Pan American Health Organization
World Health Organization
REGIONAL OFFICE FOR THE Americas

162nd SESSION OF THE EXECUTIVE COMMITTEE

Washington, D.C., USA, 18-22 June 2018

Provisional Agenda Item 7.4

CE162/INF/4
11 April 2018
Original: English

CYBERSECURITY IN PAHO

Introduction

1. As cyber threats continue to impact international organizations, the Pan American Sanitary Bureau (PASB) is committed to strengthening the cybersecurity measures needed to protect data and maintain a safe digital environment.

2. This document reports on PASB's efforts to assess and strengthen cybersecurity. It summarizes ongoing initiatives and the roadmap that has been developed to further strengthen the Bureau's cybersecurity posture.

Background

3. PASB makes extensive use of information technology (IT) to carry out its work. With this increased dependence on technology, it is imperative to continuously maintain a high level of confidence in the security of PASB data.

4. In 2016, PASB received strategic advisory services on cybersecurity from the United Nations International Computing Centre (UNICC). Existing cybersecurity measures were assessed against industry best practices outlined in the International Organization for Standardization's ISO 27001 standard, and a Cybersecurity Roadmap was defined.

Accomplishments in 2017

Completion of ISO 27001 assessment

5. In 2017, PASB completed a cybersecurity assessment that measured currently implemented controls against industry best practices as outlined in the ISO 27001 standard. Part of the ISO 27000 series, ISO 27001 is a widely accepted standard that identifies requirements for establishing, implementing, operating, monitoring, reviewing, maintaining, and continually improving an information security management system (ISMS). The assessment evaluated adherence to the standard in the context of the mission of the Pan American Health Organization (PAHO).

6. The assessment utilized the Capability Maturity Model to measure the maturity of information security controls implemented within PASB. During the course of the assessment, several strengths in PASB's cybersecurity capabilities were identified, including:

a) introduction of a full-time information security officer position;

b) continued engagement for advisory support on strategic information security, provided by the United Nations International Computing Center (UNICC);

c) continued engagement in efforts to implement externally managed security services on the network security;

d) consolidated framework for information security policies and procedures;

e) data backup and recovery capabilities;

f) Organization-wide use of anti-malware software;

g) Organization-wide use of vulnerability-scanning software;

h) cyber-incident response integrated into Business Continuity Plan;

i) Organization-wide modernization of firewalls and web filtering;

j) enhanced security of wireless infrastructure;

k) strengthened controls on physical access to PASB data centers;

l) cybersecurity contractual requirements integrated into supplier contracts.

7. The assessment prioritized recommendations as high, moderate, or low, depending on their alignment with the requirements of the ISO standard. In total, there are two high-priority recommendations, four moderate-priority recommendations, and nine low-priority recommendations.

8. The two high-priority recommendations call on PASB to strengthen cyber-incident response capabilities and to increase cybersecurity awareness in the Organization's workforce. The study also recommended increased cybersecurity operational capabilities to detect and remediate weaknesses and threats in the existing information technology environment.

Completion of PMIS security assessment

9. A security assessment of the PASB Management Information System (PMIS) was performed. The assessment was carried out by comparing the controls implemented in the PMIS environment to those recommended by *a)* international standard ISO 27001 on information security management systems, and *b)* the Cloud Security Alliance. The Cloud Security Alliance promotes the use of best practices for providing security assurance within cloud computing, and provides education on the uses of cloud computing to help secure all other forms of computing. The assessment did not identify any critical information security

vulnerabilities. Nine medium-priority recommendations were identified to further enhance the cybersecurity of the platform.

Cybersecurity incidents

10. During 2017, PASB registered no critical cybersecurity incidents affecting the confidentiality, availability, or integrity of PASB information or information technology resources. PASB did experience several phishing incidents in 2017, the purpose of which was to acquire usernames and passwords of users in order to carry out unauthorized activities on PASB systems. With its current cybersecurity capabilities, PASB was able to detect these incidents and implement mitigating controls, and PASB did not detect any unauthorized activities on its IT systems. PASB also observed that the cybersecurity capabilities of the PMIS provider played a critical role in preventing any unauthorized transactions. The rise in the frequency and sophistication of phishing, however, indicated a need to bolster the access control mechanisms in PASB's information IT systems, and this recommendation was included in the Cybersecurity Roadmap detailed below.

Cybersecurity Roadmap

11. Based on the recommendations from the assessments and on the security incidents detected, and in line with the strategic plan of the Organization, PASB developed a Cybersecurity Roadmap that identifies projects and initiatives to improve cybersecurity. A number of those identified in the roadmap were implemented in 2017, and others are to be implemented throughout 2018 and 2019. The implementation of these initiatives will raise the maturity of PASB's cybersecurity capabilities and enhance the Bureau's ability to protect its information.

12. The following projects and initiatives were accomplished in 2017 to enhance PASB's capabilities in cybersecurity, following the Cybersecurity Roadmap:

a) *Recruitment of full-time information security officer:* The recruitment of the information security officer was completed in 2017.

b) *Antivirus reporting and monitoring:* The antivirus protection in use was upgraded to the latest version in order to enhance capabilities to monitor and detect advanced threats. In addition to this, alerting capabilities were implemented that strengthened the Organization's capabilities to respond to major virus incidents.

c) *Consolidation and implementation of firewall managed security services:* PASB completed the implementation of externally managed security services in 28 locations to protect the Organization's information technology infrastructure from external threats. Work at the remaining two locations will be completed in the first quarter of 2018.

d) *Threat intelligence services:* Subscription to an external threat intelligence service was procured with the aim of receiving early notifications on cyber threats that could affect the Bureau. The service will enable PASB to receive intelligence

reports on threat actors and networks involved in cybercrime, hacking, and fraud, leveraging its unique access to malicious actor communities across the dark web and the deep web more broadly. The relevant information will be triaged and forwarded to PASB. The subscription to this service will also provide PASB with access to actionable threat intelligence information from other United Nations agencies subscribing to the service. Additionally, the service will enable PASB to monitor the dark web for credential thefts.

e) *Security risk rating services:* A security risk rating service monitors the Organization's internet presence and generates alerts when a security vulnerability or incident is observed. The subscription service also provides PASB with a security rating that indicates the effectiveness of the Bureau's cybersecurity capabilities and enables PASB to compare its cybersecurity program to those of other agencies in the United Nations system. Any increase or decrease in the security rating generates an alert that will be monitored.

f) *Regular security briefings with all PASB country offices and Pan American centers:* Regular monthly meetings with all country offices and centers were introduced with a view to sharing progress on implementation of the Cybersecurity Roadmap.

g) *Penetration testing:* A security test of a critical application was completed. The aim was to assess the cybersecurity measures implemented to protect the information stored and processed by the application. The test did not identify any critical vulnerability.

h) *Fine-tuning of vulnerability management system:* The vulnerability scanning software implemented was further fine-tuned and configured in order to establish a global picture of vulnerabilities affecting PASB IT systems. This tool played a critical role in protecting PASB IT systems from the global cyber incident commonly known as WannaCry, which occurred in the second quarter of 2017. WannaCry reportedly affected thousands of computers in more than 150 countries globally, but PASB IT systems were not affected and remained protected through the continuous monitoring provided by this software.

i) *Advanced threat protection:* The procurement of Microsoft's advanced threat protection was completed with the aim of enhancing the ability to detect and respond to cyber threats. The implementation of this system will provide preventive protection, allow detection of cyber attacks, and enable centralized end-to-end management of the security lifecycle of PASB IT systems.

j) *Decommissioning of legacy systems:* Approximately 63 legacy systems were decommissioned with the aim of reducing vulnerabilities that were not being patched by the vendors.

k) *Consolidation and enhancement of security patch management:* The software used to deliver security patches to computers was further consolidated to ensure that it can be monitored centrally.

l) *Protection of PAHO's public website:* A web application firewall was procured to further protect PAHO's public website from cyber attacks. The service will provide protection from advanced persistent threats targeting PAHO's public website. Additionally, the service will improve the performance and delivery of the website.

m) *Security awareness:* Several information security bulletins were sent out in PASB to raise user awareness of cyber threats such as phishing, ransomware, and viruses, as well as to provide general cybersecurity information.

13. Several cybersecurity projects are planned for completion in 2018-2019. The paragraphs below briefly summarize these projects by category:

a) *Enhancement of authentication and digital access control mechanisms:* These projects will aim at further enhancing the mechanisms employed by PASB to protect services such as PMIS, email, and remote access. These projects will also safeguard PASB IT systems from currently prevalent cyber threats that target vulnerabilities in access control and authentication mechanisms.

b) *Improvements to cyber-incident response capabilities:* As it is impossible to always prevent cyber incidents from occurring, projects in this category will aim to further strengthen PASB's cyber-incident response and remediation capabilities.

c) *Information security awareness:* PASB will continue to roll out its information security awareness program to include different ways of raising awareness in users who access PASB information resources.

d) *Protection of publicly accessible PASB information systems:* PASB will continue to implement several projects aimed at increasing the defenses that shield its publicly accessible information systems from being targeted by attackers seeking to compromise the cybersecurity of PASB information systems.

e) *Enhancement of monitoring and alerting capabilities:* With the rise in the sophistication and frequency of cyber threats, PASB will increase and further enhance security monitoring capabilities aimed at the rapid detection of cyber incidents. These initiatives will significantly improve the response and remediation techniques already implemented within PASB, and will allow PASB to have early detection and remediation of computer vulnerabilities.

14. The implementation of various initiatives identified in the Cybersecurity Roadmap will improve PASB's cybersecurity posture to further align it with the recommendations of ISO 27001. These initiatives are in line with industry best practices and will enhance PASB's capabilities in detecting, reacting, remediating, and learning from cybersecurity incidents.

Action by the Executive Committee

15. The Executive Committee is invited to take note of the report and provide any comments it deems pertinent.

- - -