private sectors in Dubai, and in particular, agreements need to be established across borders to manage cyber crimes.

DEVELOPMENT JOURNEY

In 2016, DESC decided to develop a Cyber Security Strategy to protect Dubai from cyber security risks with the aim of supporting the growth and innovation of Dubai and its economy. The Cyber Security Strategy will impact all different sectors in Dubai, including the public and private sector, as well as the individuals. Therefore, the strategy was developed in cooperation with different stakeholders representing these different sectors.

The development of the Cyber Security Strategy started by a benchmarking exercise, in which cyber security strategies from about 15 different countries had been compared and analyzed. This was followed by a number of workshops and meetings with different stakeholders in Dubai to collect comments and identify synergies. This was used to further improve the strategy, and set the road for its implementation. These stakeholders are the main drivers for the successful implementation of the strategy, and their collaboration is of utmost importance.

The launch of the Cyber Security Strategy is the beginning of our journey, in which we are developing an operational Plan together with the stakeholders. This operational Plan is in the process of implementation with the engagement of a large number of different stakeholders. The overall time frame for the implementation of this Cyber Security Strategy is five years.


2016
JUL
PROJECT LAUNCH
AUG
RESEARCH AND BENCHMARKING
SEP
PRELIMINARY STRATEGY FRAMEWORK DEVELOPMENT
NOV
FRAMEWORK DISCUSSION WORKSHOPS
2017
JAN
OPERATIONAL PLAN DEVELOPMENT
FEB
STRATEGY ALIGNMENT WITH OTHER STRATEGIES
MAR
SITUATIONAL ANALYSIS
JUN
STRATEGY LAUNCH
JUL
KPI REVIEW AND APPROVAL
AUG
GOVERNMENT ORIENTATION SESSIONS
DEC


DUBAI ELECTRONIC SECURITY CENTER
مركز دبي للأمن الإلكتروني