

La norme ISO/CEI 17799 améliorée ouvre la voie à une nouvelle série sur les systèmes de gestion de la sécurité de l'information

par Ted Humphreys

La norme ISO/CEI 17799:2005, Technologies de l'information – Techniques de sécurité – Code de pratique pour la gestion de sécurité de l'information, récemment publiée, est une version révisée et améliorée de la norme qui est devenue le référentiel international dans ce domaine. Elle sera suivie cette année par la nouvelle ISO/CEI 27001, Systèmes de gestion de la sécurité de l'information – Exigences, destinée à la certification du système de gestion.

Tous les organismes disposent de biens qui sont essentiels pour leur pérennité. L'information, sous ses différentes formes, version imprimée, stockée électroniquement, affichée sur site Web ou communiquée par courrier électronique, représentée par films ou expliquée oralement, est un des biens les plus importants.

Pour la plupart des entreprises, la sécurité de l'information peut être essentielle pour se démarquer de la concurrence, conserver des liquidités, assurer la rentabilité, la conformité juridique et l'image commerciale. Mais pour de nombreuses entreprises, et pour la plupart des organismes à but non lucratif, les informations peuvent être le seul et unique bien. L'absence de sécurité de l'information peut menacer leur sécurité et donc leur existence même.

Une étude réalisée en 2002 sur les délits et la sécurité informatiques¹⁾ auprès de 503 praticiens

de la sécurité informatique aux États-Unis indique que les risques de délits informatiques et autres violations de la sécurité de l'information sont toujours aussi présents et que leur coût financier augmente.

En effet, 90 % des personnes interrogées ont détecté des failles dans la sécurité informatique durant les 12 mois couverts par l'enquête, 80 % ont reconnu avoir subi des pertes financières dues à ces incidents, ces per-



Ted Humphreys est Directeur de XiSEC, une entreprise spécialisée dans les systèmes de gestion de la sécurité de l'information. Il est Animateur de l'ISO/CEI JTC 1, Technologies de l'information, Sous-comité 27, Techniques de sécurité des TI, Groupe de travail 1, Exigences, services de sécurité et directives.

E-mail tedxisec@aol.com

Web www.xisec.com

Tél. + 44 1473 626615

tes s'élevant pour 46 % (223 réponses) à USD 455 848 000 au total²⁾ (chiffres extraits de l'article « Normes pour l'entreprise : la sécurité informatique – sécuriser les atouts de votre entreprise », *ISO Management Systems*, juillet-août 2003).

La norme ISO/CEI 17799:2005, *Technologies de l'information – Techniques de sécurité – Code de pratique pour la gestion de sécurité de l'information*³⁾, qui vient de paraître, intègre les tout derniers développements dans le domaine pour rester le code de bonne pratique international de référence.

La sécurité de l'information peut être essentielle pour se démarquer de la concurrence



Lignes directrices améliorées pour la protection

L'exploitation de ces vulnérabilités informatiques s'accroissant à un rythme alarmant, les travaux du Comité technique mixte ISO/CEI JTC 1, Technologies de l'information, Sous-comité 27, Techniques de sécurité des TI, Groupe de travail 1, Exigences, services de sécurité et directives, sont plus que jamais d'actualité.

Compte tenu du besoin critique, pour le monde économique, de protéger la confidentialité et l'intégrité de l'information, le groupe de travail ISO/CEI a développé une version améliorée de la norme commune ISO/CEI devenue, pour la communauté florissante du commerce électronique, le référentiel international en matière de gestion de sécurité de l'information.

À ce titre, elle n'est pas une norme destinée à la certification, n'a jamais été conçue dans cette optique et ne s'y prête pas. Sa publication sera suivie, au dernier trimestre de cette année

1) Cette enquête (Computer Crime and Security Survey) est réalisée par le Computer Security Institute avec la participation de la brigade Piratage informatique du San Francisco Federal Bureau of Investigations (FBI).

2) Ce chiffre se rapporte aux personnes interrogées qui souhaitaient et/ou pouvaient quantifier leurs pertes financières.

3) ISO/CEI 17799:2005, *Technologies de l'information – Techniques de sécurité – Code de pratique pour la sécurité de gestion de l'information*: disponible au prix de 200 francs suisses auprès des instituts nationaux membres de l'ISO (voir la liste complète avec les coordonnées sur le site Web de l'ISO : www.iso.org) et du Secrétariat central de l'ISO (sales@iso.org).

(publication attendue en novembre 2005), de la norme ISO/CEI 27001, *Technologies de l'information – Techniques de sécurité – Systèmes de gestion de sécurité de l'information – Exigences*, qui, elle, pourra être utilisée à des fins de certification.

Un langage international

Cette norme ISO/CEI 17799 révisée est la plus importante à ce jour pour la gestion de la sécurité de l'information. Elle établit, pour que toutes les entreprises du monde puissent s'engager dans des transactions commerciales, un langage international commun dans ce domaine.

Elle fournit aux entreprises de nombreux compléments et adjonctions reflétant l'état de la technique en ce qui concerne les meilleures pratiques de sécurité de l'information. Par exemple, meilleure gestion des dispositions de sécurité avec les entreprises extérieures, les sous-traitants et les prestataires de services, capacité de traitement renforcée des indicateurs, traitement des problèmes associés à la gestion des correctifs logiciels, aux dispositifs mobiles, aux technologies sans fil et aux codes mobiles nocifs par l'Internet, amélioration des meilleures pratiques de gestion des ressources humaines et plusieurs autres caractéristiques.

La nouvelle version traite de la sécurité de l'information au sens le plus large, établissant pour *tout* organisme produisant et utilisant des informations, sous *quelque* forme que ce soit, les meilleures pratiques, les lignes directrices et les principes généraux pour la mise en œuvre, la tenue à jour et la gestion de la sécurité des informations.



La nouvelle version établit les meilleures pratiques pour *tout* organisme

La norme ISO/CEI 17799:2005 identifie les mesures qui constituent le point de départ de la sécurité de l'information. Elle couvre les aspects suivants : facteurs cruciaux de réussite, organisation de la sécurité de l'information, gestion des biens, sécurité liée aux ressources humaines, sécurité physique et environnementale, gestion opérationnelle et gestion de la communication, acquisition des systèmes d'information, développement et maintenance, gestion des incidents, gestion de la continuité des activités et conformité. Elle est destinée à servir d'outil fondamental pour les entreprises de n'importe quel type et de n'importe quelle taille, tant dans le secteur public que dans le secteur privé.

Voici certains des éléments moteurs qui sous-tendent cette édition révisée du code de bonne pratique et font ressortir les caractéristiques nouvelles qui répondent aux exigences économiques les plus récentes.

Éléments moteurs des affaires et exigences

Plusieurs changements intervenus dans l'environnement économique et l'apparition de nouvelles manières de mener les affaires se sont avérés importants pour animer l'élaboration de la norme ISO/CEI 17799:2005 révisée. Nous avons admis :

- la dépendance croissante par rapport aux services tiers et à la gestion de la prestation de ces services ;
- les changements intervenus dans les risques et menaces pour les entreprises ;
- les technologies nouvelles et émergentes et une plus grande connectivité, avec leurs effets sur la protection de l'information, et
- les exigences croissantes de sécurité pour la conformité à la réglementation.

Services tiers

L'édition révisée introduit un certain nombre d'améliorations, de mises à jour et de dispositions supplémentaires concernant les meilleures pratiques.

Le monde économique dépend plus que jamais de services tiers pour la sous-traitance, la délocalisation, la mise en réseau

et l'hébergement Internet. De plus, il y a davantage de transactions avec des clients, partenaires commerciaux et chaînes logistiques qui utilisent divers dispositifs de travail en ligne et de mise en réseau.

Source d'une plus grande efficacité et d'un meilleur partage de l'information dans des marchés hautement concurrentiels, cette évolution facilite néanmoins l'accès aux systèmes organisationnels et accroît la vulnérabilité des informations sensibles et essentielles.

La norme ISO/CEI 17799:2005 étend les meilleures pratiques aux services tiers pour répondre aux exigences économiques d'aujourd'hui, et introduit aussi de nouvelles mesures de gestion de ces services visant à assurer la disponibilité et l'accessibilité des services tiers.

Ressources humaines

Un autre aspect de la révision se situe dans le domaine essentiel des personnels et de la sécurité de l'information. Aussi bonne que soit la technologie de la sécurité, les personnels sont susceptibles d'une exploitation et la sécurité s'en trouve ainsi compromise. La norme ISO/CEI 17799:2005 améliore les meilleures pratiques dans trois domaines clés :

1. Avant le recrutement

- le processus de recrutement ;
- références et sélection des salariés ; et
- contrats et conditions d'embauche.

2. Pendant la durée du contrat

- attribution des rôles et responsabilités ;
- octroi des droits d'accès et création de comptes utilisateurs ; et

ISO/CEI 17799: qu'en pensent les utilisateurs ?

Quelle est la valeur de la norme ISO/CEI 17799 pour les utilisateurs ? Qu'attendent-ils de la version révisée ?

Voici les réactions de certains organismes sur les avantages qu'ils ont retirés de l'application des meilleures pratiques données dans cette norme pour appuyer la bonne santé économique de leurs entreprises.

Microsoft: « Un ensemble d'outils inestimables »

« La norme ISO/CEI 17799, en particulier la version récemment révisée, est un ensemble d'outils inestimables pour les professionnels de la sécurité de l'information. Elle leur donne une approche universelle pour communiquer les meilleures pratiques de gestion dans ce domaine, une méthode pour assurer la cohérence des pratiques et un moyen d'établir et d'améliorer le fondement de la gestion de la sécurité de l'information dans leur environnement. »

Meng-Chow Kang,

CISSP, CISA et Conseiller principal pour la sécurité et la confidentialité, Région Asie-Pacifique, Microsoft.

Fujitsu: « Bien plus conviviale »

« La version 2000 de la norme ISO/CEI 17799 donnait à la direction d'entreprise un outil pour s'assurer que tous les domaines importants de la sécurité de l'information étaient inclus dans les programmes de contrôle de la sécurité, y compris des conseils sur les meilleures pratiques à adopter pour traiter des risques d'accès des tiers – fournisseurs, sous-traitants et prestataires de services. La nouvelle version 2005 simplifie considérablement la définition de normes internes, les exigences étant maintenant décrites de manière claire et cohérente pour chaque mesure adoptée. Nous prévoyons de commencer à l'utiliser dans notre travail SGSI dès que possible parce qu'elle est bien plus conviviale. »

John Snare, Fujitsu Australia.

PCCW: « en a bénéficié considérablement »

« En améliorant en permanence son approche stratégique et opérationnelle de la gestion cohérente de la sécurité de l'information, PCCW a bénéficié considérablement de l'approche structurée décrite dans la norme ISO/CEI 17799. Avec la publication de la nouvelle version, y compris les nouvelles mesures multiples, le renforcement des mesures existantes et la nouvelle structure simplifiée, la norme permettra à PCCW de s'améliorer immédiatement et d'être à la pointe de l'industrie en appliquant les meilleures pratiques de sécurité de l'information à la protection de ses ressources d'information. »

Dale Johnstone,

Gestion des risques en sécurité de l'information, PCCW Limited, Hong Kong.

– formation et sensibilisation, y compris par l'application de procédures et le rapport sur les incidents.

3. À la fin du contrat

– retrait des droits d'accès et des comptes utilisateurs, pour empêcher un accès ultérieur aux systèmes et processus de l'organisme ;

– retrait de l'accès aux locaux, par exemple annulation des laissez-passer ; et

– restitution de biens, par exemple informations, documents, supports de stockage, logiciels et ordinateurs portables.

• *Problèmes potentiels associés au code mobile* – répondre à la nécessité d'un contrôle du code logiciel mobile pour éviter les brèches dans la sécurité de l'information, y compris l'utilisation non autorisée ou l'interruption de systèmes, réseaux ou applications.

• *Utilisation généralisée des dispositifs mobiles et des réseaux sans fil* – il faut être conscient que les personnes qui participent aux réseaux sans fil peuvent avoir accès aux dispositifs mobiles, aux ordinateurs portables et à l'information de l'entreprise.



Menaces et vulnérabilités

La norme ISO/CEI 17799:2005 reconnaît un certain nombre de menaces et de vulnérabilités récemment apparues, notamment :

• *Gestion des correctifs logiciels* – en reconnaissance du risque croissant que de nouveaux logiciels soient exploités avant que l'on puisse installer des correctifs pour contrecarrer ce risque.

Aider les organismes dans le monde entier

La norme a pour but d'apporter aux organismes de par le monde des pratiques nouvelles et meilleures pour les aider à :

• créer une plus grande confiance chez les consommateurs en donnant l'assurance que leurs systèmes et services sont « aptes à l'emploi » ;

• faire un usage plus profitable de leurs investissements



dans la sécurité de l'information, outil habilitant pour les affaires ;

- améliorer le contrôle de gestion des ressources d'information des entreprises et la maîtrise des risques pour la sécurité de l'information ;
- améliorer les politiques de sécurité internes et les procédures, ainsi que les dispositions de sécurité avec les fournisseurs et les prestataires de services ;
- réaliser la conformité aux exigences de sécurité nationales et internationales applicables.

La norme ISO/CEI 27001 servira la **sécurité de l'information**, tout comme ISO 9001:2000 est au service de la **qualité**

Un complément et un soutien

La norme ISO/CEI 17799:2005 est un code de bonne pratique pour la gestion de la sécurité de l'information et n'est pas applicable à la certification du système de gestion. En revanche, la norme complémentaire et de soutien ISO/CEI 27001, *Systèmes de gestion de sécurité de l'information — Exigences*, est conçue à cette fin.

Sa publication est attendue en novembre 2005. Cette spécification est une version révisée de la norme BS 7799 Partie 2:2002, norme SGSI (Système de gestion de la sécurité de l'information) utilisée en certification ces sept dernières années. Toutes deux utilisent le modèle de processus P-D-C-A (Planifier – Faire – Vérifier – Agir), illustré dans les normes SMQ (Système de management de la qualité) ISO 9001:2000 et SME (Système de management environnemental) ISO 14001:2004, et sont fondées sur le même processus de certification.

Activités internationales de certification

Plus de 1 300 organismes dans plus de 50 pays ont déjà fait certifier leur SGSI. Ce chiffre augmente d'environ 80-100 par mois et la certification ISO/CEI 27001:2005 devrait s'accélérer grâce aux quelque 45 organismes de certification accrédités qui participent à ce processus.

Un registre en accès libre sur le site Web du groupe international des utilisateurs SGSI (www.xisec.com) donne des précisions sur les certificats à enregistrer et/ou à modifier/annuler. Ces informations sont régulièrement soumises par tous les organismes de certification accrédités.

La série ISO/CEI 27000

La norme ISO/CEI 17799:2005 et la future ISO/CEI 27001 font partie de la série de normes ISO/CEI 27000 du JTC 1/SC 27. Il existe une proposition d'attribuer le numéro ISO/CEI 27002 à ISO/CEI 17799 en 2007.

Actuellement, le SC 27 élabore les normes ISO/CEI 27003 et ISO/CEI 27004, qui ont pour but d'apporter des lignes directrices de soutien pour la norme ISO/CEI 27001.

La création d'une famille de normes relatives au SGSI est destinée à refléter l'approche adoptée par la série de normes SMQ ISO 9000:2000 – la norme ISO/CEI 27001 servira ainsi la sécurité de l'information, tout comme ISO 9001:2000 est au service de la qualité. •