

Establishing a National CERT/CISRT in Egypt

Sherif HASHEM, PhD, CISM, Senior Member, IEEE

Chairman, Executive Bureau, Egyptian Supreme Cybersecurity Council, Cabinet of Ministers
Principal Cybersecurity Advisor, National Telecom Regulatory Authority
Professor, Faculty of Engineering, Cairo University
Giza, EGYPT
shashem@tra.gov.eg, shashem@ieee.org

ABSTRACT

This paper highlights the lessons learned while establishing and developing a national computer emergency readiness team for Egypt, namely EG-CERT. We discuss the role played by EG-CERT in supporting national cybersecurity initiatives, especially the Supreme Cybersecurity Council, and in launching the national cybersecurity strategy with participation from key sectors. We emphasize the importance of cooperation and knowledge exchange at the national, regional and international levels, while developing and implementing cybersecurity initiatives. Responsiveness, transparency, dedication and perseverance are key to the success of national CERT/CISRTs in carrying out their cybersecurity related mission, while confidentiality, integrity, and the team spirit are key to earn the trust of their constituents as well as of their peers in the professional community nationally and internationally.

Keywords: Egypt, cybersecurity, CERT, CISRT, EG-CERT, National Strategy, Supreme Cybersecurity Council.

1. INTRODUCTION

Computer Emergency Response Teams (CERTs) which are also referred to as Computer Security Incident Response Teams (CSIRTs) date back to 1988 when the first CERT, namely CERT-Coordination Center or CERT-CC, was established at Carnegie Mellon University in response to the large scale outage caused by the Morris worm in

1988 [1]. Since then, over 450 CERTs and CSIRTs have been created, in more than 90 countries, and became members of the Forum of Incident Response Security Teams (FIRST), which was formed in 1990 [2].

The development of the CERTs/CSIRTs and the enhancement of their capabilities have been addressed by key international and regional organizations, such as the International Telecommunications Union (ITU), the European Network and Information Security Agency (ENISA) of the European Union (EU), and the Organization of American States (OAS), as well as by leading CERTs and professional organizations [1-7].

Cybersecurity is currently viewed as a key component of national security by many countries across the globe, and national CERTs have emerged as active players in defending against cyberattacks and cybercrimes. National Cybersecurity strategies often highlight the role of national CERTs in protecting critical infrastructure [8-11]. The role of national and sectoral CERTs/CSIRTs has been also emphasized in the ITU's Global Cybersecurity Agenda (GCA), which was launched in 2008 as a framework for international cooperation to promote cybersecurity and enhance confidence and security in the information society [12,13].

At a higher policy level, the role of national CERTs has been emphasized by the United Nations' Groups of Governmental Experts (UN GGEs) on Developments in the Field of Information and Telecommunications in the Context of International Security [14].

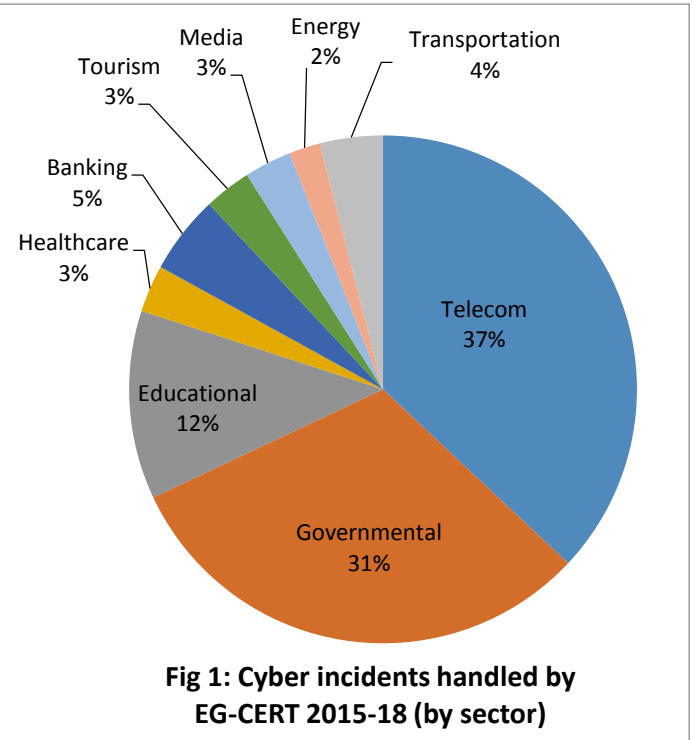
2. EGYPT'S NATIONAL CERT (EG-CERT)

The idea to develop an Egyptian cybersecurity and CIIP framework was initiated in 2007, within a working group at the Egyptian Ministry of Communications and Information Technology. The first implementation step was the establishment of the Egyptian national Computer Emergency Readiness Team (EG-CERT) in April 2009. EG-CERT is affiliated with the National Telecom Regulatory Authority (NTRA), and provides support to several entities in the ICT sector, the financial sector as well as the governmental sector, in order to help them tackle Cybersecurity threats and deal with cyber incidents and denial of service (DDOS) attacks. EG-CERT provides both reactive as well as proactive services, including incident handling, cyber forensics, malware analysis, vulnerability assessment, and penetration testing.

It is worth mentioning that EG-CERT started as an ICT sector specific CERT. However, a few weeks after its establishment, it was called upon to provide support and services to entities in other critical sectors, especially in the financial and governmental sectors. Furthermore, in Oct 2009, EG-CERT was contacted to assist the prosecutor in investigating an international cybercrime case "Operation Phish Phry" that involved a phishing ring of about 100 alleged criminals from Egypt and the USA, targeting thousands of victims in US Banks. That phishing ring was considered one of the largest worldwide at that time [15]. EG-CERT professionals spent over 1600 man hours on the cyber forensics analysis, and produced a report in excess of 600 pages. EG-CERT's efforts were timely, professional, and instrumental in the successful prosecution of such a challenging case, and was recognized by the national as well as by the US officials. By the end of 2009, EG-CERT had emerged as the National CERT.

Currently, EG-CERT prepares over 250 reports annually for its constituents and for relevant authorities and key organizations. EG-CERT leads and coordinates efforts to confront distributed denial of services (DDOS) attacks on critical infrastructure by local and international "cyber hacktivist" groups, such as Anonymous. EG-CERT assists in dealing with web defacement attacks on several

governmental and strategic websites in the financial sector. EG-CERT support and services are provided, whether to governmental or private entities, is free of charge, in full confidence and discretion. EG-CERT's engagement is generally based on the criticality of the threat and/or the severity of the incident. The breakdown of the cyber incidents handled by EG-CERT shown by sector during the last four years is shown in Fig. 1.



As soon as EG-CERT assumed its national responsibilities, providing support to key CII entities, it was immediately realized that empowering those responsible for CIIP in the critical sectors, and enhancing their technical skills, should be of utmost priority. Hence, a pilot national cybersecurity training program was organized and sponsored by the NTRA between 2009-2010, for training 220 professionals in 38 organizations within the governmental/public sector, banking sector, education sector, as well as from ICT private sector companies (Telecom companies, mobile operators, CSPs, etc.). The program covered key cybersecurity topics: security essential, incident handling,

penetration testing and ethical hacking, perimeter security, advanced wireless penetration testing and ethical hacking. As an outcome of the program, 179 of those professionals obtained international certificates from SANS, some of them obtained up to 4 different advanced cybersecurity certificates within the program. The launch of the pilot training program had an immediate positive impact in creating awareness, enhancing readiness, and establishing a network of trust and enhanced cooperation spirit among participating entities as well as among professionals. The financial sponsorship from the NTRA was also a strong message of commitment, partnership and support from a leading public entity, a message that extended beyond professionals from public sector to partners from the private sector, and even beyond the telecom sector to other critical sectors. The success of the pilot training program inspired several programs among various sectors.

EG-CERT has broad regional and international cooperation, including the participation in annual international cyber drills with Asia Pacific – APCERT annual cyber drill (since 2012), Organization of Islamic Countries - OIC-CERT annual cyber drills (since 2012), and ITU Arab region cyber drill (since 2012). EG-CERT is a member of the international Forum of Incident Response and Security Teams (FIRST), and is a founding member of the Organization of Islamic Countries CERT (OIC-CERT) and Africa CERT.

EG-CERT has also organized several regional and international events, including an ITU Arab Regional Cybersecurity Workshop (2011), the ITU Arab regional cyber drill (2015), the ITU ARCC Regional Cybersecurity Summit (2016) and the FIRST Regional Cybersecurity Symposium for the Arab and African Region (2016).

EG-CERT has cooperation agreements with: Cybersecurity Malaysia, US-CERT, Uganda, Tanzania, Team Cymru, IMPACT, and Indian CERT. It also has strong relationships with many CERTs in the Arab region, in Africa, and across the Globe.

3. EG-CERT AND THE NATIONAL CYBERSECURITY STRATEGY

In 2014, a new Egyptian constitution was adopted. Article (31) of the new constitution recognizes that: “a safe and secure cyberspace is essential for the Egyptian economy and is a main pillar of Egypt’s national security.”

Later in December 2014, and in light of Article (31) of the new Egyptian constitution, a Supreme Council for Critical Information Infrastructure Protection and Cybersecurity (namely the Egyptian Supreme Cybersecurity Council ESCC), was established at the Cabinet of Ministers level. ESCC is chaired by the Minister of Communications and Information Technology, and has members from the critical sectors as well as the key security agencies.

ESCC began its work in 2015, and was initially mandated to develop a national cybersecurity strategy for Egypt. The key goal of the national strategy is to:

“REDUCE THE RISKS AND SECURE THE BENEFITS OF A TRUSTED DIGITAL ENVIRONMENT FOR BUSINESSES AND INDIVIDUALS.”

The cybersecurity strategy aims at developing and implementing a comprehensive framework for enhancing the security of and the trust in the ICT infrastructure, applications and services in Egypt, while protecting the privacy of various users.



Fig. 2: Pillars of the National Cybersecurity Strategy

The national cybersecurity strategy document highlighted the main cyberthreats, and the key “critical” sectors that may be affected the most by these cyberthreats, including the ICT sector, the financial sector, the energy sector, the government services sector, transportation, and healthcare. Seven strategic pillars were identified (Fig. 2) and six national programs were proposed to be implemented over a period of five years. The development of the proposed national cybersecurity strategy was finalized by the ESCC in May 2017 [11]. The strategy document was forwarded to the Cabinet of Ministers, and the implementation of the strategy started later in the fall of 2017.

At the operational level, EG-CERT has taken the role of the “Technical Arm” of the ESCC. It is assisting in the implementation of the national cybersecurity strategy, especially in developing and empowering CERT teams in critical sectors, with a special focus on the financial, energy, and transportation sectors. In parallel, plans are being implemented for developing a national security operations center (SOC) and national cybersecurity certification center.

Successful Egyptian cybersecurity initiatives and activities has led to the **advanced cybersecurity rank that Egypt has achieved in 2015 (27th among 193 countries) and further advanced in 2017 (14th among 194 countries)** as reported by the International Telecommunications Union (ITU) **Global Cybersecurity Index [16]**.

4. LESSONS LEARNED

- **Start small, then grow.** In 2009, EG-CERT started with a team of 6 professions, divided between incident management and cyber forensics. As the demand for its services grow, EG-CERT grew to employ over 50 professionals. It expanded its scope of services to include proactive services, such as penetration testing and malware analysis. It also developed research and development capabilities [17-27].
- **The human factor is central.** When it comes to cybersecurity, humans often are the weakest link. Cybersecurity readiness starts and flourishes with empowered and skilled workforce. The launch of EG-CERT was supported by recruiting talented professionals and an advanced training and skill development program, targeting not only EG-CERT professionals, but also professionals from 38 key entities, including government, academia and private sector.
- **Stay focused and avoid turf fights.** It is important, especially for a national CERT, to stay focused on its mission, and on enhancing its services and empowering its staff. Any distractions, especially internal and external organizational politics, conflicts, and turf fights, should be avoided. CERTs should be viewed as “*professional cyber peace keepers and guardians of safety and security in cyberspace for all.*”
- **Cybersecurity and physical security are highly interdependent.** When called upon to investigate a cyber incident or assess cyber-related vulnerabilities of an ICT system, EG-CERT professionals often realize that the more evident root cause or vulnerability is actually more fundamental and physical, such as lack of proper access control, absent or expired staff certification and clearance, unclear work flow, missing data and information classification, or improper authorizations. Thus, cyber risk needs to be addresses as a part of a holistic approach for overall operational risk management, rather than an isolated technical or technological risk.
- **Security-by-Design is key to successful cybersecurity.** Attempting to “fix” serious vulnerabilities or shortcomings in critical systems can be both costly, time consuming, and sometimes impossible, once the system has been designed or deployed. Cybersecurity need to be addressed from the very early phases of system design and incorporated in the design for the beginning.

- **Build partnerships.** A CERT professionals should be open to share knowledge and expertise with their peers. EG-CERT professionals often provide seminars, workshops, and training to professionals working in key entities and organizations, nationally, regionally, and internationally. They also support in organizing cyber competitions, such as Capture the Flag (CTFs) and cyberdrills. At the operational level, public-private partnerships and empowering the cybersecurity industry are key to the success of CERT operation as well as for drafting and implementing cybersecurity strategies, at the organizational and at the national levels.
- **Research and Development are essential for comprehensive cybersecurity.** Most CERTs rely on technologies and solutions from a variety of vendors, national and international. Having the capability to investigate and test emerging technologies and new gadgets is essential for successful deployment. Furthermore, CERT professionals often need to develop new tools or customize systems provided by the vendors, for better utility or higher efficiency. R&D capabilities expand the operation horizon and provide a much needed and desired effectiveness.
- **Establish trust.** The engagement with the constituents should be based on dedication, full confidence and discretion. Although EG-CERT is affiliated with the telecom regulator, the NTRA, the information on cyber incidents or vulnerabilities provided to the EG-CERT professionals are kept fully confidential, and thus are not shared with the NTRA regulatory division.
- **Balanced awareness.** When raising awareness with regard to an emerging cyberthreats, the message should be balanced: it needs to be clear and relevant in order to affect those who are unaware of the cyber risk ahead of them, especially if they are in a “*State Of Denial*”. Yet, it needs not to be exaggerated, so as not to cause a “*State Of Panic*.”

5. REFERENCES

- [1] ENISA, **A Step-by-Step Approach on How to Set Up a CSIRT, Deliverable**, WP2006/5.1 (CERT-D1/D2), <http://www.enisa.europa.eu/>, 2006.
- [2] **Forum of Incident Response and Security Teams (FIRST)**, <https://www.first.org/>
- [3] M.Brown, D.Stikvoort, K.Kossakowski, G.Kilcrece, R.Ruefle, and M.Zajicek, **Handbook For Computer Security Incident Response Teams (CSIRTs)**, Software Engineering Institute – Carnegie Mellon University, Report CMU/SEI – 2003-HB-002, 2003.
- [4] **Create A CSIRT**, Software Engineering Institute – Carnegie Mellon University, <https://www.sei.cmu.edu>, 2017.
- [5] ENISA, **Baseline Capabilities: National/Governmental CERTs – V1.0**, Dec 2009, <http://www.enisa.europa.eu/>, 2009.
- [6] Organization of American States, **Best Practices for Establishing a National CSIRT**, <https://www.sites.oas.org/cyber/Documents/2016%20-%20Best%20Practices%20CSIRT.pdf>, 2016.
- [7] M. van de Heide, **Establishing a CSIRT**, Ver 1.2, Nov 2017, <https://www.first.org/resources/guides/Establishing-CSIRT-v1.2.pdf>, 2017.
- [8] USA, **The National Strategy To Secure Cyberspace**, The White House, Washington DC, 2003.
- [9] USA, **National Cyber Strategy of the United States of America**, The White House, Washington DC, 2018
- [10] ENISA, **National Cyber Security Strategies: Practical Guide On Development And Execution**, ENISA, Greece, 2012.

- [11] ESCC, **Egypt's National Cybersecurity Strategy**, ESCC, Cairo, 2017, <http://www.escc.gov.eg/>.
- [12] ITU, **Report Of The Chairman Of High Level Expert Group on Cybersecurity**, ITU, Geneva, 2008.
- [13] ITU, **National Cybersecurity/CIIP Self-Assessment Tool**, ITU, Geneva, 2010.
- [14] UN GGE, **Report of the United Nations Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security**, United Nations, New York, July 2015.
- [15] FBI, **Archives on Operation Phish Phry**. (Oct 2009).https://archives.fbi.gov/archives/news/stories/2009/october/phishphry_100709
- [16] ITU, **Global cybersecurity Index (GCI) 2017**, ITU, Geneva, 2017.
- [17] M. Rasslan and M. Nasreldin, "Identification Protocols Based on Discrete Log Representation Problem," **Procedia Computer Sciences**, Vol. 21, pp. 368-373, Elsevier Science, 2013.
- [18] M. Rasslan and H. Aslan, "On the Security of Two Improved Authenticated Encryption Schemes, International Journal of Security and Networks," Vol. 8, No. 4, pp. 194-199, 2013.
- [19] M. Rasslan, "Security comments on Hwang-Lo-Hsiao-Chu Authenticated Encryption Schemes," **Procedia Computer Sciences**, Vol. 19, pp. 565-569, Elsevier Science, 2013.
- [20] H. Aslan and M. Rasslan, "A New Multicast Authentication Protocol using Erasure Code Functions and Signcryption Techniques," **World Congress on Internet Security (WorldCIS-2013)**, Vol. , No. , pp. , Proceedings of the IEEE, 2013.
- [21] S. Sayed, R. Darwish and S.A. Salem, "A Real-Time Approach for Detecting Malicious Executables," **Proceedings of the International Conference on Systems Science 2013 (ICSS 2013)**, Vol. 240, 2014, pp 355-364
- [22] A.A. Awad, S.G. Sayed and S.A. Salem, "A network-based framework for RAT-bots detection," **Proceedings of the 8th IEEE Annual Information Technology, Electronics and Mobile Communication Conference (IEMCON)**, 2017.
- [23] A.A. Awad, S.G. Sayed and S.A. Salem, "A Host-based framework for RAT-bots detection," **Proceedings of the IEEE International Conference on Computer and Applications (ICCA)**, 2017.
- [24] D. Wael, A. Shosha and S.G. Sayed, "Malicious VBScript detection algorithm based on data-mining techniques," In **Proceedings of the International Conference on Advanced Control Circuits Systems (ACCS) Systems & International Conference on New Paradigms in Electronics & Information Technology (PEIT)**, 2017.
- [25] S.G. Sayed and M. Shawkey, "Data Mining Based Strategy for Detecting Malicious PDF Files," In **Proceedings of the 17th IEEE International Conference on Trust, Security And Privacy In Computing And Communications (IEEE TrustCom-18)**, 2018.
- [26] M. Medhat, S.G. Sayed, and N. Abdelbaki, "A New Static-based Framework for Ransomware Detection," In **Proceedings of the 16th IEEE International Conference on Dependable, Autonomic and Secure Computing (DASC 2018)**, 2018.
- [27] D. Wael, S.G. Sayed and N. Abdelbaki, "Enhanced Approach to Detect Malicious VBScript files Based on Data Mining Techniques," In **Proceedings of Fifth International Workshop on Privacy and Security in HealthCare 2018**. (Accepted)