sciendo

Land Forces Academy Review
Vol. XXIII, No 3(91), 2018

ISSUES IN CYBERSECURITY: SECURITY CHALLENGES AND PROBLEMS IN THE DOMINICAN REPUBLIC

Maurice DAWSON
Illinois Institute of Technology, School of Applied Technology,
Center for Cyber Security and Forensics Education, Chicago, Illinois, USA
mdawson2@iit.edu

Pedro Manuel TAVERAS NUÑEZ
Mother and Teacher Pontifical Catholic University,
Faculty of Engineering Sciences, Santo Domingo, Dominican Republic
PedroTaveras@pucmm.edu.do

ABSTRACT

Many developed countries are placing resources to combat the growing threats in cyberspace, and emerging nations are no different. Since 2016, the Dominican Republic is undergoing massive changes within the current government to prioritize cybersecurity through laws, policies, and doctrine. This initiative is causing politicians, industry, and even government entities such as the national police to start the journey to begin to fully understand what are the issues in cybersecurity as they apply to the nation. It is essential that the security challenges and problems identified are addressed through a process of discovery while mitigating risks. This paper is to present those challenges and offer solutions that can be used to achieve an acceptable level of cyber risk.

KEYWORDS: Cybersecurity, Workforce Development, Policy, STEM Education

1. Introduction

Cybersecurity has become the current platform for modern warfare. It has allowed nations to conduct information warfare which has altered the election outcomes to directly attacking a nation's power grid (Burns & Elthan, 2009; Case, 2016). For emerging countries, this should raise alarms and serve as a wake-up call to establish strong cybersecurity policies that become rooted in education, technology, and laws. With nearly 30 Million tourists travel to the Caribbean and spending upwards of $35 billion in 2016 this area serves as a prime target for attacks (Bosman, 2017). Approximately 25 % of those travelers come to the Dominican Republic. These tourists come to the island unaware of the cybersecurity challenges faced and the growing concerns within the country.

It is known that in terms of security, a network will be as strong as its weakest link. This adage can be applied to the situation of cybersecurity of the countries of the Central American Region (CAR), from the context and the reality of a hyperconnected world. The lack of information security culture is one of the main obstacles when trying to implement a national IT security policy. Most incidents are hidden, faded or ignored, in different structures: Industry and government. Making these facts public could represent a loss of confidence and of clients, in the private case and loss of prestige in the case of the

DOI: 10.2478/raft-2018-0020

government. For these reasons, it is common that the first reaction is to concealment and denial of the existence of security violations or related events (Clark, 2015).

In the Central American and Caribbean region, since 2006, various efforts have been made to promote a less vulnerable ecosystem in our countries through:

- Training workshops to form Cybersecurity Incident Response Centers;
- Training of identified personnel from key institutions;
- Workshop simulation of attacks and situations;
- Technical cooperation in the preparation of draft laws that allow for prosecution of computer crimes;
- Use of recognized standards;
- Awareness of institutions and companies in aspects of computer security.

Despite all this cooperation, optimal results have not yet been produced. It is necessary to form the necessary critical mass to promote actions that can be recognized at the national level. Each year that passes it becomes more necessary to have adequate and specialized legislation on the subject of Cybersecurity. ICT applications, such as e-government, e-commerce, e-learning, e-health, and cyberspace, are considered enabling for development. They provide an effective channel to distribute a wide range of basic services in remote and rural areas. ICT applications can facilitate the achievement of millennium development goals, reduce poverty and improve sanitary and environmental conditions in developing countries (ITU, 2009a). ICT applications and tools can improve productivity and quality and at the same time allow greater access to basic services.

However, the growth of the information society is accompanied by new and important threats. Essential services such as water and electricity supply are currently based on ICT. Automobiles, traffic control, elevators, air conditioning and telephones also depend on the proper functioning of ICT. Attacks against these infrastructures and Internet services can cause damage to society in a critical way not seen before (Pultarova, 2016). In this regard, the theft of online identity and the appropriation of credentials or personal information through the Internet, online fraud, the spread of child pornography and digital attacks to automated systems are just examples of computer-related crimes that are committed on a large scale every day. The financial damages caused by cybercrime are enormous. However, there is just a short list of the main threats that hinder the further development of e-government and cyber-commerce services (ITU, 2009b).

2. Initiatives

The Dominican Republic is the first Latin American country to ratify the Convention on Cybercrime, due to the fact that at the beginning of 2013 it ratified its accession as a non-member State of the Council of Europe, an agreement that entered in effect in June of the same year, being from that moment a model for South and Central America. According to the National Congress of the Dominican Republic (2007) computer crimes with the highest prison sentence in this nation are the following:

- *"The sabotage, espionage or supply of information, through a computer, electronic, telematic or telecommunications system, attacking the fundamental interests and security of the Nation".*
- *"Perform acts of terrorism, with the use of electronic, computer, telematic or telecommunications systems".*

The Dominican policy on computer security and cybersecurity is divided between several laws and international agreements (which according to the Dominican Republic legislation, if signed, have the force of law), and the security of personal data is covered by the laws of electronic communications and the protection of personal data.

On April 23, 2007, Law 53-07 on high-tech crimes and offense was enacted in the Dominican Republic. The objective of this law is the protection of ICT systems and their content, as well as the prevention and punishment of crimes committed against them or any of their components. The law also punishes all crimes committed through the use of said technologies in prejudice of physical or moral persons. The integrity of information systems and their components, information or data transmitted or stored through them, commercial agreements or any other type of transactions carried out over such systems constitute legally protected assets.

In November 2014, Law 310-14 was enacted to regulate the sending of unsolicited commercial, advertising or promotional communications, made by email. Without prejudice to the current provisions on commercial matters regarding advertising and consumer protection (SPAM).

The protection of personal data is a fundamental right as stated in Article 44.2 of the Constitution of the Dominican Republic, which establishes that: "Any person has the right to access information and data about himself or his/her assets, that reside in official or private records, as well as knowing the destination and the use made thereof, with the limitations set by law. The treatment of personal data and information or their property must be done respecting the principles of quality, lawfulness, loyalty, security, and purpose. You can request before the competent judicial authority the update, opposition to the treatment, rectification or destruction of that information that unlawfully affects your rights".

The country has an organic law on the protection of personal data. Law 172-13, promulgated by the Executive Power on December 13, 2013, has as its fundamental object: *"the comprehensive protection of personal data stored in archives, public records, data banks or other technical means of data processing intended to give reports, be these public or private, as well as ensure that the right to honor and privacy of people is not injured"*.

3. DICAT

The Department of Investigations of Crimes and Crimes High Technology (DICAT), is part of the Scientific Police and its objective is to combat high technology crime within the Dominican Republic. Its primary function is to investigate all complaints of crimes or crimes considered high technology. Respond with an investigative capacity to all threats and attacks to the critical national infrastructure.

DICAT warned in mid-2016 about the presence in the country of bands of foreigners who bring advanced technologies to steal identities, clone credit cards in the Dominican tourist areas. The authorities have discovered some of these international mafias, confirmed by nationals from Hungary, Colombia, Venezuela, and other nationalities that arrived as tourists and settled in Bavaro, Puerto Plata, Veron and Cabarete (Isa, 2017).

In November 2017, the National Police reported that since the commissioning of the DICAT, four thousand people had been submitted to the courts in the last ten years for cases related to cybercrimes. Since the foundation of the department in 2007, it has managed to recover more than 300 million Dominican Pesos (~ 6 million US Dollars) stolen from different people and financial entities. The report states that the profile of the computer delinquent in the Dominican Republic is no longer the person with advanced knowledge in computing, but people with a criminal record in common crimes who have advanced in the use of technologies. The report indicates that these criminals are frequently documented of foreigners established in the country, with extensive knowledge in this type of crimes. Most common cyber crimes are related to the kidnapping of information, the cloning of credit cards, electronic fraud, and child pornography, among others. In regards to transnational crimes and financial theft, they are generally perpetrated by cyber criminals of the national coast operating from countries with legal holes. According to Yunes (2017), director of DICAT, the Dominican legislation on high-tech crimes dates back ten years and is in the process of being revised to adapt it to new behaviors and cybernetic tendencies, as well as to impose greater sanctions and sentences on the accused.

4. Specialized Prosecutor's Office against High-Tech Crimes and Offences

The Specialized Prosecutor's Office against High-Tech Crimes and Crimes (PEDATEC) is made up of a team of prosecutors, lawyers, computer experts and technicians dedicated to working on crimes committed through any technological device. These crimes include threats via telephone, credit card cloning, defamation through social networks, illegal obtaining of funds, illicit electronic funds transfers, electronic fraud, electronic blackmail, identity theft, acquisition and possession of online child pornography. In the same way, PEDATEC advises and assists prosecutors in the field of criminal actions related to high-tech crimes, to ensure speed in the processing of processes and ensure citizen rights, by the institutional policies and laws. This Specialized Attorney was created on February 4, 2013, by resolution of the Superior Council of the Public Prosecutor, based on the exercise of regulation, promotion, and application of Law 53-0.

5. National Framework for Cybersecurity

The cybersecurity axis aims to ensure that citizens make secure and reliable use of information and communication technology systems, through the strengthening of national capacities for the prevention, detection, and response to cyber threats.

This project seeks to establish a national cybersecurity framework to guarantee and promote the safe use of networks and information systems through the strengthening of national capacities for prevention, detection and response to cyber attacks. The project will be carried out within the framework of the Cooperation Agreement signed on November 20, 2015, between the Dominican Telecommunications Institute (INDOTEL), representing the Dominican government, and the Organization of American States (OAS), through the Inter-American Committee against Terrorism (CICTE), which establishes working together to develop projects in the area of cybersecurity, through the implementation of the following components:

- Preparation of a National Cybersecurity Strategy for the Dominican Republic.
- Creation of a Cyber Security Incident Response Center (CSIRT).
- Creation of awareness and the development of capacities on cybersecurity.

In the United States (U.S.) the National Institute of Standards and Technology (NIST) have provided guidance that can be located in the Computer Security Resource Center (CSRC). These Special Publications (SP) addresses things from cloud computing to risk management for enterprise systems. One particular document, NIST SP 800-53, has even been adopted by the U.S. Army. This document provides a catalog of cybersecurity and physical controls for all federal systems.

6. Cybersecurity Manpower

As of July 2018 in the U.S. the current total cybersecurity job openings are at 301,873 while the current total employed cybersecurity workforce is at 768,096. Reviewing this data among other reports show that the cybersecurity talent in the

U.S. is deficient. There is a severe shortage, and the U.S. is trying to address this with the infusion of money for cybersecurity education at the university and K-12 levels of education to create a pipeline of talent. To make matters worse jobs of national security requirements that the positions are held by U.S. citizens that can undergo a security clearance review at the secret level or high. Moreover, if you look at rural and small metropolitan area, the talent is nonexistent. When looking at European markets, they are experiencing the same difficulties with hopes of Asians and Eastern Europeans to obtain necessary talent. In Europe, there is an expected shortage of 350,000 cybersecurity professional by the year 2022 (Ashford, 2017). A workforce is one of the most significant challenges facing cybersecurity at this time.

At the moment there is not a national framework for cybersecurity education in the Dominican Republic. The resulting factor from this means there is no oversight of cybersecurity education taught in the country or any entity trying to inject cybersecurity into the classroom. Reviewing the country's offered degree programs from the Universidad Autónoma de Santo Domingo (UASD), Pontificia Universidad Católica Madre y Maestra (PUCMM), Universidad Nacional Pedro Henríquez Ureña (UNPHU), and others you will not find a consistent list of courses or knowledge areas addressed. In the U.S. the National Security Agency (NSA) and Department of Homeland Security (DHS) oversee the Centers of Academic Excellence (CAE). Universities that wish to obtain accreditation from these agencies are required to meet rigorous requirements. Some of the requirements require full-time faculty with terminal degrees and recent significant in the last five years. Other requirements are the embedment of cybersecurity topics in programs outside computing such as nursing or political science.

7. Review of Cybersecurity Attacks

In the Dominican Republic attacks are in a wide range of external and internal threats due to the locale of the island and proximity to other nations in the Americas. The internal threats are individuals targeting banks to external threats to national security. In Figure no. 1 it shows three different categories with the associated type of crimes. The blue section shows crimes against confidentiality, integrity and data availability. The three most significant issues in this section are the following; 1. Phishing, 2. Card cloning, and 3. Hacking. Other issues are CD/DVD cloning, unauthorized access, theft of email, cloning of modem boxes, damage of data, data manipulation and software piracy. As it relates to cloning, there is an inadequate system for training individuals to identify phishing scams. Many people in the Dominican Republic using mobile phone and applications such as Whatsapp. On mobile devices, people rarely inspect links to ensure that they originate from legitimate sources. Studies have shown that in the United States (U.S.) that a significant number of Android users lack Anti Virus (AV). Additionally, these devices do not employ hardening techniques to lock down the mobile device further. In this country there is not a governing body providing guidance on these types of matters as the National Institute of Standards and Technology (NIST) does in the U.S.

Crimes against confidentiality, integrity and data availability		**Content crimes**		**Crimes against telecommunications**	
Phishing	858	Defamation and threat via Web page	444	Annoying calls and/or threatening	1815
Card Cloning (Skimming)	506	Defamation and threat via email	441	Scam via phone	474
Hacking	208	Electronic fraud to people and companies	381	Activations of fraudulent mobile telephone	36
Electronic fraud to sport betting agencies and lottery draws	155	Identity theft	206	Illegal termination of calls	6
Cloning CD and DVD	50	Internet scam	59	Alternation to telephone line	6
Illicit access	37	Extortion via web page	59		
Theft of email	23	Sexting	38		
Cloning of modem boxes	10	Child pornography	14		
Data damage or alteration	2	Harassment via Internet	14		
Software stealing	1	Copyright violation	2		
Software piracy	1	Documents forgery	2		

Figure no. 1: Sub-classification of crimes and crimes of high technology (Solved Cases)

The yellow section in Figure no. 1 shows content crimes. The three most significant issues in this section are the following: 1. defamation and threat via the Web page, 2. defamation and threat via email, and 3. electronic fraud to people and companies. The other issues found are the following: 1. identity theft, 2. Internet scams, 3. extortion via the web, 4 sexting, 5. child pornography, 6. harassment via the Internet, 7. copyright violation, and 8. document forgery. The green section shows crimes against telecommunications. The three most significant issues in this section are the following: 1. harassing or threatening calls, 2. phone scams, and 3. activations of fraudulent mobile lines. Out of these three major issues the phone scams resemble the infamous Nigeria 419 Scams however the dollar amount taken is significantly lower than that those that fall victim to those from Nigeria. Also, the 419 is a scam is a more elaborate scheme in which a sender requests help in facilitating the transfer of a substantial sum of money in exchange for commission payment. In 2018, there were 74 arrests made in connection to the infamous Nigerian 419 email scams (Wootson, 2018). This categorization of crime is also related to content crimes.

8. Further Analysis and Review

In an interview with Ing. Ney Aldrin Bautista Almonte and the founding officer for the cybersecurity division with the Dominican National Police many things were revealed. In 2017, there were approximately 42 uniformed and civilian personnel dedicated to cybersecurity. They are degreed however mainly users of applications that rather than developers. Thus if there were more severe attacks on infrastructure in the forms of malware, worms, etc. no one had the knowledge to do reverse engineering. Not single personnel in this division could perform low-level code analysis or advise a company for secure coding practices to ensure they are safer once they deploy their applications. Additionally, there is a lack of cybersecurity talent in the uninformed and government service personnel. Lastly, there is an issue in recruiting the talent that is here locally due to the competitive salaries offered by commercial entities such as local software consulting companies. There are no programs to develop cybersecurity leaders and current the highest level ranking officer for cybersecurity is a colonel. In constant, the U.S. has general officers and Senior Executive Service (SES) members providing leadership to cyber personnel. Additionally, the organization has created senior roles for cybersecurity such as the Chief Information Security Officer (CISO).

Figure no. 2 displays the Mission Framework that was created by reviewing the education, policy, and technology of that specific entity. This framework can be applied to a country, organization or group of institutions. Using this as a base to further develop items to secure the Dominican Republic may be the solution needed.

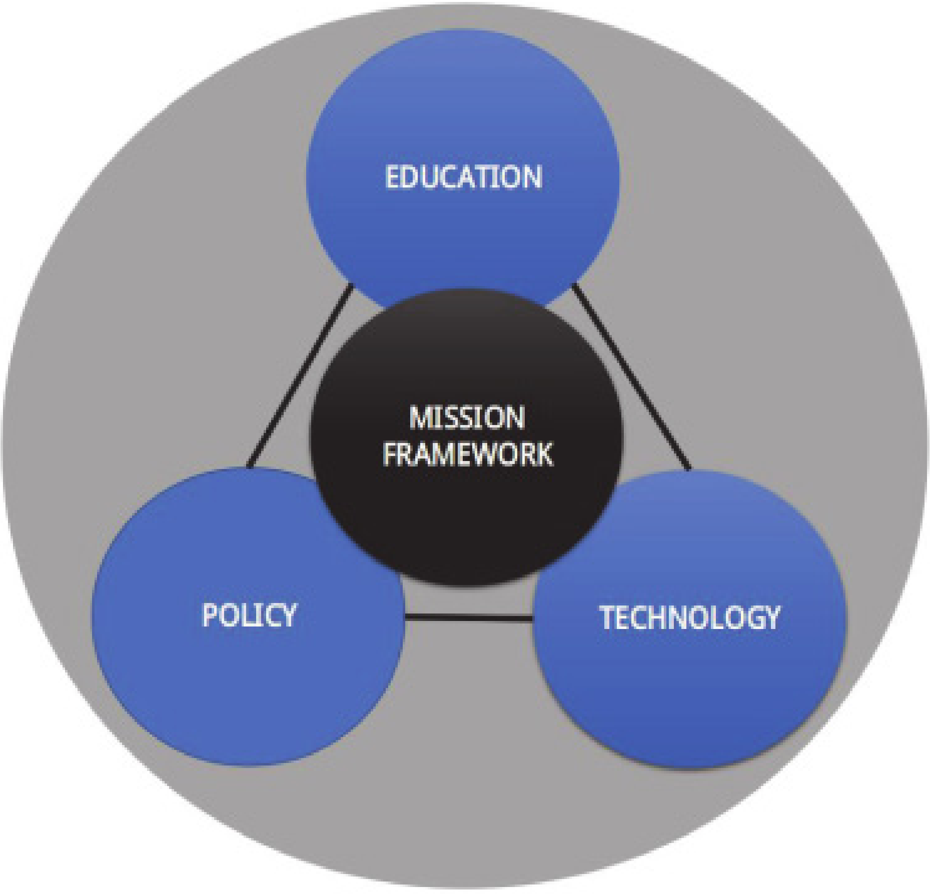

Figure no. 2: Mission framework

9. Conclusion

For a nation and organization to be prepared for cybersecurity planning needs to occur at the highest levels of government. There needs to be a holistic framework that creates an atmosphere of uniformity among government and commercial entities (Dawson, 2017; Dawson 2018). The universities in the country need a framework for developing a workforce capable of handling the present and future threats. (Dawson, Wang, & Williams, 2018). Once this framework is in a process, it is imperative to have a review annual to review attacks and the status of cybersecurity within the nation. With the newly formed task force to tackle cybersecurity issues, these concerns must be addressed to secure the country (Republica Digital, 2018).

REFERENCES

Ashford, W. (2017*). Europe faces shortage of 350,000 cyber security professionals by 2022*, available at: https://www.computerweekly.com/news/450420193/Europe-faces-shortage-of-350000-cyber-security-professionals-by-2022, accessed on: July 19, 2018.

Burns, A., & Eltham, B. (2009). Twitter free Iran: An evaluation of Twitter's role in public diplomacy and information operations in Iran's 2009 election crisis.

Bosman, J. (2017). *The Storms Moved On. The Caribbean Islands Fear the Tourists Might, Too*. available at: https://www.nytimes.com/2017/09/23/us/tourism-hurricane-economy-caribbean-islands.html, accessed on: July 19, 2018.

Case, D. U. (2016). *Analysis of the cyber attack on the Ukrainian power grid*. Electricity Information Sharing and Analysis Center (E-ISAC).

Clark, F. (2015). *Generalities of the cybersecurity regulation in the members States of COMTELCA*, available at: https://www.itu.int/en/ITU-D/Regional-Presence/Americas/Documents/EVENTS/2015/0910-PA-IXP/6%20Viernes%20SIT%20Clark%20Generalidades%20Regulaci%C3%B3n%20Ciberseguridad.pdf

Dawson, M. (2017). *Hyper-connectivity: Intricacies of national and international cyber securities.* (Doctoral dissertation). London, UK: London Metropolitan University.

Dawson, M. (2018). Applying a holistic cybersecurity framework for global IT organizations. *Business Information Review*, *35(2),* 60-67.

Dawson, M., Wang, P., & Williams, K. (2018). The Role of CAE-CDE in Cybersecurity Education for Workforce Development. *Information Technology-New Generations, 15th International Conference on Information Technology,* 127-132.

Isa, M. (2017). *Crime without borders, another scourge of economic security and peace in the DR*, available at: http://hoy.com.do/ciberdelincuencia-delito-sin-fronteras-otro-azote-a-la-seguridad-economica-y-sosiego-en-rd/

ITU. (2009a). *ICT Applications and Cybersecurity Background Note to the 2009 Pacific ICT Ministerial Forum*, available at: http://www.itu.int/ITU-D/asp/CMS/Events/2009/PacMinForum/doc/Background%20Note-Theme-4-ICT%20Apps%20&%20Cybersecurity.pdf

ITU. (2009b). *Cybercrime: A guide for developing countries*, available at: https://www.itu.int/dms_pub/itu-d/oth/01/0B/D010B0000073301PDFS.pdf

National Congress of the Dominican Republic. (2007). *Law number 53 of 2007, on "High Technology Crimes and Offenses"*. Santo Domingo.

Pultarova, T. (2016). News Briefing: Cyber security-Ukraine grid hack is wake-up call for network operators. *Engineering & Technology, 11(1)*, 12-13.

Republica Digital. (2018). *Ciberseguridad*, available at: from https://republicadigital.gob.do/eje/ciberseguridad/, accessed on: July 21, 2018.

Wootson, C. R., Jr. (2018). *It's time to stop laughing at Nigerian scammers – because they're stealing billions of dollars*, available at: from https://www.washingtonpost.com/news/business/wp/2018/06/12/its-time-to-stop-laughing-at-nigerian-scammers-because-theyre-stealing-billions-of-dollars/?noredirect=on&utm_term=.e64a26210213, accessed on: June 27, 2018.

Yunes, L. (2017, June 12). *Personal interview.*