Nations Unies A/68/552

Assemblée générale

Distr. générale
25 octobre 2013
Français
Original : anglais

Soixante-huitième session
Point 134 de l'ordre du jour
Projet de budget-programme pour l'exercice biennal 2014-2015

État d'avancement de l'application des recommandations relatives au renforcement de la sécurité des systèmes informatiques au Secrétariat

Rapport du Secrétaire général

Résumé

Le présent rapport est soumis en application du paragraphe 18 de la première partie de la résolution 67/254, dans laquelle l'Assemblée générale a prié le Secrétaire général de décrire, dans le projet de budget-programme pour l'exercice biennal 2014-2015, l'état de l'application des mesures prises pour régler les problèmes de sécurité informatique. Une évaluation indépendante et des atteintes à la sécurité informatique intervenues en 2013 mettent en évidence des défaillances qui exposent l'Organisation à des risques d'un degré inacceptable. On trouvera dans le présent rapport les mesures prises pour parer à toute menace de cyberattaque et le montant des crédits supplémentaires (3 440 700 dollars) avant actualisation des coûts, demandés au titre du chapitre 29E (Bureau de l'informatique et des communications) du projet de budget-programme pour l'exercice biennal 2014-2015, afin de répondre aux besoins de sécurité informatique de l'Organisation les plus urgents.

13-53217 (F) 061113 061113

I. Introduction

1. Au paragraphe 107 de sa résolution 66/246, l'Assemblée a prié le Comité consultatif pour les questions administratives et budgétaires de demander au Comité des commissaires aux comptes de vérifier et d'évaluer la manière dont les questions relatives à l'informatique et aux communications sont traitées au Secrétariat, notamment au Bureau de l'informatique et des communications, et de lui faire rapport à ce sujet durant la partie principale de sa soixante-septième session. Le Comité des commissaires aux comptes a procédé à un audit en octobre 2012 et présenté son rapport (A/67/651) au Secrétaire général le 19 décembre 2012.

2. Au paragraphe 95 de son rapport, le Comité des commissaires aux comptes a dit que la sécurité informatique de l'ONU comportait des lacunes et que les contrôles en place étaient bien insuffisants pour une organisation moderne d'envergure mondiale. Il a également dit que le Secrétariat disposait de très peu de moyens pour contrôler la sécurité et qu'il n'était donc pas en mesure de détecter toutes les atteintes ou tentatives d'atteinte à la sécurité ni d'y répondre.

3. Dans le rapport suivant sur l'application des recommandations du Comité des commissaires aux comptes (A/67/651/Add.1), le Secrétaire général a dit que l'Administration avait pris des mesures pour appliquer d'urgence la recommandation relative au renforcement de la sécurité des systèmes informatiques au Secrétariat et qu'elle mettait au point un plan d'action prévoyant des mesures à court terme visant à régler les problèmes les plus urgents et une stratégie à moyen et long terme pour la sécurité informatique. Composé de 10 initiatives relevant de trois domaines, le plan d'action s'articule comme suit :

a) Des contrôles préventifs. Le Secrétariat renforcera les contrôles techniques de l'infrastructure informatique afin :

i) De mettre en place des contrôles plus stricts des moyens informatiques reliés au réseau de l'ONU;

ii) D'empêcher les contenus malveillants sur les sites Web et la messagerie électronique en renforçant les mesures techniques qui protègent le périmètre du réseau de l'ONU;

iii) D'isoler les portions du réseau qui abritent des virus informatiques pouvant entraîner des attaques;

iv) De mieux sensibiliser le personnel de l'ONU à la sécurité informatique en organisant des séances de formation et des campagnes d'information;

b) Renforcement des capacités de détection des incidents et d'intervention. Afin de s'adapter à un environnement où les menaces se sont dangereusement multipliées, le Secrétariat mettra en place des systèmes supplémentaires de détection des intrusions et surveillera ses réseaux de manière systématique;

c) Gouvernance, risque et respect des normes. Une directive définissant les principes fondamentaux de la sécurité informatique à l'ONU et servant de fondement pour l'établissement d'instruments d'orientation générale et de gouvernance sera approuvée et appliquée.

4. Dans les observations qu'il a faites sur le rapport du Comité des commissaires aux comptes consacré à la manière dont les questions relatives à l'informatique et

aux communications sont traitées au Secrétariat (A/67/770), le Comité consultatif pour les questions administratives et budgétaires a recommandé que le Secrétaire général soit prié, lorsqu'il formulerait ses propositions pour l'application du plan d'action concernant la sécurité informatique, de n'épargner aucun effort pour redéployer les ressources en fonction des priorités et éviter dans la mesure du possible de demander des crédits supplémentaires. Il a également dit qu'il partageait les préoccupations du Comité des commissaires aux comptes en ce qui concernait la sécurité informatique. Il a recommandé que le Secrétaire général soit prié de pourvoir à titre prioritaire à l'application de son plan d'action et de veiller à ce que soient adoptés sans plus tarder la charte de sécurité informatique et les instruments d'orientation générale connexes de manière à ce que les responsabilités de chacun, à tous les niveaux de l'Organisation, soient arrêtées. Il a également dit que le Secrétaire général devrait prendre d'urgence des mesures pour lever les éventuels obstacles empêchant la bonne application de son plan d'action ou l'adoption et la mise en œuvre des politiques de sécurité informatique au Secrétariat, et recommandé qu'il soit prié de décrire, dans le projet de budget-programme pour l'exercice biennal 2014-2015, l'état de l'application des mesures prises pour régler les problèmes de sécurité informatique. Il a en outre demandé au Comité des commissaires aux comptes de suivre l'application des recommandations qu'il avait faites à ce sujet.

5. Au paragraphe 11 de la première partie de sa résolution 67/254, l'Assemblée générale a demandé au Secrétaire général de lui présenter un rapport sur les mesures prises pour répondre aux priorités définies par le Comité des commissaires aux comptes dans son rapport (A/67/651), en particulier concernant la sécurité informatique, et au paragraphe 18, elle l'a invité à décrire, dans le projet de budget-programme pour l'exercice biennal 2014-2015, l'état de l'application des mesures prises pour régler les problèmes de sécurité informatique, y compris pour parer à toute menace de cyberattaque.

II. Situation actuelle

6. Le Secrétaire général s'emploie activement à promouvoir le plan d'action visant à renforcer la sécurité informatique au Secrétariat et s'est principalement intéressé aux domaines les plus urgents et les plus critiques du plan. Le Bureau de l'informatique et des communications n'a épargné aucun effort pour redéployer les ressources en fonction des priorités, dans les limites des crédits inscrits au budget, et pour absorber dans la mesure du possible le coût des activités de mise en service qui appuieraient les initiatives arrêtées dans le plan d'action. Cependant ces ressources ne suffisent pas pour régler tous les problèmes qui ont été détectés. De plus, depuis la parution du rapport du Comité des commissaires aux comptes, les atteintes de portée mondiale à la sécurité informatique se sont multipliées, devenant de plus en plus fréquentes et de plus en plus sophistiquées, et le Secrétariat a pâti directement de certaines.

7. En conséquence, le Secrétaire général considère qu'il faut absolument prendre d'urgence des mesures, en complément de ce que le Bureau a fait jusqu'ici.

III. Premières mesures prises pour appliquer le plan d'action visant à renforcer la sécurité informatique

8. Le plan d'action entendait régler les problèmes les plus urgents et définir une stratégie à moyen et long terme pour la sécurité informatique au Secrétariat. L'ONU devant procéder à une analyse solide de l'état de la sécurité informatique et ne disposant guère des compétences nécessaires en interne pour ce faire, il a été décidé de faire appel à des experts extérieurs qui valideraient ou vérifieraient les risques détectés. En juillet 2013, le Bureau de l'informatique et des communications a décidé de confier à une société de consultants externes le soin de lui fournir une évaluation indépendante de la sécurité informatique au Secrétariat, l'objectif étant de valider et de compléter ce qui avait été détecté en interne et de cerner les faiblesses et les défaillances de l'Organisation dans ce domaine. Cette évaluation indépendante, ainsi que la multiplication des atteintes à la sécurité informatique en 2013, a mis en évidence les défaillances qui exposaient l'Organisation à des risques d'un degré inacceptable.

9. Le Secrétaire général a conclu de l'évaluation indépendante, qui portait essentiellement sur l'infrastructure à New York, qu'il fallait absolument renforcer la sécurité informatique au Siège et élargir d'urgence le champ de l'évaluation, compte tenu de l'augmentation du nombre de cyberattaques qui frappaient l'Organisation, et, en 2014, étendre aux bureaux hors siège, aux commissions régionales et aux missions les activités visant à renforcer la sécurité informatique. L'information obtenue dans le cadre de la collaboration avec ces entités montre qu'il reste beaucoup à faire pour remédier aux défaillances observées. De même, bien que les bureaux extérieurs qui reçoivent l'appui du Département de l'appui aux missions soient moins exposés aux risques, puisque ce sont la Base d'appui des Nations Unies à Valence (Espagne) et la Base de soutien logistique des Nations Unies à Brindisi (Italie) qui les assistent, il faut néanmoins analyser de près leurs faiblesses.

10. Les activités déjà menées pour appliquer le plan d'action sont décrites ci-après :

a) Les contrôles préventifs ont été renforcés en limitant les privilèges d'administrateur sur les nouveaux ordinateurs et les nouveaux portables et sur ceux qui ont été mis à niveau. D'ici à la fin novembre 2013, des systèmes de filtrage supplémentaires pour les sites Web et la messagerie électronique devraient avoir été achetés. Les serveurs sont en cours de reconfiguration avec les nouveaux correctifs de sécurité pour pallier les éventuelles défaillances. L'infrastructure de pare-feux du Siège a été revue et la technologie de pointe qui va la remplacer permettra de mieux protéger les systèmes informatiques des attaques extérieures et d'améliorer la segmentation du réseau interne. En outre, un cours de formation sur ordinateur a été acheté pour sensibiliser le personnel du Secrétariat au problème de la sécurité informatique;

b) Une évaluation de tous les logiciels installés a commencé afin de confirmer qu'ils sont conformes aux normes et aux bonnes pratiques de sécurité informatique. Ces mesures s'inscrivent dans le cadre de l'initiative qui vise à déterminer quelles applications devront être conservées après la mise en service d'Umoja et d'autres logiciels de gestion et à s'assurer qu'ils ne présentent aucun risque pour la sécurité;

c) Des services gérés pour le déploiement et le fonctionnement des systèmes de détection d'intrusions ont été obtenus pour les principaux centres de données situés dans les centres informatiques principaux et secondaires de New York et du New Jersey, ainsi que pour les pôles informatiques de la Base d'appui et de la Base de soutien logistique. Les sources de cyberveille du Secrétariat ont également été regroupées de sorte qu'elles sont mieux à même d'ajuster préventivement les mesures défensives;

d) Une directive sur la sécurité informatique a été établie et publiée à l'intention de tous les chefs de départements et bureaux le 7 mars 2013; elle récapitule les orientations, les procédures et la marche à suivre en la matière dans l'Organisation. Elle prévoit que les atteintes à la sécurité informatique soient signalées et que les renseignements suffisamment fiables pour justifier une intervention soient partagés au Secrétariat. À partir d'un projet établi par le Bureau de l'informatique et des communications et approuvé par le Réseau Technologies de l'information et des communications du Comité de haut niveau sur la gestion du Conseil des chefs de secrétariat pour la coordination, le groupe d'intérêt pour la sécurité informatique a mis au point un ensemble de contrôles techniques et de contrôles de procédure établissant des critères minimum de sécurité pour les sites Web publics. De plus, 52 règles et procédures sont actuellement mises au point pour améliorer la performance et la sécurité des systèmes et l'intégrité de la production. En coopération avec le Département de l'information, le document paraîtra sous forme d'instruction administrative en 2014, l'objectif étant de faire face aux problèmes de sécurité importants qui se posent pour les sites Web publics et aux nombreuses atteintes à la sécurité dont on sait qu'ils ont pâti dans le passé. En outre, le Bureau de l'informatique et des communications a réaffecté des ressources à la mise en place d'un mécanisme permettant de mieux veiller au respect des règles et procédures internes et des bonnes pratiques du secteur de la sécurité informatique. Il a aussi créé un groupe de travail pour la sécurité informatique, qui relève du Groupe de coordination de la gestion des questions relatives à l'informatique et aux communications, afin que les différents centres de conférences, y compris les bureaux extérieurs, les commissions régionales et les missions, communiquent davantage les uns avec les autres.

11. Outre les mesures prises dans le cadre du plan d'action, l'Organisation procède à l'échelle mondiale à d'importants changements de ses systèmes informatiques, afin de les mettre en conformité avec Umoja et d'autres systèmes annexes et d'aider la mise en service du progiciel de gestion. Elle met en place notamment un réseau longue portée mondial qui repose sur la commutation de labels multiprotocole, utilise un système d'accès standard (Citrix) pour tous les progiciels de gestion et procède à la migration des applications vers les pôles informatiques de Valence et de Brindisi. Ces changements permettront de mieux contrôler l'accès aux systèmes et de mieux gérer l'infrastructure informatique en la rendant moins vulnérable aux intrusions.

12. La sécurité informatique, qui est un élément capital pour la continuité des opérations et la reprise après sinistre, joue aussi un rôle important dans les missions, étant donné le contexte dans lequel elles fonctionnent. Le Département de l'appui aux missions a récemment établi un cadre général pour la sécurité informatique dont est chargé le Centre informatique des missions, qui regroupe les systèmes informatiques de la Base d'appui et de la Base de soutien logistique. Des évaluations de la sécurité des systèmes, infrastructures et autres moyens informatiques déployés sont régulièrement effectuées au Centre et dans les missions.

IV. Autres mesures à prendre

13. Suite à l'évaluation indépendante effectuée en 2013 et aux atteintes à la sécurité informatique constatées cette même année, il est apparu que les dispositifs de contrôle de la sécurité en place à l'ONU étaient insuffisants, tant pour les éléments classiques que pour les éléments plus récents de l'infrastructure informatique. Les systèmes d'administration des bâtiments, de contrôle d'accès, de téléphonie et de vidéoconférence et le matériel audiovisuel, qui n'étaient pas numériques autrefois, sont aujourd'hui exposés à des risques nouveaux, qui touchent les systèmes de communication numériques et les systèmes de communication par Internet. Il faudra procéder à de nouvelles évaluations précises pour faire en sorte que ces équipements soient pris en compte dans une stratégie complète de sécurité de l'information.

14. Une évaluation des systèmes utilisés dans le Département de l'appui aux missions a révélé qu'il fallait acquérir de nouveaux logiciels pour assurer la surveillance et le filtrage nécessaires pour lutter contre les intrusions, et mettre à niveau les pare-feux pour renforcer la sécurité de l'Organisation aussi bien dans les sites mentionnés plus haut que dans d'autres sites. De nouvelles mesures de sécurité ont été instituées et des travaux sont déjà en cours.

15. L'évaluation a également révélé que le risque pour la réputation de l'Organisation pourrait être revu à la hausse en raison de défaillances dans la gestion des contenus Web. En conséquence, l'Organisation a déterminé qu'il fallait surveiller de près les sites Web hébergés sur des serveurs extérieurs, passer en revue les dispositifs de sécurité et aider les départements du Secrétariat à revoir la conception de leurs sites pour les protéger contre les intrusions ou les dégradations.

16. La stratégie complète de sécurité de l'information, qui porte sur les systèmes de communication par Internet et les systèmes modernes et résout des problèmes systémiques, sera une composante essentielle de la stratégie informatique globale qui sera présentée à l'Assemblée générale, à sa soixante-neuvième session, pour qu'elle l'examine.

17. Dans l'intervalle, il faudra toutefois agir rapidement pour continuer de maîtriser les risques inacceptables auxquels est exposée l'Organisation, en s'inspirant des progrès déjà accomplis grâce aux mesures de renforcement de la sécurité de l'information mises en œuvre dans l'ensemble du Secrétariat.

18. Les systèmes informatiques du Secrétariat étant interdépendants et devant de plus en plus fonctionner en réseau, une attaque ou une intrusion, où qu'elle se produise, risque de mettre en péril l'ensemble des sites. Par conséquent, les mesures prises à ce jour pour exécuter le plan d'action devront aussi être mises en œuvre dans les autres lieux d'affectation et complétées par un sérieux renforcement des moyens de contrôle de l'Organisation.

19. Les mesures suivantes, pour lesquelles des ressources sont demandées dans le présent rapport, sont proposées en attendant la révision de la stratégie informatique[1] :

[1] Compte tenu du caractère sensible de ces mesures et afin de limiter les risques opérationnels, seule une description générale peut être fournie dans le présent rapport.

a) Mise en place du service de détection d'intrusions dans les bureaux hors Siège et les commissions régionales. Financé au moyen des ressources existantes du Bureau de l'informatique et des communications qui lui ont été réaffectées en 2013, ce service est actuellement limité aux centres informatiques principal et auxiliaire de New York et du New Jersey et aux pôles informatiques de la base d'appui et de la base de soutien logistique. Il faudra prévoir des ressources supplémentaires en 2014 pour continuer de le financer dans les sites où il est déjà en place et pour l'étendre aux lieux d'affectation à l'étranger;

b) Extension de la zone protégée par le pare-feu et mise à niveau de cette infrastructure, et mise en conformité des systèmes de filtrage de courrier électronique et de contenus Web à installer dans les bureaux hors Siège et les commissions régionales, le but étant de renforcer le dispositif de sécurité du réseau à l'échelle mondiale;

c) Renforcement des moyens de contrôle de la sécurité interne. L'Organisation a besoin de nouveaux outils et d'effectifs supplémentaires pour pouvoir mieux contrôler l'environnement informatique et le protéger contre d'éventuelles atteintes à la sécurité;

d) Déploiement d'un système de gestion des risques consistant pour l'Organisation à déceler les failles du système et à y remédier en priorité;

e) Nouvelle évaluation des dispositifs de protection et de détection équipant les éléments d'infrastructure modernes du Siège et l'environnement informatique des bureaux hors Siège, des commissions régionales et des pôles informatiques de Valence et Brindisi.

20. Il est évident qu'en raison du caractère fragmenté du réseau informatique de l'Organisation, il est difficile et coûteux de le sécuriser. La stratégie de l'Organisation a consisté à déménager promptement ses centres informatiques à Valence et à Brindisi afin de pouvoir mettre en œuvre des mesures de sécurité et de contrôle plus rapidement tout en améliorant l'efficacité des opérations et en réduisant les coûts. Par ailleurs, un des grands axes de la nouvelle stratégie informatique du Secrétaire général, que celui-ci présentera à l'Assemblée générale à sa soixante-neuvième session pour qu'elle l'examine, consistera à remédier à la fragmentation du réseau.

V. Modification du programme de travail demandé pour la période 2014-2015

21. Afin d'assurer la sécurité de l'information dans l'ensemble du Secrétariat, il faudra réviser le programme de travail du Bureau de l'informatique et des communications qui a été approuvé pour la période 2014-2015 (A/67/6/Rev.1, prog. 25), afin qu'il prenne en compte les activités liées à l'exécution du sous-programme 5 (Gestion et coordination stratégiques des technologies de l'information et des communications).

VI. Ressources supplémentaires demandées au titre du projet de budget-programme pour l'exercice biennal 2014-2015

22. Les demandes de crédits supplémentaires mentionnées dans le présent rapport résultent d'une évaluation indépendante menée en 2013 à la suite de la présentation du projet de budget-programme du Secrétaire général pour l'exercice biennal 2014-2015 [A/68/6 (Sect. 29E)], et s'expliquent par l'augmentation du nombre et de la fréquence des cyberattaques perpétrées contre l'ONU. Des crédits supplémentaires seront donc nécessaires pour financer la mise en œuvre des activités décrites plus haut.

23. Comme l'indique le tableau 1 ci-après, on estime à 3 440 700 dollars le montant total, avant actualisation des coûts, nécessaire au titre du chapitre 29E pour répondre, pendant une période de 12 mois, aux besoins les plus pressants de l'Organisation en matière de sécurité de l'information (décrits précisément dans le présent rapport), en attendant que l'Assemblée générale examine la stratégie révisée à sa soixante-neuvième session.

Tableau 1
Récapitulatif des ressources nécessaires, par objet de dépense
(En milliers de dollars des États-Unis)

Objet de dépense	*2014-2015 (montant prévu)*
Autres dépenses de personnel	581,4
Voyages	150,0
Services contractuels	1 325,0
Frais généraux de fonctionnement	59,3
Mobilier et matériel	1 325,0
Total	**3 440,7**

Tableau 2
Ressources nécessaires au titre du chapitre 29E du projet de budget-programme pour l'exercice biennal 2014-2015, avant actualisation des coûts
(En milliers de dollars des États-Unis)

Objet de dépense	*Montant prévu dans le rapport A/68/6(Sect.29E)*	*Ressources supplémentaires demandées*	*Montant total des ressources nécessaires*
Postes	36 168,6	–	36 168,6
Autres dépenses de personnel	5 634,0	581,4	6 215,4
Voyages	467,8	150,0	617,8
Services contractuels	12 697,0	1 325,0	14 022,0

Objet de dépense	*Montant prévu dans le rapport A/68/6(Sect.29E)*	*Ressources supplémentaires demandées*	*Montant total des ressources nécessaires*
Frais généraux de fonctionnement	16 574,5	59,3	16 633,8
Fournitures et accessoires	202,4	–	202,4
Mobilier et matériel	948,2	1 325,0	2 273,2
Total	**72 692,5**	**3 440,7**	**76 133,2**

Autres dépenses de personnel

24. Le montant prévu de 581 400 dollars permettra de couvrir les dépenses liées au personnel temporaire (autre que pour les réunions) qui sera chargé, pendant une période de 12 mois, de régler les problèmes de sécurité urgents, dans le cadre de la refonte et de l'application des mesures de sécurité du Bureau de l'informatique et des communications. Les emplois de temporaire demandés sont les suivants :

a) Un technicien spécialiste de la sécurité (P-4) chargé d'aider à mettre en œuvre le nouveau système de détection d'intrusions. L'Organisation devrait recevoir, au bas mot, entre 70 000 et 100 000 alertes par mois. En coopération avec un prestataire extérieur, le technicien chargé de la sécurité déterminera, en fonction de leur importance, quelles alertes nécessitent des mesures immédiates, et les traitera. Lorsque le système de détection d'intrusions sera mis en service dans les bureaux hors Siège et les commissions régionales, il collectera des informations au niveau mondial. Par conséquent, la coordination entre les alertes déclenchées dans les divers sites et les interventions auxquelles elles donnent lieu doit se faire au niveau mondial. Cette fonction de coordination mondiale sera essentielle lorsque le système de détection d'intrusions permettra de mieux connaître le réseau. Le technicien pourra également aider à l'analyse et à la gestion du nouveau pare-feu;

b) Deux temporaires (P-3) chargés d'exécuter de nouvelles fonctions : analyse des logiciels malveillants, création de modèles et coordination entre les alertes et les interventions auxquelles elles donnent lieu. Ce sont des activités essentielles pour déterminer le type d'attaques auxquelles est exposée l'Organisation, compte tenu des menaces continuelles et sérieuses que toutes sortes d'acteurs dans le monde font peser sur elle. Ces emplois donneront également à l'Organisation des moyens accrus pour contrôler les intrusions, évaluer la vulnérabilité des systèmes, établir des rapports et coordonner les contrôles de sécurité des applications Web. Par ailleurs, ces temporaires pourront travailler en liaison avec les équipes de développement de logiciels pour renforcer la sécurité des normes et des contrôles en vigueur dans les sites à l'échelle mondiale.

Voyages

25. Le montant prévu de 150 000 dollars permettra de financer, pour une période de deux semaines minimum, les voyages dans tous les bureaux hors Siège, les commissions régionales et les pôles informatiques de Valence et de Brindisi, de deux fonctionnaires chargés de :

a) Réaliser sans délai des évaluations indépendantes de la conformité de leurs systèmes aux normes de sécurité ainsi que des contrôles d'ordre technique, afin de s'assurer que les politiques et les instructions permanentes en vigueur sont

régulièrement appliquées. Ils évalueront les problèmes locaux et les risques liés à la sécurité de l'information qui n'ont encore jamais été recensés, les valideront et collecteront des informations à leur sujet. Cette mission permettra au personnel du Siège de contrôler la conformité des différents systèmes, ce qui est essentiel pour la mise en œuvre de la stratégie centralisée en matière de sécurité informatique, et de rendre compte à ce sujet;

b) Fournir des avis techniques sur la mise en œuvre de la politique de sécurité et une assistance en la matière et vérifier les nouveaux systèmes et applications prévus;

c) Organiser des réunions et des séances de formation sur le terrain avec tous les acteurs du monde des affaires et de la technologie afin de s'assurer que la conception et l'architecture des mesures préventives de sécurité de l'information sont bien comprises et mises en œuvre dans tous les lieux d'affectation.

26. Les ressources proposées au titre de cette catégorie serviront à financer des voyages lorsque la communication par Internet ou les téléconférences ne seront pas possibles en raison de la confidentialité des travaux. Dans la mesure du possible, on continuera d'organiser des missions qui se suivent sans interruption afin d'utiliser les ressources de manière plus rationnelle.

Services contractuels

27. Le montant prévu de 1 325 000 dollars permettra de financer :

a) Des services de détection d'intrusions (800 000 dollars) à déployer ou à entretenir, dans le cadre de la mise en œuvre du plan d'action. Ceux qui ont déjà été déployés à New York, Brindisi et Valence ont été financés par la réaffectation de ressources. Toutefois, pour assurer une couverture complète à l'échelle mondiale, il faudra mettre ces services en place dans tous les centres informatiques et les lieux d'affectation. Il est essentiel que l'Organisation ait les moyens de détecter des tentatives d'intrusion afin de pouvoir y réagir promptement;

b) Un système de gestion des risques (25 000 dollars) consistant à passer au crible de façon rigoureuse et régulière tous les biens informatiques de l'Organisation – serveurs et autres systèmes essentiels – pour vérifier qu'ils sont bien configurés et que les mises à jour de sécurité sont installées en temps voulu, afin de contribuer à l'administration de ces biens et de déceler leurs failles avant qu'ils ne fassent l'objet d'attaques extérieures;

c) Des services à la carte (500 000 dollars) dispensés par des experts de haut vol qui, selon les besoins, mèneront des activités essentielles à la mise en œuvre de la stratégie de sécurité de l'information du Secrétariat, notamment des nouveaux systèmes, et procéderont à de nouvelles évaluations des éléments d'infrastructure essentiels. Par ailleurs, des experts dotés de compétences pointues seront nécessaires pour résoudre en peu de temps des problèmes techniques précis et effectuer des recherches complémentaires d'ordre scientifique et légal permettant de comprendre au mieux comment remédier aux lacunes en matière de sécurité de l'information. Leurs travaux, dont l'objectif est de transmettre aux membres du personnel les connaissances ainsi acquises, seront limités dans le temps et très spécialisés.

Frais généraux de fonctionnement

28. Le montant prévu de 59 300 dollars permettra de financer la location de bureaux (47 700 dollars) et un accord de prestation de services (« A ») (6 300 dollars) pour trois emplois de temporaire affectés à New York; un réseau local (1 800 dollars); et des communications (3 500 dollars).

Mobilier et matériel

29. Le montant prévu de 1 325 000 dollars permettra de financer :

a) Des moyens de contrôle permanents (200 000 dollars). La collecte et l'analyse centralisées des journaux d'exploitation complètent l'information fournie par le système de détection d'intrusions et permet à l'Organisation de détecter des activités anormales ou suspectes qui ne sont pas jugées dangereuses. Outre de détecter les abus et les violations furtives du dispositif de sécurité, ce système permettra d'analyser les causes profondes des intrusions ainsi détectées et d'en déterminer l'ampleur. Le système de gestion des événements et des informations de sécurité qu'il est proposé d'acheter comprend du matériel spécialisé, des logiciels et des licences correspondant au volume d'informations collecté;

b) La modernisation du pare-feu (1 000 000 de dollars), notamment la mise à niveau des pare-feux existants (500 000 dollars) et du système de filtrage (500 000 dollars) à l'aide de dispositifs de protection de la dernière génération et de filtres intelligents qui permettront à l'Organisation de prévenir ou de détecter les tentatives d'attaque et d'intrusion censées échapper aux outils de détection classiques. Cette mise à niveau est essentielle pour s'adapter aux différentes formes que peuvent prendre les attaques perpétrées contre l'Organisation, qui ne cessent d'évoluer. Elle a déjà été effectuée au Siège et dans les pôles informatiques de Valence et de Brindisi, et financée au moyen des ressources existantes, réaffectées en 2013. Toutefois, cette modernisation devra être étendue à tous les centres informatiques et les lieux d'affectation;

c) Le contrôle de la sécurité des applications Web (125 000 dollars), notamment l'acquisition d'outils de contrôle pouvant être utilisés localement (achat de licences) ou à distance (logiciels fournis à la demande par des prestataires extérieurs). Ces outils peuvent être utilisés par le personnel interne chargé de la sécurité de l'information ou par des développeurs Web pour renforcer la sécurité du site Web de l'ONU.

VII. Décisions que l'Assemblée générale est appelée à prendre

30. L'Assemblée générale est priée :

a) De prendre acte du présent rapport;

b) D'approuver, au titre du chapitre 29E (Bureau de l'informatique et des communications) du projet de budget-programme pour l'exercice biennal 2014-2015, l'ouverture d'un crédit additionnel de 3 440 700 dollars pour mettre en œuvre d'urgence des mesures de renforcement de la sécurité informatique au Secrétariat, et d'imputer ce crédit au fonds de réserve.