International Civil Aviation Organization

WORKING PAPER

AN-Conf/13-WP/279
27/9/18
English and Spanish only[1]

THIRTEENTH AIR NAVIGATION CONFERENCE

Montréal, Canada, 9 to 19 October 2018

COMMITTEE A

Agenda Item 5: Emerging issues
5.4: Cyber resilience

AERONAUTICAL CYBER RESILIENCE

(Presented by the State Members of COCESNA)

EXECUTIVE SUMMARY

In this paper COCESNA wants to highlight his interest in the subject of the Cyber resilience, as a support for an organization to have the ability to address adverse conditions, before an eventual attack against assets essential to the functioning of the agencies, companies or administrations and the purposes of its reason to be.

Action: The Conference is invited to:
a) Recommend to the aviation Community be duly prepared to generate an effective response to the cyber incidents that may occur in the operations day by day;
b) Recognize the importance of developing the Government's cyber-security to cope with cyber threats; and
c) Address cyber threats, through appropriate tactics, techniques and procedures based on worldwide Standards and practices.

1. INTRODUCTION

1.1 The cyber resilience is a company's ability to anticipate, withstand, recover and evolve to improve their capabilities to confront adverse conditions, extreme situations or attacks against the assets needed to operate. A Cyber resilience company makes an alignment of priorities of cybersecurity with the mission and goals of the business.

1.2 The cyber incident threaten both assets and critical business processes, therefore, the objective of the cyber resiliency is to ensure that these processes are still available to an acceptable level even during an incident. To achieve this objective, it is vital that they understand and they prioritize the needs of interest groups, identified the critical business processes required to achieve the mission and

[1] English and Spanish versions provided by COCESNA.

goals set by the company. An IT governance framework can help mitigate some of the risks of cyber security.

1.3 COCESNA has established a project for the implementation of a framework of Government and Information Technology and Communications management, whose objective is to generate the expected value of the TIC investments being made, through the establishment of good practices and the strengthening of the company's capabilities (enablers). This helps to get optimum value of information technologies while maintaining a balance between the benefits, risks and resources. Within this framework, the Strategic Plan of information technologies and communications (SPICT) was developed. The creation of value as defined in COBIT5, is a balance between profit, the optimization of risks and the optimization of resources.

2. DISCUSSION

2.1 Within the improvements identified with the establishment of the framework of TIC management and Government has made security of information taking as a reference the ISO 27000 standard, as result was obtained a gap analysis and a plan of action that comes to strengthen and ensure the availability, integrity and confidentiality of the data.

2.2 By a proper compliance with information security regulations a number of policies and procedures that help with the regulation of hardware and software tools, as well as a proper classification of information, have developed access controls robust, response to security incidents, support information, etc. Strategies and activities to develop the Strategic Plan of the information technology and communications are summarized in:

- The consideration that persons may also cause or contribute significantly to an incident, has been defined a training plan to employees of COCESNA, regarding security of information and persistent threats to which they are exposed by part of the attackers;

- A diagnosis of cybersecurity taking as a reference the framework of cybersecurity for critical infrastructure, developed by the National Institute of standards and technology (NIST), the basic features of the framework are intended to identify, protect, detect, respond and recover and

- Strengthen the organizational structure using a unit of cybersecurity, which will take care of managing cyber risk to increase and strengthen the value of the business through a proper strategy that allows a proper cyber resilience in the Corporation. This unit will have the aim of detect, analyze and respond to incidents of cyber security in a timely manner before any attempt at attack on networks, servers, databases, applications, web site, etc.

2.3 Due to the need to provide the necessary expertise on cybersecurity a group of employees has been selected to receive training on cyber security (CSX) fundamentals, promoted by the Information Systems Audit and Control Association (ISACA), which has been developed in collaboration with experts from leading cybersecurity worldwide companies.

3. CONCLUSION

3.1 Cybersecurity evolves globally, becoming transformed into some of the really shocking technological disruptions, so that it must be properly prepared and generating an effective response to the cyber incidents that may occur in the daily operations.

3.2 COCESNA now is in process of developing the government's cyber-security to cope with cyber threats, establishing a framework that will guide the development and continuous improvement of the strategy of value creation-oriented cybersecurity. Through the cybersecurity government an appropriate treatment will be giving to cyber threats, allowing to have the appropriate tactics, techniques and procedures based on worldwide standards and practices.

— END —