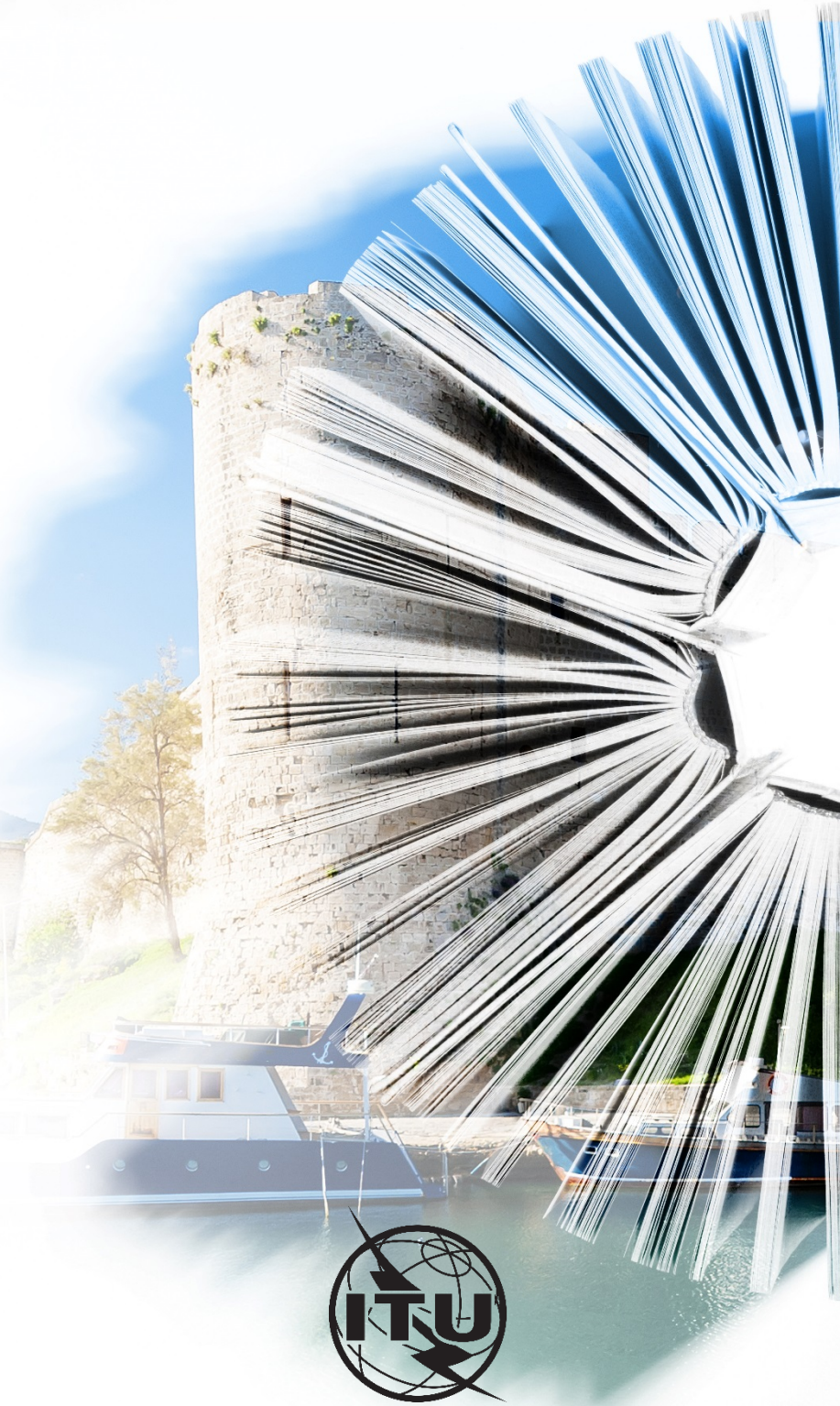
CASE STUDY

Republic of Cyprus

Governmental Computer Incident Response Team (CIRT) Establishment (9CYP13001)



BACKGROUND

The project assisted the Government of Cyprus to establish its own Governmental CIRT (Computer Incident Response Team) to serve as a trusted, central coordination point of contact for cybersecurity, aimed at identifying, defending, responding and managing cyber threats. This project focused on assisting the Government of Cyprus to organize and equip itself to better respond to cyber threats. It paid particular attention to improve cybersecurity in Cyprus and to ensure better protection of Cyprus' ICT infrastructure, including critical information infrastructure, and the availability of dependent services provided to Cyprus' government agencies, citizens and businesses.

REGION

WHY WAS THE PROJECT NEEDED?

There is a growing need to be able to communicate, coordinate, analyze, and respond to cyberattacks across different business sectors and national borders. The Internet itself has become a critical infrastructure to many nations, businesses and people that must also be protected. The absence of proper institutional structures in countries around the world to deal and respond cyber incidents, threats and attacks is a genuine problem. ITU is working with Member States to deploy capabilities to build capacity at the national and regional levels, in addition to establishing National Computer Incident Response Teams (CIRTs).

PARTNER

Office of the Commissioner of Electronic Communications and Postal Regulation, Republic of Cyprus

http://www.ocecpr.org.cy

The Office of the Commissioner of Electronic Communications and Postal Regulation (OCECPR) is an independent regulatory authority of the Republic of Cyprus in matters of electronic communications and postal services, with additional responsibilities in the areas of terminal equipment, network and information security and protection of critical information infrastructures. It is the body responsible for coordinating the implementation of the National Cybersecurity Strategy of the Republic of Cyprus, which is accountable for the pillars of network and information security (cybersecurity), cybercrime, cyberdefense and related external affairs. As part of these responsibilities, OCECPR assists in the exchange of information between the competent authorities, stakeholders and consumers in Cyprus regarding issues and activities relating to network and information security.

OCECPR is responsible for the creation and coordination of bodies for the response to incidents related to Computer Emergency Response Teams in Cyprus. It also supervises and regulates the activity of the these CIRT entities.

NATIONAL CIRT | CAPACITY BUILDING

The absence of institutional structures to deal with cyber incidents and attacks is a genuine problem in responding to cyber threats.

ITU is working with its Member States to build cybersecurity related capacity at national and regional level, in addition to establishing CIRTs.

ITU is helping countries to establish their National Computer Incident Response Team (CIRT), which serves as a national focus point to coordinate cybersecurity incident response to cyberattacks in the country.

After an assessment at the country level, ITU assists with the planning, implementation, and putting the CIRT into operation. Continued collaboration from ITU with the newly establish CIRT ensures that support remains available.

OBJECTIVES

01

To establish institutional structures in Cyprus, such as the computer incident response team (CIRT)

02

To identify, manage and respond to cyber threats

03

To establish national cooperation mechanisms related to cybersecurity

04

To equip the government of Cyprus with a functioning and operational Governmental CIRT

RESULTS

- A functioning Governmental CIRT was established, which was able to provide Cyprus' constituents with a basic set of cybersecurity related services.
- National expertise on cybersecurity was enhanced and the human capacity gap in cybersecurity was diminished.
- National preparedness was improved on the identification, prevention, response, and resolution of cybersecurity incidents (preliminary assessment and post implementation assessment required.)

"Improved national preparedness and response regarding cybersecurity incidents "

CIRT

Computer Incident Response Team

RESULTS

- An effective and efficient CIRT was built and made operational, that is ready to respond to cyberattacks targeting the governmental critical information infrastructure. The governmental CIRT will be the trusted advisor to the government of Cyprus on matters concerning cybersecurity.
- National awareness training programmes were developed, which resulted in the improvement of cybersecurity procedures, to defend and protect government infrastructures and agencies.
- Increased ability to enact effective security measures and instill mature responses when such cyber threats occur.

“Improved national preparedness and response regarding cybersecurity incidents ”

“In embracing technological progress, cybersecurity must form an integral and invisible part of that process,”

Mr Brahima Sanou

Director of BDT, ITU

PROJECT ACTIVITIES

Built a knowledge base that supported Cyprus' development and implementation of a national cybersecurity strategy, as well as a national approach for the protection of critical information infrastructures

Supported the building of a national culture of cybersecurity, and established related awareness raising initiatives

Assisted in planning and developing a national strategy on child online protection

Enabled Cyprus to develop and enhance its national cybersecurity incident response and management capabilities

Supported the development of related national cybersecurity platforms, for example: the national Public-Key Infrastructure (PKI), e-Government framework and approach, national identity and access management framework, combating SPAM, botnets, etc.

LESSONS LEARNED

Cyber threats are increasingly affecting the lives of ICT users. Therefore, the CIRT is considered to be a sustainable solution against cyber threats.

Collaboration at the national and international level is necessary to effectively align capabilities and expertise, hence to manage incidents and raise awareness of potential incidents and steps toward remediation. Governments play a key role in ensuring the coordination among these national and international entities.

At WSIS, Heads of States and world leaders entrusted ITU to be the Facilitator of Action Line C5, "Building confidence and security in the use of ICTs", in response to which ITU launched, in 2007, the Global Cybersecurity Agenda (GCA), as a framework for international cooperation in this area. Enhancing security and building confidence in the use of ICTs is one of priority domains for Objective 3 of the Dubai Action Plan adopted at the 2014 World Telecommunication Development Conference.

LESSONS LEARNED

Based on ITU's commitment, similar projects to assist Member States in the establishment of CIRTs, improve the CIRTs that are already in operation, as well as to provide assistance with legal frameworks and other cybersecurity related activities should be replicated.

ITU's assistance in building and deploying the technical capabilities and related trainings was necessary to establish the Governmental CIRT in Cyprus. It lead to the development of national cybersecurity capacities while assisted the government of Cyprus in enhancing regional and international collaboration.

Risks:

The main risk was the possibility of inadequate human resources assigned to the project, which would have increased the time for completion of the project. This risk was reduced by the support of the government of Cyprus, which administered the appropriate site and also through country training courses provided by ITU. The Government of Cyprus also provided human resources to efficiently operate the CIRT.

CONCLUSION AND RECOMMENDATIONS

Overall reliance on the Internet continues to increase. Unfortunately, in this dynamic and interconnected environment, cyberattacks occur rapidly and can spread across the globe in minutes without regard to borders, geography, or national jurisdiction. As a result, there is a growing need to be able to communicate, coordinate, analyze, and respond to cyberattacks across different business sectors and national borders. The Internet itself has become a critical infrastructure for many nations, businesses and people, who all must be protected.

It is important for each government to create or identify a national organization that serves as a focal point to secure their cyberspace and protect of critical information infrastructures. Its mission should include efforts to watch, respond and recover as well as to facilitate the collaboration between government entities, the private sector, academia, and the international community when dealing with cybersecurity issues.