World Health Organization

EXECUTIVE BOARD
148th session
Provisional agenda item 18.1

EB148/30
11 January 2021

Update on information management and technology

Report by the Director-General

1. At the thirty-first meeting of the Programme, Budget and Administration Committee of the Executive Board in January 2020, the Secretariat reported on its initiatives on cybersecurity.[1] In addition, the most recent Report of the Internal Auditor,[2] considered at the Committee's thirty-second meeting, highlighted key elements of the audit of the Cybersecurity Roadmap. The present report is a response to the Committee's request to the Secretariat to report on the management of cybersecurity.

PROGRESS PRIOR TO THE PANDEMIC

2. Cybersecurity is one of the key result areas in the information management and technology strategy. The objective is to protect the Secretariat's digital assets, strengthen data security and ensure the ability to deliver services with an acceptable level of risk.

3. Initiatives undertaken in support of cybersecurity have included the implementation of Organization-wide mandatory training on cybersecurity awareness; regular phishing exercises conducted monthly; the launch of the annual cybersecurity awareness event; the creation of a central repository of system logs for forensics purposes; the standardization of firewall management; the deployment of a global anti-virus solution; the implementation of an internet network traffic filtering service; and the implementation of threat intelligence so that proactive measures can be taken to avoid future and predicable incidents.

4. The Secretariat also established a dedicated and independent cybersecurity team. It furthermore initiated the establishment of a fit-for-purpose integrated security operations centre, covering identification, prevention, detection, protection and response to cyberattacks when they occur.

5. The governance area was strengthened through: the publication of the approved cybersecurity strategy, the Cybersecurity Roadmap and global policy, rules, standards and standard operating procedures; the establishment of the Cybersecurity Council; and the revision of the charter of the global Information Technology Steering Committee to address the need for a holistic responsibility for cybersecurity.

[1] Document EB146/40.

[2] Document A73/28.

RESPONSE TO COVID-19 RELATED ATTACKS

6. Since the declaration of the COVID-19 pandemic, the Secretariat has observed increasing targeted cyberattacks. These include spear phishing, impersonation, phishing, vishing (voice phishing) and attacks on IT infrastructure and applications. Between March and May 2020, over 130 000 domains related to COVID-19 were registered, of which 70% were estimated by researchers to be fake and to have been used for multiple cyberattacks.

7. Cyberattacks continue to increase significantly in volume and complexity. The initial threat intelligence solution was deemed to be insufficient. A new solution was implemented on 7 May 2020, which revealed further threats from advanced persistent threat groups. This allowed the Secretariat to act faster in remediating existing IT infrastructure, systems and tools.

8. However, based on trend analyses conducted by companies that specialize in cybersecurity, cyberattacks are expected to continue. Efforts to identify, prevent, protect against, detect, respond to and recover from these cyberattacks need to continuously be intensified. Consequently, the Secretariat has accelerated the implementation of the cybersecurity programme. **Key actions have been taken**, including those set out below.

(a) **Funding.** The report of the Internal Auditor of October 2020[1] stated that the US$ 1.3 million received was inadequate to implement the Cybersecurity Roadmap. The global Information Technology Steering Committee provided an additional US$ 4.7 million, allocating a total of US$ 6 million to the programme.

(b) **Cybersecurity team.** The size of the team has been increased from six members to 11, with resources located in Geneva and Budapest. A *red team* was established to undertake offensive actions to check IT systems security, including identification of system vulnerability and risk assessment.

(c) **Establishment of a managed and integrated security operations centre.** A managed security operations centre, in which security operations are integrated with a security information and event management service, was set up in June 2020. The centre provides visibility on all the security incidents and allows the Secretariat to focus on escalated security events. Between August and November 2020, 14.5 billion security events were identified. With the implementation of the security operations centre, the Secretariat was able to filter, process, analyse and focus its efforts on 243 escalated security incidents.

(d) **Better enforcement of user authentication.** The Secretariat is augmenting traditional authentication methods (such as username and password authentication) with multifactor authentication services (e.g. soft tokens) to prove user identity. The full enforcement of multifactor authentication has been completed, covering all the Secretariat's services available over the Internet.

(e) **Continuous monitoring of the Organization's IT assets.** The Secretariat has implemented an endpoint detection and response solution to address the need for continuous monitoring of and response to threats against the Organization's IT assets by using tools to detect, contain (if necessary) and investigate suspicious activities. It provides visibility across the working environment and creates the capability to detect, protect and respond in a timely manner.

[1] Document A73/28.

To date, 88% of all computers and servers across the Organization have been covered and work is under way to complete 100% implementation by the second quarter of 2021.

(f) **System to prevent email impersonation of the Organization to the public.** On average, 2.3 million unique email messages every month are being sent on behalf of <@who.int>. In April 2020, about 80% of these messages were impersonations. The Secretariat implemented a domain-based message authentication, reporting and conformance (DMARC) solution in May 2020 in order to minimize this behaviour and allow only authorized sources to send messages in the name of the Organization. Since then, 96% of the email messages have been compliant, with the remaining 4% involving impersonations that were removed and never reached mailboxes of organizations that have implemented DMARC solutions.

(g) **Retirement of legacy applications.** Old systems developed using obsolete technology are vulnerable to sophisticated attacks. Security patches are being applied, but in some instances outdated system design and architecture mean that such patches are not sufficient to defend against malicious attacks. Therefore, the Secretariat has replaced a significant number of applications that can no longer be remediated or patched.

9. Effective management of the cybersecurity programme requires constant communication and coordination. In particular:

(a) internally, global coordination is channelled through the cybersecurity group, which is composed of the cybersecurity team and representatives of all regions. This group coordinates WHO's activities related to cybersecurity, including the implementation of cybersecurity procedures, standards and solutions;

(b) a direct communication channel has been established with multiple computer emergency response teams, government organizations and private companies in order to receive and share actionable threat intelligence. Indicators of compromises are shared daily.

10. In addition, corporate systems and applications − including the Global Management System, email, websites, collaborative platforms, development platforms − are constantly monitored and security patches are applied without delay to reduce or eliminate cybersecurity risks.

SUSTAINING CYBERSECURITY EFFORTS

11. Cybersecurity breaches and attacks, when successful, are costly. Potential costs include damage to the Secretariat's value and reputation; direct financial loss (remediation, time worked, legal costs, public relations costs, and notification costs); impact on system availability; loss of critical data; and loss of data integrity.

12. In spite of all the aforementioned efforts made by the Secretariat, there are still gaps to address and a number of areas to improve. The following eight new workstreams are essential to protect the Secretariat against actors posing an advanced persistent threat and are included in the scope of the Cybersecurity programme.

(a) **Improved email protection, with safe links and attachments.** More than 90% of cyberattacks start with e-mail phishing, using links and attachments. Built-in email safety features will provide protection by means of enhanced automatic checking of email attachments for malicious content and time-of-clicks in email messages will be verified.

(b) **Safer Internet access.** Use of a global cloud proxy will provide protection to endpoint devices accessing the Internet, both inside and outside the Organization's offices. This establishes control of Internet access for endpoint devices by providing website verification, filtering and malware protection.

(c) **Application vulnerability scanning.** This will provide consistent and better security assessment for mobile and web-based applications during development, testing and operations. The objective is to identify system, network and application vulnerabilities.

(d) **Web application firewall.** This represents a new generation of protection and access for web applications. A web application firewall acts as a shield and gateway that is placed between the web applications and the Internet and prevents applications from being attacked. External access is tracked, filtered and monitored.

(e) **Vulnerability tracking control.** This creates an online, automatic verification and reporting system that will be integrated with incident, change and patch management processes. It will facilitate the remediation of vulnerabilities related to unpatched systems and applications.

(f) **Privileged access management.** This not only provides the Organization with visibility of the potential threats posed by various types of privileged access but also, through the implementation of appropriate tools, provides protection against the abuse of accounts with high privileges (such as system administrators).

(g) **Segregation of duties management.** This ensures that there is a clear division of duties and roles to access systems. There should be no instances in which an individual is able to both raise and approve transactions in order to commit cybercrime (theft or fraud for personal gain).

(h) **Deception technology.** This generates traps or deception decoys that are designed to trick threat actors into thinking they have gained a foothold in the Organization (for example, to steal credentials or secrets). This will improve the Secretariat's ability to detect external intruders' behaviour and use that knowledge to strengthen the security of its systems.

13. Sustaining momentum is critical. The inclusion of these workstreams in the Secretariat's cybersecurity effort will further strengthen identification, detection, prevention, protection and response modalities leading to the implementation of the Cybersecurity Roadmap.

SUSTAINABLE FUNDING

14. Decision WHA70(16) (2017) authorized the Director-General to allocate, by the end of each biennium, at least US$ 15 million, as available, for information technology investment needs within the Infrastructure Fund.[1] The current cybersecurity programme is funded from the Infrastructure Fund.

15. The Secretariat considers cybersecurity to be a top priority. It is important to safeguard all the efforts made to date and to continue the work being done to protect the Organization. Initial cost estimates have been made in order to complete the cybersecurity programme. However, sustaining

[1] See document WHA70/2017/REC/1.

cybersecurity operations beyond programme completion will also require significant investments in the coming years.

16. The Independent Expert Oversight Advisory Committee has recommended that an overall review of the Organization's IT spending be undertaken as part of the overall planning cycle.[1] This review should consider both the costs of running the Secretariat's business and all IT change initiatives, including cybersecurity. The Secretariat is conducting this review in the broader context of the preparation of the Proposed programme budget 2022–2023.

17. The Secretariat will provide Member States, through the thirty-fourth meeting of the Programme, Budget and Administration Committee with the ratio of initiatives (i.e. operations versus changes), including an updated overall review of future IT spending.

ACTION BY THE EXECUTIVE BOARD

18. The Board is invited to note the report.

= = =

[1] See document EBPBAC30/2.