United Nations A/68/552

General Assembly

Distr.: General
25 October 2013

Original: English

Sixty-eighth session
Agenda item 134
Proposed programme budget for the biennium 2014-2015

Progress on the implementation of recommendations related to strengthening information and systems security across the Secretariat

Report of the Secretary-General

Summary

The present report is submitted pursuant to paragraph 18 of part I of General Assembly resolution 67/254, in which the Assembly requested the Secretary-General to provide an update on the status of implementation of the actions taken to address information security issues in the context of the proposed programme budget for the biennium 2014-2015. An independent assessment and information security breaches that occurred in 2013 demonstrate significant shortcomings that expose the Organization to an unacceptable level of risk. The present report includes measures taken to guard against any threats of cyberattack and additional resource requirements in the amount of $3,440,700 before recosting, under section 29E, Office of Information and Communications Technology, of the proposed programme budget for the biennium 2014-2015, in order to address the most urgent information security needs of the Organization.

13-53216 (E) 311013

I. Introduction

1. In paragraph 107 of resolution 66/246, the General Assembly requested the Advisory Committee on Administrative and Budgetary Questions to request the Board of Auditors to audit and evaluate the handling of information and communications technology (ICT) affairs in the Secretariat, including the Office of Information and Communications Technology, and to report thereon to the Assembly at the main part of its sixty-seventh session. The Board conducted its audit in October 2012 and submitted its report (A/67/651) to the Secretary-General on 19 December 2012.

2. In paragraph 95 of its report, the Board of Auditors stated that the United Nations does not have an adequately secure information environment and that existing security controls fall short of what the Board would expect in a modern global organization. It also stated that the Secretariat had extremely limited capacity for security monitoring and as a result was not positioned to adequately detect and respond to all attempted or successful breaches.

3. In a subsequent report on the implementation of the recommendations of the Board of Auditors (A/67/651/Add.1), the Secretary-General stated that the recommendation related to strengthening information and systems security across the Secretariat was being addressed as a matter of urgency and that the Administration was developing an action plan, comprising short-term measures to address the most urgent shortcomings and the definition of a sustainable medium- and long-term strategy for information security. The action plan consists of 10 initiatives focusing on 3 areas, as follows:

(a) Preventive controls. The Secretariat will strengthen technical controls of the ICT infrastructure designed to:

(i) Establish stricter controls of computing devices used on the United Nations network;

(ii) Prevent harmful forms of Internet traffic and e-mail by strengthening technical measures that protect the perimeter of the United Nations network;

(iii) Segment the network in order to isolate areas where viruses may hide potential attacks;

(iv) Improve information security awareness among United Nations personnel through the delivery of training and outreach;

(b) Improved incident detection and response capabilities. In order to adjust to an environment where the risk of threats has significantly increased, the Secretariat will introduce additional intrusion detection systems and monitor its networks systematically;

(c) Governance, risk and compliance. An information security directive, which establishes the fundamental principles of information security in the United Nations and acts as the foundation for policy and governance instruments, will be ratified and implemented.

4. The Advisory Committee on Administrative and Budgetary Questions, commenting on the report of the Board of Auditors on the handling of information and communications technology affairs in the Secretariat (A/67/770), subsequently

recommended that the Secretary-General be requested, when developing his proposals for the implementation of the information security action plan, to make every effort to prioritize and redeploy resources and to avoid, to the extent possible, submitting requests for additional resources. The Advisory Committee also stated that it shared the concerns of the Board with regard to the information security situation. It recommended that the Secretary-General be requested to proceed with the implementation of his action plan as a matter of priority and ensure adoption, without further delay, of the information security charter and associated policy documents in a manner that assures accountability at all levels of the Organization. In addition, the Advisory Committee stated that the Secretary-General should take prompt remedial action to address any hindrances that may arise to the effective implementation of the action plan or the promulgation and enforcement of information security policies throughout the Secretariat, and recommended that the Secretary-General be requested to provide, in the context of the proposed programme budget for the biennium 2014-2015, an update on the status of implementation of the actions taken to address information security issues. The Committee further requested the Board of Auditors to follow up on the implementation of its recommendations in this regard.

5. In paragraph 11 of part I, of its resolution 67/254, the General Assembly subsequently requested the Secretary-General to submit a progress report on the measures taken to address the priorities identified by the Board in its report (A/67/651), including on information technology security, and in paragraph 18 invited the Secretary-General to provide, in the context of the proposed programme budget for the biennium 2014-2015, an update on the status of implementation of the actions taken to address information security issues, including measures taken to guard against any threats of cyberattack.

II. Present situation

6. The Secretary-General is actively engaged in advancing the action plan to strengthen information security across the Secretariat and has concentrated on the most urgent and critical areas of the action plan at Headquarters. To date, the Office of Information and Communications Technology has made every effort to reprioritize and redeploy resources within its approved appropriation and to absorb, to the extent possible, the cost of implementing activities that would support the initiatives of the action plan. However, those resources have proven insufficient to address adequately all identified weaknesses. Furthermore, since the issuance of the report of the Board of Auditors, global information security breaches have increased significantly, both in frequency and sophistication, some of which have been directly experienced by the Secretariat.

7. As a result of those incidents, the Secretary-General considers it imperative that urgent action be taken, beyond what the Office of Information and Communications Technology has done thus far.

III. Initial steps in the implementation of the action plan to strengthen information security

8. The action plan was intended to address the most urgent shortcomings in information security as a matter of urgency and to define a sustainable medium- and long-term strategy for information security for the Secretariat. In view of the shortage of in-house expertise and the need for a solid analysis of the security posture of the Organization, it was determined that external expertise was necessary to validate and/or verify the potential risk. In July 2013, the Office of Information and Communications Technology decided to obtain an independent assessment of the status of information security at the Secretariat from an external consultancy firm, which validated and complemented internal findings and identified the vulnerabilities and operational deficiencies of the Organization in the area of information security. The independent assessment, as well as the occurrence of further information security incidents throughout 2013, demonstrated significant shortcomings that expose the Organization to unacceptable risks.

9. On the basis of the independent assessment, which focused primarily on the infrastructure in New York, the Secretary-General believes it is critical to further strengthen information security at Headquarters, urgently expand the independent assessment, in view of the increases in the number of cyberattacks against the Organization, and broaden the scope of activities to further strengthen information security at offices away from Headquarters, at the regional commissions and in field missions in 2014. Information made available through collaboration with those offices indicates that significant work is required to address vulnerabilities in them. Similarly, although field offices supported by the Department of Field Support may be less vulnerable, given that service is centrally provided from the United Nations Support Base in Valencia, Spain, and the United Nations Logistics Base in Brindisi, Italy, their vulnerabilities also need to be thoroughly assessed.

10. Activities already carried out to date to implement the action plan are detailed below:

(a) Preventive controls have been strengthened by limiting administrative privileges on newly issued and/or upgraded desktop and laptop computers. The acquisition of additional filtering systems for e-mail and Internet traffic is in process and is expected to be completed by the end of November 2013. Furthermore, servers are being reconfigured with current security patch levels to ensure that they are up to date insofar as their potential vulnerabilities are concerned. The firewall infrastructure at Headquarters has been reviewed and is being replaced with more advanced technology, which will increase protection against external attacks and internal network segmentation. In addition, a computer-based training course to raise awareness of information security among all staff across the Secretariat has been acquired;

(b) An assessment of all software applications presently in operation has been initiated to ensure their compliance with information security standards and best practices. This effort is carried out in the context of identifying all software applications that are to remain active after the implementation of Umoja and other enterprise systems and to ensure that they do not pose security risks;

(c) A managed service for the deployment and ongoing operation of intrusion detection systems has been obtained for the main data centres in the

primary and secondary data centres in New York and New Jersey, as well as the enterprise data centres in the Support Base and the Logistics Base. Furthermore, existing sources of cyberintelligence across the Secretariat have been consolidated to increase its ability to proactively adjust defensive measures;

(d) An information security policy directive was developed and issued to all heads of departments and offices on 7 March 2013 as a general framework for the information security policies, procedures and guidelines of the Organization. This directive also mandates that information security incidents be reported and that related actionable intelligence across the Secretariat be shared. A set of technical and procedural controls for minimum requirements for public websites has been developed by the Information Security Special Interest Group of the United Nations System Chief Executives Board for Coordination (CEB), based on a draft by the Office of Information and Communications Technology, and endorsed by the ICT network within the CEB High-level Committee on Management. In addition, 52 ICT policies and procedures are being developed to help improve system performance, security and production integrity. In cooperation with the Department of Public Information, the document will be issued as an administrative instruction in 2014 to address the significant exposure of public websites and the historical evidence of several breaches. In addition, the Office of Information and Communications Technology has reallocated resources to build an internal compliance function intended to increase compliance with internal policies and procedures and industry best practices. The Office has also established an information security working group as part of the ICT Management Coordination Group to increase the level of communication across duty stations, including offices away from Headquarters, the regional commissions and field missions.

11. In addition to the measures implemented as part of the action plan, the Organization is introducing significant changes to its global ICT operations, in line with, and to support the implementation of, Umoja and other ancillary systems. These changes include, inter alia, the implementation of a new global wide-area network based on Multiprotocol Label Switching, the use of a standard access layer (Citrix) for all enterprise systems and the migration of software applications to the enterprise data centres in Valencia and Brindisi. These changes will enable tighter access control and a more robust management of the ICT infrastructure and reduce its vulnerability to intrusion.

12. ICT security, as an essential part of business continuity and disaster recovery, also plays an important role for field missions, in view of their operational environment. The Department of Field Support has recently established a security policy framework that is centred on the Department’s Field Technology Operational Centre, comprising the ICT facilities in the Support Base and the Logistics Base. In line with this policy framework, security assessments of deployed information systems, infrastructure and other information assets are regularly conducted in the Field Technology Operational Centre and in field missions.

IV. Further action needed

13. Following the independent assessment and the information security breaches that occurred in 2013, it has become apparent that the United Nations has insufficient information security controls in place, not only for traditional

components of the information and communications infrastructure, but also with respect to other infrastructure elements. Building management systems, access control and monitoring solutions, telephony and videoconferencing systems and audiovisual devices, which traditionally have not been digitally controlled, are now also exposed to digital and potentially Internet-based threats. Additional detailed assessments will be required to ensure that these devices are included in a comprehensive information security strategy.

14. An assessment of the systems used in the Department of Field Support has revealed the need for new software tools to enable intrusion monitoring and filtering, along with upgraded firewalls, to enhance the security environment of the Organization in both of the locations cited above and in other locations. New security measures have been instituted and more work is already under way.

15. It has also been revealed that the reputational risk of the Organization may be increased due to operational deficiencies in the management of web information. The Organization has consequently identified a need to examine closely externally hosted websites, reviewing security controls and providing assistance to Secretariat departments in the area of website redesign for the purposes of resistance against intrusion or defacement.

16. The comprehensive information security strategy, which includes web-based and non-traditional systems and addresses the underlying systemic issues, will be a central part of the overall ICT strategy, which will be submitted for consideration by the General Assembly at its sixty-ninth session.

17. In the interim, however, further immediate actions are urgently needed for continued mitigation of unacceptable risks to the Organization, building on the progress made so far through the implementation of the action plan to strengthen information security across the Secretariat.

18. Due to the increasing need for interconnectivity and the interdependence of the Secretariat ICT systems, an attack or intrusion anywhere can lead to a compromise everywhere. Consequently, measures taken to date to execute the action plan also need to be implemented at other duty stations and complemented by a significant enhancement of the monitoring capacity of the Organization.

19. The following actions, for which resources are being requested in the present report, are proposed as interim measures until the revised ICT strategy is presented:[1]

(a) Expansion of the intrusion detection service to cover offices away from Headquarters and the regional commissions. This service has been established and is limited to the primary and secondary data centres in New York and New Jersey and the enterprise data centres at the Support Base and the Logistics Base through the reprioritization of the existing resources of the Office of Information and Communications Technology in 2013. However, additional resources will be required in 2014 to continue to cover the cost of services in locations already established and increase the coverage to overseas duty stations;

[1] Owing to the sensitive nature of these actions and in order to minimize operational risks, only a generic description can be provided in the present report.

(b) Increased coverage and upgrading of the firewall infrastructure and upgrading of filtering solutions for e-mail and Internet traffic to include offices away from Headquarters and the regional commissions to strengthen the security capabilities of the network globally;

(c) Enhancement of the internal security monitoring capacity. Additional tools and staff resources are required to establish a significantly enhanced capacity to monitor the information and communications technology environment for attempted and successful information security breaches;

(d) Deployment of a vulnerability management system to enable the Organization to proactively identify specific weaknesses and prioritize their mitigation;

(e) Additional assessments of protective and detective controls for non-traditional infrastructure elements at Headquarters and the information and communications technology environment at offices away from Headquarters, the regional commissions and the enterprise data centres in Valencia and Brindisi.

20. It is clear that the fragmented ICT network of the Organization makes ensuring security more difficult and costly. The strategy of the Organization has been to move its data centres to Valencia and Brindisi in an expedited fashion in order to be able to deploy security and monitoring measures faster while improving the performance of operations and reducing costs. Furthermore, eliminating fragmentation will be a pillar of the new ICT strategy of the Secretary-General, to be submitted for consideration by the General Assembly at its sixty-ninth session.

V. Modification of the programme of work required for the period 2014-2015

21. In order to address information security properly across the Secretariat, it will be necessary to revise the approved programme of work of the Office of Information and Communications Technology for the period 2014-2015 (A/67/6/Rev.1, prog. 25) to incorporate activities related to the implementation of subprogramme 5, information and communications technology strategic management and coordination.

VI. Additional requirements under the proposed programme budget for the biennium 2014-2015

22. The additional resource requirements set out in the present report have emerged as a result of an independent assessment carried out in 2013, subsequent to the submission of the Secretary-General's proposed programme budget for the biennium 2014-2015 (A/68/6 (Sect. 29E)), and are based on an increase in the number and frequency of cyberattacks at the United Nations. Hence an additional appropriation will be required to cover the implementation of the activities described in detail above.

23. As detailed in table 1 below, it is estimated that a total amount of $3,440,700, before recosting, will be required for a 12-month period under section 29E in order to address the most urgent information security needs of the Organization, described

in detail in the present report, pending the consideration of a revised ICT strategy by the General Assembly at its sixty-ninth session.

Table 1
Summary of requirements by object of expenditure
(Thousands of United States dollars)

Object of expenditure	*2014-2015 estimate*
Other staff costs	581.4
Travel of staff	150.0
Contractual services	1 325.0
General operating expenses	59.3
Furniture and equipment	1 325.0
Total	**3 440.7**

Table 2
Resource requirements under section 29E of the proposed programme budget for the biennium 2014-2015, before recosting
(Thousands of United States dollars)

Object of expenditure	*Provision in A/68/6 (sect. 29E)*	*Additional requirements*	*Total requirements*
Posts	36 168.6	–	36 168.6
Other staff costs	5 634.0	581.4	6 215.4
Travel of staff	467.8	150.0	617.8
Contractual services	12 697.0	1 325.0	14 022.0
General operating expenses	16 574.5	59.3	16 633.8
Supplies and materials	202.4	–	202.4
Furniture and equipment	948.2	1 325.0	2 273.2
Total	**72 692.5**	**3 440.7**	**76 133.2**

Other staff costs

24. The provision of $581,400 will cover general temporary assistance for a 12-month period to carry out functions aimed at addressing immediate security concerns associated with the redesign and application of the security practices of the Office of Information and Communications Technology and the associated incident response. The required temporary positions are as follows:

(a) One general temporary position equivalent to a P-4 post to carry out the duties of Security Engineer. The position will provide the additional technical expertise associated with the application of the recently implemented intrusion detection system. It is estimated that the Organization will experience, at a minimum, 70,000 to 100,000 security alerts monthly. The Security Engineer will work with an external contractor to systematically determine and address alerts of critical importance to be considered for immediate action. As the intrusion detection system will be rolled out to offices away from Headquarters and the regional commissions, it will gather information globally. The correlation of alerts between

locations and associated incident response activities must be coordinated globally. This global coordination function will be paramount for the effectiveness of the increased network insight as provided by the intrusion detection system. In addition, the Security Engineer may assist with the implementation of next-level firewall analysis and management;

(b) Two general temporary assistance positions equivalent to P-3 posts to perform new functions of malware analysis, pattern creation and incident correlation, which represent critical activities in determining the types of attacks the Organization may experience from so-called advanced persistent threats from various actors globally. The positions will also expand existing capabilities for penetration testing, vulnerability assessment and report generation and coordination of web application security testing. In addition, the positions may interface with software development teams to strengthen secure development standards and testing in offices globally.

Travel of staff

25. The provision of $150,000 is required to cover the cost of travel of two staff members to all offices away from Headquarters, the regional commissions and the enterprise data centres in Valencia and Brindisi for a minimum two-week period in order to:

(a) Conduct immediate independent security compliance assessments and technical testing, which must be completed to ensure that existing policies and standard operating procedures are adhered to and enforced on a regular basis. The mission will assess, validate and document previously undocumented local issues and information security risks. Furthermore, this will enable Headquarters staff to monitor and report levels of compliance, which is critical for implementation of the central ICT security strategy;

(b) Provide technical advice on and assistance with the implementation of the policy as well as verification of all new systems and applications that are planned;

(c) Hold meetings and conduct on-site and hands-on training with all business and technology stakeholders to ensure that the design and architecture of the preventive information security measures are understood and effectively implemented at all duty stations.

26. Proposed resources under this category would cover travel where Internet and/or audio conference technology is not an effective alternative in view of the confidential nature of the work involved. To the extent possible, back-to-back missions will continue to be undertaken to enable more efficient use of resources.

Contractual services

27. The provision of $1,325,000 would cover requirements for:

(a) Intrusion detecting services ($800,000) for the deployment and ongoing operation of intrusion systems, which have been initiated as part of the implementation of the action plan. The initial deployment in New York, Brindisi and Valencia was executed through the reallocation of existing resources. However, in order to achieve complete coverage globally, this service needs to be extended to

cover all data centres and duty stations. The ability to detect attempted intrusions is critical to allowing the Organization to respond in a timely manner;

(b) A vulnerability management system ($25,000), which would systematically and periodically scan all United Nations ICT assets, such as servers and other critical systems, to ensure their correct configuration and the timely deployment of critical security updates, assisting with the management of such assets and identifying vulnerabilities prior to their exploitation through an external attack;

(c) Individual personal services ($500,000) for highly specialized expertise to carry out, as needed, activities essential to the ongoing implementation of the information security strategy of the Secretariat, including newly established technologies, and conducting additional assessments of critical infrastructure elements. In addition, critical expertise will be required to address specific technical problems on a short-term basis and provide additional forensic or investigative abilities to ensure maximum understanding of the way in which information security deficiencies are addressed. The nature of the work, the aim of which is to transfer the knowledge gained to staff members, will be short-term and highly specialized.

General operating expenses

28. The provision of $59,300 would cover the cost of renting office space ($47,700) and a service level agreement (“A”) ($6,300) for three temporary positions in New York; a local area network ($1,800); and communications charges ($3,500).

Furniture and equipment

29. The provision of $1,325,000 would cover requirements for:

(a) Continuous monitoring capabilities ($200,000). The central collection and analysis of system logs complements the information provided by the intrusion detection system and allows the Organization to detect anomalous or suspicious activities not considered malicious. In addition to the ability to detect abuse and stealthy breaches, such a system will provide the ability to analyse the root cause of intrusions after their discovery and to determine their scope. The Security Information and Event Management system, the purchase of which is proposed, consists of specialized hardware, software and licensing based on the volume of information gathered;

(b) Enhancements to the firewall infrastructure ($1,000,000), including upgrading of existing firewalls ($500,000) and filtering solutions ($500,000) with the so-called “next generation” state-of-the-art firewalls and content-aware filters, which will enable the Organization to prevent or detect attempted attacks and intrusions that are designed to avoid detection by traditional tools. The upgrade is critical to addressing the constantly changing nature of attacks against the Organization. The upgrade has already been initiated at Headquarters and the enterprise data centres in Valencia and Brindisi by reallocating existing resources in 2013. However, enhancements must be extended to cover all data centres and duty stations;

(c) Web application security testing ($125,000), including the acquisition of updated web application security testing tools in the form of software licences for local use or as third-party “software as a service” for enterprise-wide

implementation. The tools may be used by in-house security personnel and/or web developers to strengthen United Nations website security.

VII. Actions to be taken by the General Assembly

30. **The General Assembly is requested:**

(a) **To take note of the present report;**

(b) **To approve an additional appropriation in the amount of $3,440,700 under section 29E, Office of Information and Communications Technology, of the proposed programme budget for the biennium 2014-2015 in order to implement urgent requirements to strengthen ICT security in the Secretariat, as a charge to the contingency fund.**