Politiques en matière de sécurité des systèmes d'information ...
Dagorn, Nathalie
Systèmes d'Information et Management; Jun 2008; 13, 2; ABI/INFORM Complete
pg. 97

Politiques en matière de sécurité des systèmes d'information inter-organisationnels : une enquête dans dix grandes entreprises

Nathalie DAGORN

ICN Ecole de Management, Nancy
Laboratory of Algorithmics, Cryptology and Security (LACS), Luxembourg

RÉSUMÉ

Cet article synthétise les résultats d'une enquête par questionnaire centrée sur les pratiques et enjeux en matière de coopération et de sécurité des systèmes d'information, menée en octobre 2007 auprès de dix grands groupes français des secteurs d'activité de l'industrie, de la recherche, des banques et assurances. Il confirme notamment la tendance de coopération par l'intermédiaire du Web, ainsi que les récents efforts des organisations en management de la sécurité (protections techniques, politiques de sécurité conformes aux normes ISO du domaine, budget, etc.).

Mots-clés : Enquête, Système d'information, Coopération, Sécurité, Pratiques.

ABSTRACT

This article analyzes the results of a questionnaire survey, the aim of which was to study the practices employed, and the issues involved in the cooperation and security of information systems. This survey was conducted in October, 2007 with ten leading French companies of the sectors of industry, research, banking and insurance. It confirms the trend of Web cooperation, as well as the recent efforts of the organizations to manage their security (technical protections, security policies that conform to ISO standards in the field, budget, etc.).

Key-words: Survey, Information system, Cooperation, Security, Practices.

Remerciements : Sans les nommer, nous tenons à remercier vivement toutes les organisations ayant contribué à notre enquête de sécurité (et plus particulièrement leurs DSI, qui se reconnaîtront à la lecture de cet article) ; chacun de leurs témoignages nous a apporté des informations d'autant plus précieuses que le cadre de recherche exploré était hautement confidentiel, abordant un sujet encore « tabou » pour la plupart des organisations aujourd'hui.

Reproduced with permission of the copyright owner. Further reproduction prohibited without permission.

INTRODUCTION

Des enquêtes et statistiques pouvant être trouvées à l'heure actuelle dans la littérature traditionnelle et électronique sur la sécurité des systèmes d'information, deux problèmes majeurs se dégagent : d'une part, les chiffres avancés peuvent provenir de sources douteuses ou d'enquêtes pas assez rigoureusement menées, générant des résultats parfois contradictoires ; d'autre part, les enquêtes recensées peuvent ne pas concerner notre zone géographique, ne pas porter sur les points souhaités, ou tout simplement être obsolètes (vu l'évolution rapide des technologies de l'information, particulièrement en matière de sécurité).

Dans le cadre d'un projet d'étude sur les pratiques et enjeux de la sécurité des systèmes d'information en France, nous avons entrepris d'interroger directement les Directions des Systèmes d'Information (DSI) de dix grands groupes français ; nous nous sommes intéressés en particulier à deux sujets d'actualité, qui sont (i) la *coopération* des systèmes d'information de l'organisation avec d'éventuelles organisations partenaires, et (ii) la *sécurité* des systèmes d'information (inter-organisationnels) déployés.

Cet article est structuré de la manière suivante : la section 1 présente le cadre de l'étude, renseignant sur le contexte de la consultation, l'échantillon des organisations consultées et la mise en œuvre de l'étude. Puis les résultats de l'enquête sont dévoilés dans la section 2, en mettant successivement l'accent sur les pratiques et enjeux en matière de coopération et de sécurité des systèmes d'information des organisations consultées. Enfin, la section 3 analyse et discute les résultats obtenus, avant de conclure dans la section 4.

1. CADRE DE L'ÉTUDE

1.1. Contexte de la consultation et échantillon d'organisations consultées

Cette étude a été menée dans le cadre d'un projet de recherche au sein de Nancy-Université (France). Elle s'appuie sur un questionnaire d'enquête (fourni en Annexe) diffusé en octobre 2007 à cent quatorze grandes entreprises françaises (d'après une liste fournie par le CIGREF[1]). Seules douze organisations ont répondu à notre sollicitation, la sécurité des systèmes d'information étant généralement perçue comme un sujet extrêmement sensible sur lequel les organisations refusent de communiquer. Parmi ces douze organisations intéressées par la question de la sécurité, dix d'entre elles ont finalement été retenues selon trois critères essentiels : leur position favorable vis-à-vis de notre enquête (*i.e.*, leur accord explicite quant à leur contribution sur la totalité du questionnaire), leur crédibilité en tant qu'acteur important de leur secteur d'activité, et enfin l'hétérogénéité apparente de leur environnement de travail (hétérogénéité culturelle, hétérogénéité des outils, etc.) pressentie comme un facteur représentatif de l'évolution de nombreuses organisations.

[1] Club Informatique des GRandes Entreprises Françaises, http://cigref.typepad.fr .

Reproduced with permission of the copyright owner. Further reproduction prohibited without permission.

1.2. Mise en œuvre de l'étude

L'étude a débuté par une revue de la littérature française et anglo-saxonne récente en matière de sécurité des systèmes d'information inter-organisationnels[2]. Cette étude exploratoire était notamment destinée à sonder les politiques de sécurité mises en œuvre dans les grandes organisations, et en particulier celles s'appliquant aux systèmes d'information inter-organisationnels. Quelques modèles mathématiques formels à la base des politiques de sécurité actuelles ont ensuite été étudiés, tels que le modèle de contrôle d'accès discrétionnaire DAC (*Discretionary Access Control*) formulé par Lampson (1971), le modèle de contrôle d'accès obligatoire MAC (*Mandatory Access Control*) présenté par LaPadula et Bell (1973) et sa variante (Biba, 1975), le modèle de contrôle de flux d'information (Denning, 1976), le modèle de non-interférence (Goguen et Meseguer, 1982), le modèle à base de logique modale (Bieber et Cuppens, 1992), le modèle de contrôle d'accès à base de rôles RBAC (*Role-Based Access Control*) proposé par Sandhu *et al.* (1996), le modèle de contrôle d'accès à base de tâches TBAC (*Task-Based Access Control*) formulé par Thomas et Sandhu (1997) et sa variante à base d'équipes TMAC (*TeaM-Based Access Control*) proposée par Thomas (1997), ou plus récemment le modèle de contrôle d'accès basé sur l'organisation Or-BAC (*Organisation-Based Access Control*) présenté par El Kalam *et al.* (2003). Puis le questionnaire d'enquête a été rédigé et envoyé en date du 17 octobre 2007 aux DSI des organisations ciblées. Le délai de réponse, initialement fixé au 30 octobre 2007, a été prolongé jusqu'au 7 novembre 2007 pour permettre à une organisation de répondre tardivement. Nous avons précautionneusement suivi les organisations répondantes dans leur compréhension du questionnaire afin que les réponses fournies soient pertinentes et exploitables. Durant le traitement des résultats, peu de corrections ont été nécessaires sur les retours obtenus. Conscients de la confidentialité et de la criticité des informations de sécurité confiées par ces organisations, nous nous sommes engagés à protéger ces informations pour préserver leur intégrité durant leur traitement et empêcher qu'elles soient communiquées à des tiers sans l'autorisation de l'organisation. Nous nous sommes également engagés à n'exploiter les résultats du questionnaire que dans le cadre d'une enquête générale de manière anonyme, sans jamais divulguer ceux-ci individuellement et/ou nominativement.

2. PRÉSENTATION DES RÉSULTATS

L'enquête soumise comporte quatre parties : la première a pour but de collecter quelques données générales sur les organisations interrogées, la seconde évalue leurs pratiques en matière d'ouverture et de coopération éventuelle avec d'autres organisations partenaires, la troisième évalue leurs pra-

[2] La littérature est encore peu abondante sur ce sujet spécifique : notre revue de littérature est basée sur 39 articles académiques de la base de données Business Source Premier (économie et gestion), 8 ouvrages et 5 enquêtes de sécurité.

Reproduced with permission of the copyright owner. Further reproduction prohibited without permission.

tiques en matière de sécurité des systèmes d'information, et enfin la quatrième a pour but de recueillir l'opinion des organisations interrogées sur le questionnaire soumis (les résultats de cette partie seront présentés dans la section suivante). Les résultats des trois premières parties de l'enquête sont détaillés dans cette section.

2.1. Données générales sur les organisations interrogées

En termes de **taille de l'organisation (effectif)**, nous avons interrogé une organisation de 500 à 999 salariés, une organisation de 1 000 à 4 999 salariés, et huit organisations de 5 000 salariés et plus. Elles font toutes partie d'un groupe de 5 000 salariés et plus.

Six organisations appartiennent au **secteur d'activité** de l'industrie, deux au secteur bancaire, une au secteur des assurances et une au secteur de la recherche.

2.2. Pratiques et enjeux en matière de coopération des systèmes d'information

2.2.1. Données générales sur la coopération

La totalité des organisations interrogées **coopère de manière habituelle** avec un (ou plusieurs) partenaires : toutes coopèrent en effet avec un (ou plusieurs) fournisseur(s), neuf d'entre elles coopèrent avec une (ou plusieurs) filiale(s) du groupe, huit avec un (ou plusieurs) client(s), et cinq avec d'autres partenaires tels que des partenaires scientifiques ou d'externalisation, des organismes de recherche ou gouvernementaux, ou encore des cabinets de notation boursière.

Considérant le fait que plusieurs systèmes d'information inter-organisationnels peuvent être utilisés par les organisations interrogées, la **fréquence** de coopération est pluri-journalière pour neuf d'entre elles, journalière pour trois, hebdomadaire pour deux, mensuelle pour deux, et trimestrielle ou inférieure pour deux d'entre elles.

Les **systèmes d'information inter-organisationnels** utilisés par ces organisations pour coopérer avec leurs partenaires sont les suivants (de manière non exclusive et par ordre décroissant d'utilisation) : toutes utilisent une application Web, neuf utilisent un site Web, huit utilisent une application propriétaire, huit utilisent un extranet, sept utilisent des marchés en ligne (place de marché électronique, plateforme d'achat et d'approvisionnement, portail spécialisé), sept utilisent un système EDI (*Electronic Data Interchange*), cinq utilisent un progiciel de gestion intégré (ERP pour *Enterprise Resource Planning*) tel que SAP R/3 par exemple, cinq utilisent des services Web intégratifs basés sur XML, trois utilisent un collecticiel (*groupeware*), trois utilisent un système EAI (*Enterprise Applications Integration*), trois utilisent un système XML purement documentaire, deux utilisent un système de *workflow* intégratif (SGWf pour système de gestion de *workflow*), une organisation utilise un système de *workflow* purement documentaire, et une organisation utilise une grille informatique (*grid computing*).

Reproduced with permission of the copyright owner. Further reproduction prohibited without permission.

2.2.2. Les risques liés à la coopération

Les principaux **risques organisationnels** identifiés par les organisations interrogées sont, pour neuf d'entre elles, des risques de sécurité (réseau, Web) ; cinq identifient des risques de *lock-in* (dépendance extrême du partenaire), trois des risques de conflit avec le partenaire, et trois d'autres risques organisationnels tels que la maîtrise des flux et leur disponibilité, la mesure de la qualité de service, les risques juridiques, commerciaux, financiers ou sociaux liés à la coopération.

Les principaux **risques institutionnels** (*i.e.*, spécifiques au contexte inter-organisationnel) engendrés exclusivement par la coopération sont, pour huit organisations, l'intrusion dans leur périmètre physique (par exemple, l'intrusion physique d'un salarié d'une organisation partenaire) ; sept organisations craignent l'intrusion dans leur périmètre logique (par exemple, la propagation d'un ver ou d'une attaque par le réseau de coopération), et deux organisations redoutent d'autres risques institutionnels tels que l'éventuel comportement délictueux d'une organisation partenaire relativement à la législation en vigueur (loi Sarbanes-Oxley dite SOX, loi de sécurité financière dite LSF, lois françaises et européennes, etc.), la perte accidentelle ou frauduleuse (hors intrusion) de disponibilité, d'intégrité ou de confidentialité.

2.2.3. Les flux d'information liés à la coopération

Les **types d'informations** échangés lors de la coopération sont les suivants : huit organisations coopèrent par l'échange de messages électroniques (*mail*), de messages EDI ou XML, ou génèrent du trafic réseau ; six organisations échangent des documents papier, et une organisation échange d'autres types d'informations (tels que des tickets d'incidents sur le système d'information inter-organisationnel, par exemple).

Pour neuf organisations, les **informations sensibles** à protéger lors de la coopération sont les informations commerciales ; huit évoquent les informations ne présentant pas un caractère secret mais qui restent soumises à l'obligation de réserve ou de discrétion professionnelle, sept signalent les informations nominatives (fichiers des clients, des fournisseurs, etc.), cinq soulignent les informations relevant de la vie privée (dossiers du personnel, données de santé, etc.), cinq évoquent également les informations constitutives du patrimoine scientifique, industriel ou technologique de l'organisation, et deux ajoutent d'autres informations telles que les informations financières avant publication, les informations stratégiques du groupe (sur les fusions/acquisitions, par exemple), ou encore les informations relatives au patrimoine intellectuel et au savoir-faire des partenaires de la coopération.

Concernant la **direction** de ces flux d'information (*i.e.*, l'échange de qui vers qui ?), la totalité des organisations sont « maîtres », c'est-à-dire qu'une (ou plusieurs) organisation(s) partenaire(s) accède(nt) aux informations de l'organisation, huit sont « esclaves », signifiant que l'organisation accède aux informations d'une (ou plusieurs) organisation(s) partenaire(s), ces rôles n'étant

Reproduced with permission of the copyright owner. Further reproduction prohibited without permission.

pas exclusifs l'un de l'autre. Cinq organisations synchronisent leurs informations avec leur(s) partenaire(s), c'est-à-dire les répliquent de part et d'autre ; quatre accèdent à un système d'information commun partagé situé hors des organisations coopératives, et l'une d'elles mutualise ses informations sur une grille informatique.

Les **permissions** des utilisateurs de l'organisation sur ces flux d'information sont pour huit d'entre elles la consultation et la modification (lecture et écriture/suppression des données), pour quatre d'entre elles la consultation seule (lecture des données), et pour deux d'entre elles la modification seule (écriture/suppression des données).

Pour ce faire, les différents **rôles** incarnés au sein de l'organisation par les utilisateurs du système d'information inter-organisationnel sont les suivants : dans neuf organisations, l'utilisateur est « simple » utilisateur (sans privilèges), dans huit organisations il est utilisateur avec des privilèges spécifiques, et dans sept organisations il est administrateur (tous privilèges autorisés).

2.3. Pratiques et enjeux en matière de sécurité des systèmes d'information

2.3.1. Les risques liés à la sécurité

Pour la totalité des organisations interrogées, les principales **menaces de sécurité** auxquelles elles sont confrontées (incluant le contexte inter-organisationnel) sont les menaces physiques (par exemple, un accès physique non autorisé, la compromission matérielle du système d'information ou du réseau de communication), neuf d'entre elles craignent les menaces logicielles (par exemple, *scanning*, intrusion, altération et/ou destruction de données, saturation d'une ressource du système d'information, *malware*, etc.) ; huit organisations redoutent les menaces humaines (ingénierie sociale en particulier), huit organisations également redoutent les menaces institutionnelles (décrites plus avant), sept évoquent les menaces électroniques (par exemple, la vulnérabilité des moyens de communication sans fil, le brouillage ou la saturation des communications, l'atteinte à l'intégrité des communications par injection de données malveillantes, l'atteinte à la confidentialité par écoute des émissions radioélectriques du réseau, etc.), et trois d'entre elles signalent d'autres menaces telles que l'atteinte à l'image de l'organisation (diffamation), les recours légaux (contrats, législation sociale, réglementations), les fraudes internes, les actes de sabotage, la réduction du niveau de sécurité par méconnaissance des risques, ou encore les mesures de sécurité inadaptées ou inefficaces donnant un faux sentiment de sécurité.

Aussi les **critères de sécurité** les plus importants (incluant le contexte inter-organisationnel) sont-ils la disponibilité des données et services du système d'information inter-organisationnel pour huit des organisations interrogées ; sept d'entre elles mettent en avant l'intégrité des données, six privilégient l'authentification/identification de l'utilisateur partenaire, six organisations également évoquent la non-répudiation des transactions, cinq soulignent l'importance de la confidentialité des données, et l'une d'elles ajoute le critère de la traçabilité.

Reproduced with permission of the copyright owner. Further reproduction prohibited without permission.

Pour neuf organisations, les principaux **enjeux** liés à la sécurité (en termes de conséquences en cas de compromission de la sécurité, incluant le contexte inter-organisationnel) sont la perte de crédibilité ou de confiance ; huit organisations craignent la perte de marché ou la perte d'argent, quatre redoutent le recours juridique (tribunaux, etc.), trois soulignent la perte de temps, et une organisation ajoute d'autres enjeux tels que la perte d'image.

2.3.2. Les modèles et politiques de sécurité

Une organisation interrogée n'a pas répondu à cette question. Trois des organisations y ayant répondu n'appliquent aucun **modèle de sécurité**, trois organisations appliquent la norme ISO/IEC 27001[4] et plus généralement la série 27000, une organisation applique la norme ISO/IEC 17799[5] accompagnée de méthodes telles que COBIT[6], COSO[7], EBIOS ou FEROS[8] ; une organisation applique un modèle de maturité du système d'information[9], et la dernière applique le modèle de contrôle d'accès RBAC[10].

Nous avons également voulu savoir si une (ou plusieurs) **politique(s) de sécurité** était(en)t appliquée(s) dans les organisations interrogées : huit d'entre elles nous ont répondu appliquer une politique de sécurité centralisée (*i.e.*, existence d'une unique politique de sécurité prenant en compte l'ensemble des entités de l'organisation, avec utilisation d'un moniteur de référence regroupant les mécanismes de protection permettant de garantir le contrôle d'accès et de flux définis par les règles de la politique de sécurité), et cinq d'entre elles une politique de sécurité distribuée (*i.e.*, coexistence de plusieurs politiques de sécurité éventuellement incohérentes, chacune pouvant être définie par un administrateur de sécurité différent).

---

[4] La norme ISO/IEC 27001:2005 décrit comment mettre en place un Système de Management de la Sécurité de l'Information (SMSI). Elle est en vente à l'adresse http://www.iso.org/iso/fr/iso_catalogue/catalogue_tc/catalogue_detail.htm?csnumber=42103.

[5] La norme ISO/IEC 17799 (créée en 2000, modifiée en 2005 et renommée ISO/IEC 27002) est une norme internationale concernant la sécurité de l'information, comprenant un ensemble de bonnes pratiques relatives à la mise en place ou au maintien d'un SMSI. Elle est en vente à l'adresse http://www.iso.org/iso/fr/iso_catalogue/catalogue_tc/catalogue_detail.htm?csnumber=50297.

[6] Le référentiel COBIT (*Control OBjectives for Information & related Technology*) est une méthode d'audit et de gouvernance des systèmes d'information développée par l'ISACA (*Information Systems Audit and Control Association*) en 1996. La version 4.1 est téléchargeable sur le site de l'ISACA http://www.isaca.org/.

[7] Le référentiel COSO, développé par le *Committee Of Sponsoring Organizations of the treadway commission*, est utilisé notamment pour le contrôle interne de la mise en place de dispositions relevant des lois SOX ou LSF. COSO 1 « Internal Control – Integrated Framework » date de 1992, COSO 2 « Enterprise Risk Management Framework » de 2002 (http://www.coso.org/).

[8] La méthode EBIOS (Expression des Besoins et Identification des Objectifs de Sécurité), publiée par la Direction Centrale de la Sécurité des Systèmes d'Information (DCSSI) en 1997, permet d'identifier les besoins de sécurité d'un système d'information. Une documentation récente est présentée à l'adresse http://www.ssi.gouv.fr/fr/confiance/ebiospresentation.html; la Fiche d'Expression Rationnelle des Objectifs de Sécurité (FEROS) permet de formaliser ces besoins (http://www.ssi.gouv.fr/fr/documentation/150/).

[9] Tel que le CMM (*Capability Maturity Model*) élaboré par le Software Engineering Institute (Humphrey, 1987).

[10] *Op. cit.*, p. 3.

Reproduced with permission of the copyright owner. Further reproduction prohibited without permission.

Concernant la **gestion des accès** au système d'information, cinq organisations appliquent une politique de contrôle d'accès discrétionnaire, cinq autres appliquent une politique de contrôle d'accès obligatoire, et deux d'entre elles appliquent d'autres politiques de contrôle d'accès très opérationnelles, par exemple dédiées à la messagerie, à l'Internet, au *business*, au développement d'applications, à la classification des informations, à la lutte antivirus, à la conformité ou aux contrôles.

Si des **politiques de sécurité multiples** coexistent dans l'organisation, celles-ci sont fédérées pour quatre organisations (*i.e.*, des interactions existent : leurs règles sont composées), et cohabitent dans deux organisations (*i.e.*, aucune interaction n'existe : aucun sujet de l'une n'accède aux objets de l'autre, le système résultant pouvant être assimilé à deux systèmes indépendants).

En cas de **fédération** de plusieurs politiques de sécurité, le **mode de composition** utilisé dans quatre organisations est la combinaison des politiques (*i.e.*, les politiques initiales peuvent être incohérentes, la politique résultante pouvant ne pas préserver les conditions de sécurité associées à chaque politique initiale ; cette approche est habituellement mise en œuvre en cas de confiance mutuelle entre les différents administrateurs de sécurité pouvant résulter d'une entente préalable). Deux organisations pratiquent l'interopération des politiques (*i.e.*, si les politiques initiales sont cohérentes, la politique résultante préserve les conditions de sécurité associées à chaque politique initiale ; cette approche est habituellement mise en œuvre en cas de suspicion mutuelle ou de confiance faible entre les différents administrateurs de sécurité).

2.3.3. Les mesures de sécurité

Les **textes de sécurité** existants dans les organisations interrogées sont les suivants : toutes les organisations ont élaboré des chartes (par exemple, charte sur l'utilisation de la messagerie intranet, charte sur l'utilisation des services Internet ou d'un périmètre plus large, charte informatique, etc.) ; sept organisations consacrent à la sécurité un paragraphe spécifique dans le contrat de sous-traitance ou de partenariat, six organisations y dédient un paragraphe spécifique dans le règlement intérieur, cinq font valoir d'autres textes de sécurité sous forme écrite (par exemple, politique générale et/ou politiques techniques de sécurité, référentiels de sécurité, normes et règles de sécurité, standards associés, circulaires, etc.), et deux organisations consacrent un paragraphe spécifique à la sécurité dans le contrat de contrat de travail des salariés concernés.

Pour toutes les organisations consultées, les **règles de sécurité** en vigueur **à l'usage de la DSI** comprennent :

- la gestion des mots de passe, imposant certaines contraintes (telles que la durée de validité maximum, le nombre de caractères minimum, le nombre maximum d'essais de connexion infructueux avant révocation du compte, les principes de ré-

Reproduced with permission of the copyright owner. Further reproduction prohibited without permission.

initialisation du compte en cas de perte du mot de passe par l'utilisateur, etc.) ;

- le filtrage du pare-feu, détaillant l'ACL (*Access Control List*, liste définissant les ressources disponibles du réseau et les utilisateurs autorisés à y accéder : adresses, ports, protocoles autorisés et interdits) ; les infrastructures complexes peuvent nécessiter l'installation de plusieurs pare-feu, chacun pouvant être paramétré avec des ACL différentes ;
- la définition des VLAN (*Virtual Local Area Network*, sous-réseaux virtuels du réseau interne permettant d'isoler certaines machines) avec pour chacun d'eux sa finalité, son plan d'adressage et les flux éventuellement filtrés vers les VLAN voisins ;
- la sauvegarde des données (fréquence des sauvegardes, leur type – sauvegarde incrémentale ou totale –, temps de rétention des données, principes d'externalisation des supports magnétiques, etc.).

Neuf organisations appliquent des règles pour les produits antivirus retenus (références, principe de mise à jour, positionnement – serveur de messagerie, postes de travail –) ; huit organisations mettent en œuvre des règles d'identification de l'utilisateur en fonction de son statut, de son entité fonctionnelle, de son établissement ou de sa mission. Sept organisations appliquent des règles pour les produits de chiffrement retenus (références, périmètre d'application, environnement de fonctionnement) ou pour la configuration d'un poste de travail dédié au personnel extérieur (par exemple, bridage physique par cadenas ou verrou, suppression de certains services du système, protection du BIOS – *Basic Input Output System*, premier programme à s'exécuter lors de l'allumage d'un ordinateur –, auto-*logon*, etc.). Enfin, trois organisations appliquent d'autres règles de sécurité telles que le passage de tout projet devant un comité technique/de sécurité, le respect de directives éventuellement imposées par les normes appliquées (ISO 27001/17799), des règles sur la protection des données sensibles (santé, etc.), des clauses de sécurité contractuelles ou légales, ou encore des règles sur les transferts de fichiers.

Les **règles de sécurité** applicables **à l'usage des utilisateurs** sont, pour neuf organisations, des conseils sur le choix des mots de passe, pour huit d'entre elles des règles de protection des PC portables (par exemple, chiffrement obligatoire des données ou stockage sur un support externe, banalisation du contenu de la sacoche, arrimage du PC portable par un câble ou dépôt dans une armoire dès le retour de l'utilisateur dans l'organisation, etc.), et pour quatre d'entre elles d'autres règles dérivées de la politique locale de sécurité de l'organisation, ou dédiées à la sensibilisation et à la réglementation des comportements des utilisateurs (sur Internet, accès distant, Wi-fi, messagerie, ingénierie sociale, analyse des risques, etc.).

De la même manière, concernant les **procédures de sécurité** existantes **à l'usage de la DSI**, toutes les organisations interrogées ont mis en place une procédure d'installation et de paramétrage du produit antivirus sur le serveur de messagerie, neuf organisations appliquent une procédure d'installation et de paramétrage du produit antispam

Reproduced with permission of the copyright owner. Further reproduction prohibited without permission.

sur le serveur de messagerie, et quatre appliquent d'autres procédures relatives au management de la sécurité, au Wi-fi, au filtrage réseau, aux pare-feu applicatifs sur postes, à la gestion des adresses IP (*Internet Protocol*, protocole standard d'échange de paquets de données sur Internet), à l'analyse de trafic, de contenu et de capacité, à la gestion des accès logistiques, à la constitution d'une cellule de crise en cas d'incident de sécurité, à la gestion d'une infection virale, ou encore au plan de continuité de l'activité (BCP pour *Business Continuity Plan*).

Les **procédures de sécurité** applicables **à l'usage des utilisateurs** comprennent, dans sept organisations, un guide d'utilisation d'un dispositif d'authentification forte (tel que calculette, carte à puce, *token* USB – clef USB à puce qui contient le certificat du poste du signataire –) ; six organisations mettent à disposition de l'utilisateur un guide d'utilisation du produit de chiffrement (détaillant ses fonctionnalités, son périmètre d'application et ses instructions d'utilisation), et cinq fournissent un guide d'utilisation du programme antivirus (détaillant ses fonctionnalités et ses instructions d'utilisation) ; deux organisations mettent en œuvre d'autres procédures de sécurité, telles que des manuels d'utilisation divers ou un guide pour la connexion sur l'intranet depuis l'Internet, par exemple.

En matière de **solutions techniques de sécurité**, les organisations interrogées disposent toutes d'un pare-feu, d'un proxy (unique machine d'un réseau local connectée à l'Internet et effectuant les requêtes pour les autres ordinateurs du réseau), d'une zone démilitarisée (DMZ pour *DeMilitarized Zone*, segment du réseau où les règles de sécurité sont moins strictes pour permettre la connexion à des réseaux externes à l'organisation, tels que l'Internet), d'une solution antivirus, d'une solution antispam, et déploient pour leurs communications un réseau privé virtuel (VPN pour *Virtual Private Network*, réseau privé construit au sein d'un réseau public tel qu'Internet). Six d'entre elles utilisent un système de détection ou de prévention d'intrusion (IDS pour *Intrusion Detection System* ou IPS pour *Intrusion Prevention System*), quatre d'entre elles utilisent une solution d'authentification unique (SSO pour *Single Sign-On*), et deux mettent en œuvre d'autres solutions techniques de sécurité telles que pare-feu applicatif (sur poste), anti-espiogiciels (ou *antispyware*), synchronisation des mots de passe.

De la même manière, au niveau des **méthodes de sécurité**, huit organisations procèdent au contrôle d'URL (*Uniform Resource Locator*, adresse Internet exploitée par les navigateurs), au contrôle des messageries, ou mettent en œuvre une authentification forte ; sept organisations utilisent le chiffrement (cryptographie), et quatre la détection ou prévention d'intrusion distribuée (DIDS pour *Distributed Intrusion Detection System* ou DIPS pour *Distributed Intrusion Prevention System*). Trois organisations implémentent d'autres méthodes de sécurité telles que des contrôles sur les accréditations ou sur les solutions antivirus, utilisent un Système de Management de la Sécurité de l'Information (SMSI) ou des méthodes de sécurité telles que précédemment évoquées (EBIOS ou FEROS pour l'ana-

Reproduced with permission of the copyright owner. Further reproduction prohibited without permission.

lyse des risques, COSO ou COBIT pour le contrôle interne de la sécurité). Une organisation pratique la biométrie (ensemble des techniques permettant l'identification d'une personne sur la base de caractères physiologiques ou de traits comportementaux), et une autre la stéganographie (branche particulière de la cryptographie qui consiste à camoufler un message dans un conteneur – souvent une image – de manière à masquer sa présence).

2.3.4. La surveillance du système d'information et le pilotage de la sécurité

Nous avons voulu savoir également si les organisations interrogées effectuaient (ou non) des **audits ponctuels** (contrôles) **de sécurité**, notamment pour vérifier si leur politique de sécurité était correctement appliquée. Selon les résultats obtenus, la moitié des organisations analyse régulièrement l'association compte/propriétaire pour détecter d'éventuelles utilisations de comptes par des personnes non autorisées, ou inspecte physiquement l'état général de la salle des serveurs (par exemple, les cartons vides et les *listings* inutiles doivent être dégagés car ce sont des éléments majeurs de propagation d'incendie). Quatre organisations vérifient auprès de l'administrateur réseau la non-utilisation de commandes dangereuses (telles que telnet[10]) et l'absence de mots de passe triviaux ; quatre organisations également pratiquent d'autres audits relatifs aux modèles, politiques et référentiels de sécurité utilisés (par exemple, management de la sécurité, Windows[11], référentiel de sûreté de l'information, revues ISO, COBIT, audits internes et externes ciblés) ; trois organisations vérifient auprès d'une population choisie la bonne utilisation des logiciels de chiffrement mis à disposition et l'absence de données « en clair » (*i.e.*, non chiffrées) sur les PC portables, ou contrôlent la bonne application des règles et procédures existantes (par exemple, dépôt des disques amovibles dans un coffre, fermeture des bureaux en cas d'absence, etc.). Une organisation n'a pas répondu à cette question.

Pour réaliser ces audits, huit des organisations répondantes utilisent un **scanner de vulnérabilités** (VDS pour *Vulnerability Detection System*).

Toutes les organisations interrogées affirment pratiquer des **tests d'intrusion**.

En matière de surveillance du système d'information, toutes les organisations répondantes pratiquent un **examen des fichiers de journalisation (*logs*)** : six d'entre elles ont configuré leur logiciel antivirus pour recevoir automatiquement un *mail* d'alerte en cas de détection de virus sur le réseau interne, quatre filtrent les événements générés par les commutateurs pour faire ressortir les tentatives de connexion de postes de travail d'adresse MAC (numéro d'identification unique d'une carte réseau Ethernet) inconnue, trois filtrent les *logs* de connexion de manière à

[10] Ou ftp, par exemple. Ces commandes sont dangereuses car elles font passer les informations demandées « en clair » (*i.e.*, de manière non chiffrée) sur le réseau, les exposant à d'éventuelles interceptions (*sniffer*, etc.).

[11] Une fonction d'audit peut être activée au niveau du serveur ou du PC à surveiller.

Reproduced with permission of the copyright owner. Further reproduction prohibited without permission.

faire ressortir les révocations de comptes de session (si un nombre d'essais de connexion maximum a été défini), trois mettent en œuvre d'autres types d'examens de surveillance tels que la centralisation des *logs* suivie de leur analyse par moteur de corrélation (sur un SMSI, par exemple), l'analyse des *logs* d'accès à Internet ou aux serveurs en cas d'incident, ou encore le filtrage sur les incidents de transferts de flux de données. Deux organisations limitent leur audit à certains répertoires de manière à tracer uniquement les tentatives d'accès infructueuses à certaines arborescences choisies pour leur criticité.

L'examen des fichiers de journalisation (*logs*) du système d'information est automatisé dans huit organisations, et manuel dans trois organisations.

Pour sept organisations, cet examen est effectué périodiquement (une organisation effectue cet examen toutes les heures, deux organisations le font quotidiennement, deux organisations le font à Jour+1, une organisation le fait mensuellement et une organisation le fait sur incident seulement) ; pour quatre organisations, cet examen est effectué en temps réel (notamment pour la détection de virus).

Pour piloter la sécurité de leur système d'information, huit organisations utilisent un **tableau de bord**. Pour celles-ci, ainsi que pour les organisations n'en utilisant pas mais interrogées à ce sujet, les indicateurs de sécurité les plus suivis ou les plus intéressants à suivre sont :

- pour les **indicateurs organisationnels** : le nombre annuel d'utilisateurs ayant suivi une session de sensibilisation à la sécurité des systèmes d'information est choisi par sept organisations, le pourcentage de personnes satisfaites à ces séances de sensibilisation par quatre organisations, le suivi mensuel des dépenses relatives à la sécurité (permettant de piloter le budget alloué et de s'assurer qu'il ne sera pas dépassé) par deux organisations, et trois organisations ont proposé d'autres indicateurs organisationnels tels que le nombre annuel de projets ayant fait l'objet d'une validation par un comité de sécurité, le nombre de comités de sécurité tenus, le nombre de projets intégrés dans le plan de secours (DRP pour *Disaster Recovery Plan*), ou le suivi des cinquante applications les plus sensibles ;
- parmi les **indicateurs fonctionnels** : le taux de disponibilité de chaque application critique de l'organisation arrive en tête, sélectionné par huit organisations, suivi du nombre mensuel de blocages (ou *abends,* problèmes bloquants entraînant une perte de fonctionnalité) de chaque application critique choisi par trois organisations, puis du pourcentage de mots de passe triviaux détectés pour une application donnée choisi par deux organisations ; deux organisations également ont proposé d'autres indicateurs fonctionnels tels que la « fraîcheur » des politiques de sécurité, les postes de contrôle pourvus ou le nombre d'applications ayant un plan de secours (DRP) ;
- sur les **indicateurs opérationnels** : huit organisations ont choisi le nombre mensuel de détections virales recensées sur le réseau interne de l'organisation, six le nombre journalier de *mails* non sollicités mis en quarantai-

Reproduced with permission of the copyright owner. Further reproduction prohibited without permission.

ne par le logiciel antispam, trois le nombre mensuel de comptes révoqués (par essais de connexion infructueux, pouvant révéler une tentative d'intrusion par usurpation de compte) ; la moitié des organisations a proposé d'autres indicateurs opérationnels tels que le délai de distribution des correctifs (*patches*) de sécurité, le pourcentage de machines « patchées » (par rapport au total des machines), le suivi des *policy active directory* (politiques de l'annuaire Windows sur la définition des utilisateurs, groupes, droits par groupe), les actions illicites des administrateurs sécurité et système, les alarmes déclenchées par le SMSI, les erreurs de sauvegarde, le nombre annuel de contrôles internes auto-évalués et audités, et les indicateurs de qualité de ces contrôles.

En cas d'incident de sécurité, sept organisations déclarent élaborer des **fiches d'incident de sécurité** (ou fiches de suivi d'incident).

2.3.5. L'implication des utilisateurs dans la démarche de sécurité

Nous avons interrogé les organisations participantes sur le processus d'**information des utilisateurs** à la sécurité (en termes de méthodes et supports choisis). Les résultats révèlent que toutes les organisations diffusent les informations courantes de sécurité via l'intranet sur des pages dédiées à la sécurité des systèmes d'information, la moitié d'entre elles envoie les messages urgents par *mail* et messages *pop-up* (nouvelle fenêtre de navigateur s'ouvrant automatiquement au-dessus de la fenêtre actuelle) ou privilégient le contact direct avec les utilisateurs ; quatre organisations regroupent les règles et procédures de sécurité dans des répertoires protégés ou une base documentaire dont les accès sont gérés selon le principe de besoin, et quatre organisations utilisent d'autres supports d'information tels que plaquettes, affiches, brochures, séquences vidéo, séances d'apprentissage en ligne (*e-learning*), supports de sensibilisation diffusés à l'ensemble du personnel.

De la même manière, sur le processus de **formation des utilisateurs** à la sécurité (en termes de thèmes abordés), sept organisations forment les salariés à l'utilisation des PC portables et aux moyens de les sécuriser, cinq à l'utilisation d'Internet dans l'organisation et aux sujets connexes (virus, spam, *phishing* – usurpation d'identité en ligne –, ingénierie sociale, etc.), cinq organisent des formations ciblées pour les informaticiens (par exemple, protection des systèmes et réseaux, développement sécurisé, etc.), quatre organisent des formations moins techniques à l'attention de la hiérarchie (présentant notamment la politique de sécurité de l'ensemble du système d'information de l'organisation), deux forment les utilisateurs aux outils de chiffrement, et deux abordent d'autres thèmes de formation tels que la sensibilisation à la sécurité (campagnes obligatoires pour les utilisateurs) ou mettent à disposition des utilisateurs des articles de vulgarisation dans l'intranet corporatif.

2.3.6. Veille technologique et aspects légaux

Parmi les **canaux de veille technologique** exploités en matière de sécuri-

Reproduced with permission of the copyright owner. Further reproduction prohibited without permission.

té par les organisations interrogées, arrivent en tête, *ex æquo* avec neuf réponses positives, les sites Web institutionnels et associatifs spécialisés (tels que DCSSI[12], CNIL[13], CLUSIF[14], etc.) mettant en ligne des informations d'ordre juridique et des tendances en matière de malveillance et de protection, ainsi que les salons et revues spécialisés, fournissant un panorama intéressant de la problématique et des technologies liées à la sécurité des systèmes d'information. Suivent, avec huit votes, les CERT (*Computer Emergency Response Team*), émettant régulièrement des alertes de sécurité et maintenant des bases de vulnérabilités sur les matériels et logiciels les plus courants (en France, on trouve le CERTA dédié à l'administration, le CERT-IST pour les secteurs de l'industrie, des services et du tertiaire, le CERT-RENATER pour l'enseignement et la recherche, le CERT-LEXSI à vocation commerciale). Enfin, cinq organisations utilisent d'autres canaux de veille technologique tels que les sites SecurityFocus (www.securityfocus.com/), SANS Institute (https://www2.sans.org/), participent à des groupes de travail sectoriels (par exemple, NetFocus France), font réaliser des enquêtes spécifiques par des groupes renommés (tels que Gartner Group, Forrester, etc.), organisent des rencontres avec les fournisseurs de produits de sécurité afin qu'ils présentent leurs produits et plaquettes, ou encore s'accordent sur des pratiques de *benchmarking* avec des confrères à l'international.

Huit organisations déclarent avoir déjà eu **recours à la législation** existante en matière de sécurité des systèmes d'information sur la protection de la vie privée (CNIL, loi Informatique et Libertés du 6 janvier 1978 modifiée par la loi du 6 août 2004) ; six organisations ont eu recours à la législation sur la protection de l'information, notamment en termes de protection contre les atteintes directes au système d'information (articles spécifiques 323-1 à 323-4 du code pénal), protection des logiciels (droit d'auteur et propriété intellectuelle), protection contre le vol (article 311-1 du code pénal pour le vol de matériel, divers articles du code pénal ou du code de la propriété intellectuelle pour le vol de données informatiques). Six organisations concèdent également avoir eu recours aux lois de sécurité financière (notamment SOX, LSF, recommandation Bâle 2), cinq à la réglementation française des moyens cryptographiques (DCSSI), et trois à d'autres lois telles que les normes internationales de certification, les lois sur l'archivage légal et fiscal, la réglementation internationale sur le chiffrement, le code de la profession, les lois sur l'anti-blanchiment, ou encore les conventions Belorgey[15] et AERAS[16] dans les secteurs d'activité concernés.

[12] Direction Centrale de la Sécurité des Systèmes d'Information, http://www.ssi.gouv.fr/fr/dcssi/.
[13] Commission Nationale de l'Informatique et des Libertés, http://www.cnil.fr/.
[14] CLUb de la Sécurité de l'Information Français, http://www.clusif.asso.fr/.
[15] La convention Belorgey accorde depuis 2001 un accès au crédit aux personnes présentant un risque aggravé de santé (voir http://www.convention-belorgey-informations.fr/texte-officiel.php).
[16] La convention AERAS (s'Assurer et Emprunter avec un Risque Aggravé de Santé) met en place en 2007 un dispositif d'ensemble tendant à élargir l'accès à l'emprunt et l'accès à l'assurance des personnes présentant un risque aggravé de santé ; elle concerne les prêts professionnels, les prêts immobiliers et les crédits à la consommation (voir http://www.aeras-infos.fr/).

Reproduced with permission of the copyright owner. Further reproduction prohibited without permission.

2.3.7. La gestion du budget de sécurité

Existe-t-il un **budget dédié à la sécurité** dans les grandes organisations françaises ? Les réponses à notre enquête révèlent que la moitié d'entre elles a effectivement un budget dédié à la sécurité ; pour deux organisations, les dépenses de sécurité sont diluées dans le budget informatique mais font l'objet d'une affectation analytique qui permet de les identifier ; pour deux organisations également, les dépenses de sécurité sont diluées dans le budget informatique mais ne font l'objet d'aucune affectation analytique qui permette de les identifier ; et enfin pour l'une d'elles, les dépenses de sécurité sont (encore) imputées au budget de fonctionnement général de l'organisation.

Les diverses politiques pratiquées par les organisations interrogées au regard des **investissements de sécurité** sont les suivantes : dans huit organisations, les investissements souhaités doivent être justifiés par des critères qualitatifs ou une bonne argumentation (notamment lorsque le retour sur investissement – ou ROI pour *Return Over Investment* – n'est pas calculable ou pas exigé) ; dans cinq organisations, certains investissements sont imposés par le groupe ou dans le cadre du recours à la sous-traitance (par exemple, mise en place d'un VPN, utilisation d'outils de chiffrement spécifiques, etc.), dans quatre organisations les investissements souhaités (tels que logiciel antispam, système de signature unique, outil de gestion centralisée de la sécurité, etc.) doivent être justifiés par un calcul de ROI, et trois organisations pratiquent d'autres politiques d'investissements en matière de sécurité telles que le calcul du RROI (réduction du risque sur investissement, parfois exprimé par les termes anglais *Reduction of Risk on Investment* ou *Rapid Return on Investment*) pour les investissements liés aux applications et processus métier, ou la justification formalisée selon divers critères prédéfinis (tels que le risque technique, le risque métier, l'optimisation des coûts ou la création de valeur, par exemple). L'une des organisations n'est tenue de fournir aucune justification relativement à ses investissements.

3. ANALYSE DES RÉSULTATS ET DISCUSSION

3.1. Données générales sur les organisations interrogées

La majorité des organisations interrogées compte plus de 5 000 salariés et appartient au secteur de l'industrie (aucune organisation ne compte moins de 500 salariés ; les secteurs de la distribution, de l'énergie, de la santé et des transports ne sont pas représentés). Cette étude est donc surtout représentative des comportements des grands acteurs industriels français.

3.2. Pratiques en matière de coopération

Un premier constat intéressant s'impose : toutes les organisations interrogées coopèrent (ce qui est révélateur de tendances futures). Plus précisément, nous remarquons qu'elles coopèrent toutes avec leur(s) fournisseur(s), via une application Web ou un site Web. La tendance du Web identifiée dans la littérature est donc clairement confirmée

Reproduced with permission of the copyright owner. Further reproduction prohibited without permission.

par notre étude. Les organisations coopèrent majoritairement plusieurs fois par jour et échangent des informations essentiellement commerciales. Sur le plan technique, toutes les organisations sont « maîtres », avec permissions de consultation et de modification des données de la coopération, pour la plupart en tant qu'utilisateur simple du système d'information inter-organisationnel. Les principaux risques identifiés liés à la coopération sont des risques de sécurité (réseau/Web) et des risques d'intrusion physique spécifiques au contexte inter-organisationnel.

3.3. Pratiques en matière de sécurité des systèmes d'information

En matière de sécurité des systèmes d'information, toutes les organisations craignent les menaces physiques, suivies par les menaces logicielles. Le critère de sécurité le plus important est la disponibilité des données et services du système d'information inter-organisationnel, le souci majeur en cas de compromission de celui-ci étant la perte de crédibilité de l'organisation ; une organisation signale le critère émergent de la traçabilité.

Concernant les modèles et politiques de sécurité mis en œuvre, aucune organisation n'a implémenté les modèles *formels* (de contrôle d'accès notamment) présentés dans la section 1.2. Ceci peut s'expliquer par le fait que ces modèles, bien que performants et innovants, restent tout de même des modèles mathématiques théoriques et difficilement applicables directement dans les organisations. A défaut, les six organisations répondantes à cette question utilisent des modèles très opérationnels, tels que les normes ISO/IEC 27001 et 17799. Cet écart *a priori* important entre l'approche théorique formelle et la réalité des pratiques actuelles, ne l'est en fait pas tant que cela et s'explique par trois arguments principaux. Premièrement, la plupart des innovations proposées dans les modèles formels sont aujourd'hui incluses sous une forme « implémentable » dans les standards de sécurité évoqués. Deuxièmement, l'approche normative s'est imposée depuis une dizaine d'années comme un gage indéniable à la fois de qualité en matière de sécurité de l'information et d'ouverture à l'international, que l'organisation peut faire valoir auprès de ses clients et partenaires comme une garantie supplémentaire. Depuis mars 2005, la certification BS7799-2 (ISO 27001) est possible et assure, par l'évaluation méthodologique d'un tiers indépendant et neutre, qu'une organisation implémente tous les moyens nécessaires à la maîtrise de son système d'information. Malgré l'engouement actuel pour ces certifications, peu d'organismes français[17] permettent encore de certifier BS7799-2. Notons que cette certification n'est pas imposée, néanmoins les partenaires et les clients y sont de plus en plus attentifs. Troisièmement, dans la pratique, la plupart des méthodes (telles que COBIT, COSO, EBIOS ou FEROS), politiques et outils (tels que les annuaires LDAP ou Micro-

[17] LSTI (http://www.lsti.fr/) est le principal acteur dans ce domaine ; beaucoup d'organisations françaises se tournent vers des organismes de certification anglais ou suisses.

Reproduced with permission of the copyright owner. Further reproduction prohibited without permission.

soft *Active Directory*) de sécurité existants pour l'organisation sont compatibles avec ces normes (et non pas avec les modèles formels initiaux). Remarquons pour conclure cette question qu'en soustrayant une organisation non répondante, trois organisations (tout de même) n'appliquent aucun modèle de sécurité ! Est-ce par manque de réactivité ou d'organisation, ou n'en éprouvent-elles pas le besoin... ? Par contre, toutes les organisations mettent en œuvre au moins une politique de sécurité centralisée et/ou distribuée, confirmant ainsi l'application opérationnelle d'un certain nombre de principes de sécurité des systèmes d'information, souvent demandés par le déploiement stratégique par ailleurs de divers modèles actuels de conception et de gouvernance des systèmes d'information.

En termes de documents écrits de sécurité, la charte à l'attention des utilisateurs des moyens informatiques semble être une précaution minimale puisqu'elle a été ratifiée dans toutes les organisations.

Du point de vue des solutions techniques et méthodes de sécurité, toutes les organisations disposent aujourd'hui de pare-feu, proxy, DMZ, VPN, systèmes antivirus et antispam (phénomène relativement nouveau, mais dont l'absence pèse de plus en plus sur les utilisateurs du système d'information). Ces organisations appliquent également des règles et procédures relatives à la gestion des mots de passe, au filtrage du pare-feu, à la définition des VLAN, à la sauvegarde des données, et à la gestion des produits antivirus et antispam. Les méthodes de sécurité les plus utilisées sont le contrôle d'URL, le contrôle de messagerie et l'authentification forte ; l'usage de la biométrie et de la stéganographie semble encore peu répandu en France, en comparaison avec les pratiques affichées outre-Atlantique.

La totalité des organisations répondantes pratique des audits et contrôles de sécurité (pour rappel, une organisation n'a pas souhaité répondre à cette question) ; leurs principales préoccupations sont la surveillance des comptes utilisateurs et l'inspection physique ponctuelle de la salle des serveurs. Pour réaliser leurs audits, huit organisations utilisent un scanner de vulnérabilités.

Toutes les organisations affirment également pratiquer des tests d'intrusion. Devant cet excellent résultat (peut-être « trop bon » ?), sans aller jusqu'à mettre en doute sa véracité, l'on peut néanmoins se demander si les tests d'intrusion sont pratiqués tels qu'envisagés implicitement par la question posée, c'est-à-dire par des cabinets ou consultants externes spécialisés ? Rappelons que des tests d'intrusion réalisés en interne peuvent être biaisés (tests partiels ou exécutés en fonction des résultats attendus, non respect du principe de séparation des fonctions, etc.). Des questions complémentaires intéressantes auraient effectivement pu explorer la méthode et la fréquence des tests d'intrusion pratiqués par ces organisations.

Pour piloter la sécurité de leur système d'information, huit organisations utilisent un tableau de bord. Les indicateurs les plus fréquemment suivis sont la sensibilisation des utilisateurs (au niveau organisationnel), la disponibilité des applications (au niveau fonction-

Reproduced with permission of the copyright owner. Further reproduction prohibited without permission.

nel) et les détections virales (au niveau opérationnel). Sept organisations établissent des fiches de suivi pour les incidents de sécurité recensés.

Concernant l'implication des utilisateurs dans le processus de sécurité, l'information du personnel se fait désormais via l'intranet corporatif ; l'utilisation et la sécurité des PC portables est un thème de formation récurrent.

Les principaux canaux de veille technologique sont les sites Web institutionnels et associatifs, les salons et revues consacrés à la sécurité. En matière légale, la protection de la vie privée est au cœur des préoccupations des organisations.

La moitié des organisations interrogées a dédié un budget spécifique à la sécurité, ce qui confirme les récents efforts des grandes entreprises en matière de gestion de la sécurité des systèmes d'information ; cette tendance avait déjà été soulignée dans la dernière étude[18] du CLUSIF en 2005. Néanmoins, l'autre moitié des organisations dilue ses dépenses et investissements de sécurité dans le budget informatique voire général de l'organisation, rappelant qu'il reste encore du chemin à parcourir... Les pratiques liées aux investissements de sécurité révèlent que ceux-ci sont décidés principalement sur des critères qualitatifs.

Enfin, nous avons laissé les DSI consultés émettre un avis sur notre enquête. Si l'une des organisations a jugé le niveau théorique de l'enquête trop élevé et « rarement utilisé dans les entreprises, sauf celles de grande taille pouvant se permettre une équipe de sécurité importante » (ce qui était en fait le profil recherché), les commentaires des autres organisations témoignent de la pertinence des questions posées : « vous posez les bonnes questions », « nous rencontrons quotidiennement la plupart des problèmes évoqués », etc. Une organisation remarque toutefois que « le questionnaire aborde peu les aspects maîtrise d'ouvrage de la sécurité, les aspects légaux et les fraudes internes/externes ». Une autre organisation nous recommande également, et à juste titre, d' « envisager [davantage dans notre réflexion] les modèles de maturité, qui permettent de se placer dans une perspective de progrès plutôt que dans la recherche de solutions [dites] sûres ».

4. CONCLUSION

La contribution principale de cette étude est la synthèse (rare et fiable) de dix témoignages extrêmement intéressants d'organisations françaises de renom, nous ayant dévoilé leurs pratiques quotidiennes et retours d'expériences en matière de gestion opérationnelle de la sécurité de leurs systèmes d'information. Il ressort de leurs témoignages que, même dans les organisations de grande taille, la sécurité reste souvent le fait de petites équipes transverses portant le message aux équipes opérationnelles et veillant à la mise en place progressive, et pas forcément coordonnée, des mesures de base. Néanmoins, les résultats de cette

[18] Les principaux résultats de cette étude sont disponibles en ligne à l'adresse http://www.vulnerabilite.com/securite-informatique-etude-clusif-actualite-20060723162004.html.

Reproduced with permission of the copyright owner. Further reproduction prohibited without permission.

étude montrent que la sécurité est une préoccupation grandissante pour ces organisations (et par extension pour les organisations françaises en général), les activités de coopération aggravant malheureusement mais inévitablement leur vulnérabilité.

En guise de prolongement à cette étude, il serait intéressant de formuler une politique de sécurité spécifique aux systèmes d'information inter-organisationnels, dont le pilotage serait facilité par un tableau de bord dédié ; de telles propositions sont en cours d'implémentation et seront publiées sous peu.

BIBLIOGRAPHIE

Biba, K.J. (1975), *Integrity Consideration for Secure Computer Systems*, The MITRE Corporation, Technical report MTR-3153, June, Bedford, Mass, USA.

Bieber, P., Cuppens, F. (1992), « A Logical View of Secure Dependencies », *Journal of Computer Security*, Vol. 1, n° 1, p. 99-129.

Denning, D. (1976), « A Lattice Model of Secure Information Flow », *Communications of the ACM*, Vol. 19, n° 5, p. 236-243.

Goguen, J., Meseguer, J. (1982), « Security Policies and Security Models », *Proceedings of the IEEE Symposium on Research in Security and Privacy*, Oakland, CA, USA, May, p. 11-20.

Humphrey, W.S. (1987), *A Method for Assessing the Software Engineering Capability of Contractors*, Software Engineering Institute, Technical report CMU/SEI-87-TR-23, September, Carnegie Mellon University, Pittsburgh, Pennsylvania, USA.

Lampson, B. (1971), « Protection », *Proceedings of the 5th Symposium on Information Sciences and Systems*, Princeton University, USA, March, p. 437-443. Réédité dans *ACM Operating Systems Review*, Vol. 8, n° 1, p. 18-24, janvier 1974.

LaPadula, L.J., Bell, D.E. (1973), *Secure Computer Systems: Mathematical Foundations*, The MITRE Corporation, Technical report MTR-2547, Vol. 2, Bedford, Mass, USA. Réédité dans *Journal of Computer Security*, Vol. 4, n° 2/3, p. 239-263, décembre 1996.

Sandhu, R., Coyne, E.J., Feinstein, H.L., Youman, C.E. (1996), « Role-Based Access Control Models », *IEEE Computer*, Vol. 29, n° 2, p. 38-47.

Thomas, R.K. (1997), « TMAC: A Primitive for Applying RBAC in Collaborative Environment », *Proceedings of the 2nd ACM Workshop on RBAC*, Fairfax, Virginia, USA November, p. 13-19.

Thomas, R.K., Sandhu, R. (1997), « Task-Based Authorization Controls (TBAC): A Family of Models for Active and Enterprise-Oriented Authorization Management », *Proceedings of the 11th IFIP Working Conference on Database Security*, Lake Tahoe, California, USA, p. 166-181.

Reproduced with permission of the copyright owner. Further reproduction prohibited without permission.

ANNEXE

Enquête de sécurité

Cette enquête comporte quatre parties :

- la Partie I concerne les données générales de votre organisation ;
- la Partie II a pour but d'évaluer vos pratiques en matière de coopération éventuelle avec d'autres organisations partenaires ;
- la Partie III évalue vos pratiques générales en matière de sécurité informatique ;
- la Partie IV a pour but de recueillir votre opinion sur quelques propositions en matière de sécurité des systèmes d'information coopératifs et sur le questionnaire soumis.

Partie I. Données générales concernant votre organisation

1.1 Nom de votre organisation :

1.2 Quelle est la taille de votre organisation (en nombre de salariés) ?

- ☐ Moins de 20 salariés
- ☐ 20 à 499 salariés
- ☐ 500 à 999 salariés
- ☐ 1000 à 4999 salariés
- ☐ 5000 salariés et plus

1.3 Si votre organisation appartient à un groupe, quelle est la taille du groupe (en nombre de salariés) ?

- ☐ Moins de 250 salariés
- ☐ 250 à 999 salariés
- ☐ 1000 à 4999 salariés
- ☐ 5000 salariés et plus

Partie II. Vos pratiques en matière de coopération

Remarque : cette partie est sans objet pour les organisations ne coopérant avec aucun partenaire

1. Données générales concernant la coopération

1.1 Votre organisation coopère-t-elle de manière habituelle avec une (ou plusieurs) organisation(s) partenaire(s) ?

- ☐ Fournisseur(s)
- ☐ Client(s)
- ☐ Filiale(s) du groupe
- ☐ Autre (à préciser) :

1.2 Par l'intermédiaire de quel(s) système(s) d'information(s) coopérez-vous avec ce(s) partenaire(s) ?

- ☐ Application propriétaire
- ☐ Application Web
- ☐ Collecticiel (*groupware*)
- ☐ EAI (*Enterprise Applications Integration*)
- ☐ EDI (*Electronic Data Interchange*)

Reproduced with permission of the copyright owner. Further reproduction prohibited without permission.

- ☐ Extranet
- ☐ Grille informatique (*grid computing*)
- ☐ Site Web
- ☐ Marché en ligne (place de marché électronique, plate-forme d'achat et approvisionnement, portail spécialisé)
- ☐ Progiciel de gestion intégré (ERP pour *Enterprise Resource Planning*)
- ☐ Système XML purement documentaire
- ☐ Services Web intégratifs (basés sur XML)
- ☐ *Workflow* purement documentaire
- ☐ *Workflow* intégratif (Système de Gestion de *Workflow*)
- ☐ Autre (à préciser) :

1.3 Quelle est votre **fréquence de coopération** ?

- ☐ Plusieurs fois par jour
- ☐ Journalière
- ☐ Hebdomadaire
- ☐ Mensuelle
- ☐ Trimestrielle ou supérieure

2. Les risques organisationnels liés à la coopération

2.1 Quels sont, selon vous, les **risques organisationnels** principaux liés à cette coopération ?

- ☐ *Lock-in* (dépendance extrême du partenaire)
- ☐ Conflit avec le partenaire
- ☐ Sécurité (réseau, Web)
- ☐ Autre (à préciser) :

3. Les risques de sécurité liés à la coopération

3.1 Quels sont les **types d'informations** échangés lors de la coopération ?

- ☐ Documents papier
- ☐ Messages électroniques (*mail*)
- ☐ Messages EDI ou XML
- ☐ Trafic réseau
- ☐ Autre (à préciser) :

3.2 Quelle est la direction de ces flux d'information (de qui vers qui) ?

- ☐ Votre organisation est « maître » : une (ou plusieurs) organisation(s) partenaire(s) accède(nt) aux informations de votre organisation
- ☐ Votre organisation est « esclave » : votre organisation accède aux informations d'une (ou plusieurs) organisation(s) partenaire(s)
- ☐ Accès à un système d'information commun partagé situé hors des organisations partenaires
- ☐ Mutualisation des informations (grille informatique)
- ☐ Synchronisation des informations (réplication des informations de part et d'autre)

3.3 Quelles sont les **permissions** des utilisateurs de votre organisation sur ces flux d'information ?

- ☐ Consultation (lecture seule des données)
- ☐ Modification (écriture/suppression des données)
- ☐ Consultation et modification (lecture et écriture/suppression des données)

Reproduced with permission of the copyright owner. Further reproduction prohibited without permission.

3.4 Quels sont les différents rôles utilisés au sein de votre organisation pour la coopération ?

- ☐ Utilisateur simple
- ☐ Utilisateur avec privilèges spécifiques
- ☐ Administrateur

3.5 Quelles sont les informations sensibles de votre organisation à protéger lors de la coopération ?

- ☐ Les informations nominatives (fichiers des clients, des fournisseurs, etc.)
- ☐ Les informations relevant du secret de la vie privée (dossiers du personnel)
- ☐ Les informations ne présentant pas un caractère de secret mais qui restent soumises à l'obligation de réserve ou de discrétion professionnelle
- ☐ Les informations constitutives du patrimoine scientifique, industriel, technologique
- ☐ Les informations commerciales
- ☐ Autre (à préciser) :

3.6 Quelles sont les principales menaces institutionnelles (spécifiques au contexte coopératif) de sécurité engendrées par la coopération ?

- ☐ Intrusion dans le périmètre physique (par exemple, salarié d'une organisation partenaire)
- ☐ Intrusion dans le périmètre logique (par exemple, propagation d'un ver ou d'une attaque par le réseau de coopération)
- ☐ Autre (à préciser) :

Partie III. Vos pratiques en matière de sécurité informatique

1. Les risques liés à la sécurité

1.1 A quelles menaces de sécurité votre organisation est-elle principalement confrontée (incluant le contexte coopératif si concernée) ?

- ☐ Menaces physiques (accès physique non autorisé, compromission matérielle du système d'information ou du réseau de communication, etc.)
- ☐ Menaces électroniques (vulnérabilité des moyens de communication sans fil, brouillage ou saturation des communications, atteinte à l'intégrité des communications par injection de données malicieuses, atteinte à la confidentialité par écoute des émissions radioélectriques du réseau, etc.)
- ☐ Menaces logicielles (*scanning*, intrusion, altération et/ou destruction de données, saturation d'une ressource du système d'information, *malware*, etc.)
- ☐ Menaces humaines (ingénierie sociale en particulier)
- ☐ Menaces institutionnelles (évoquées en Partie I question 3.6)
- ☐ Autre (à préciser)

1.2 Quels sont les critères de sécurité les plus importants pour votre organisation (incluant le contexte coopératif si concernée) ?

- ☐ Confidentialité des données
- ☐ Authentification/identification de l'utilisateur partenaire
- ☐ Disponibilité des données/services du système d'information (coopératif)
- ☐ Intégrité des données
- ☐ Non-répudiation des transactions
- ☐ Autre (à préciser)

Reproduced with permission of the copyright owner. Further reproduction prohibited without permission.

1.3 Quels sont pour votre organisation les enjeux liés à la sécurité (conséquences en cas de compromission de la sécurité, incluant le contexte coopératif si concernée) ?

- ☐ Recours juridique (tribunaux, etc.)
- ☐ Perte de marché
- ☐ Perte de crédibilité, perte de confiance
- ☐ Perte de temps
- ☐ Perte d'argent
- ☐ Autre (à préciser)

2. Les modèles et politiques de sécurité

2.1 Existe-t-il un modèle formel de sécurité dans l'organisation ?

- ☐ Aucun
- ☐ Modèle de contrôle d'accès (Lampson 1971, Harrison *et al.* 1976))
- ☐ Modèle de Bell-LaPadula (Bell et LaPadula 1973)
- ☐ Modèle de contrôle de flux d'information (Denning 1976)
- ☐ Modèle de non-interférence (Goguen et Meseguer 1982)
- ☐ Modèle à base de logique modale (Bieber et Cuppens 1992-93)
- ☐ Autre (à préciser)

2.2 Une (ou plusieurs) politique(s) de sécurité est(sont)-elle(s) appliquée(s) dans l'organisation ?

- ☐ Aucune
- ☐ Sécurité centralisée (existence d'une unique politique de sécurité prenant en compte l'ensemble des entités de l'organisation), avec utilisation d'un moniteur de référence (regroupant l'ensemble des mécanismes de protection permettant de garantir les contrôles d'accès et de flux définis par les règles de la politique de sécurité)
- ☐ Sécurité distribuée (coexistence de plusieurs politiques de sécurité éventuellement incohérentes, chacune pouvant être définie par un administrateur de sécurité différent)

2.3 Si oui, quelle(s) est(sont)-elle(s) ?

- ☐ Politique de contrôle d'accès discrétionnaire
- ☐ Politique de contrôle d'accès obligatoire (multi-niveaux, avec exception d'agrégation, avec exception de séparation, avec exception de coalition, avec exception de division, à flux non-transitif)
- ☐ Autre (à préciser)

2.4 En cas de politiques de sécurité multiples, comment sont-elles gérées ?

- ☐ Cohabitation des politiques de sécurité (aucune interaction : aucun sujet de l'une n'accède aux objets de l'autre, le système résultant pouvant être assimilé à deux systèmes indépendants)
- ☐ Fédération des politiques de sécurité (des interactions existent) par composition de leurs règles (voir question 2.5 ci-après)

2.5 En cas de fédération de plusieurs politiques de sécurité, quel mode de composition est-il utilisé ?

- ☐ Approche par interopération (si les politiques initiales sont cohérentes, la politique résultante préserve les conditions de sécurité associées à chaque politique initiale ;

Reproduced with permission of the copyright owner. Further reproduction prohibited without permission.

habituellement mise en œuvre en cas de suspicion mutuelle ou de confiance faible entre les différents administrateurs de sécurité)

- ☐ Approche par combinaison (les politiques initiales peuvent être incohérentes, la politique résultante pouvant ne pas préserver les conditions de sécurité associées à chaque politique initiale ; habituellement mise en œuvre en cas de confiance mutuelle entre les différents administrateurs de sécurité pouvant résulter d'une entente préalable)

3. Les documents de securite

3.1 Quels sont les textes de sécurité existants dans l'organisation ?

- ☐ Chartes : charte sur l'utilisation de la messagerie intranet, charte sur l'utilisation des services Internet ou d'un périmètre plus large, charte informatique
- ☐ Paragraphe spécifique dans le règlement intérieur
- ☐ Paragraphe spécifique dans le contrat de travail
- ☐ Paragraphe spécifique dans le contrat de sous-traitance ou de partenariat
- ☐ Autre (à préciser) :

3.2 Quelles sont les règles de sécurité existantes dans l'organisation ?

3.2.1 A l'usage de la DSI :

- ☐ Identification de l'utilisateur en fonction de son statut, de son entité fonctionnelle, de son établissement ou de sa mission
- ☐ Gestion des mots de passe (contraintes : durée de validité maximum, nombre de caractères minimum, nombre maximum d'essais de connexion infructueux avant révocation du compte, principe de réinitialisation du compte après perte du mot de passe par l'utilisateur, etc.)
- ☐ Filtrage du pare-feu détaillant l'ACL appliquée par la DSI (adresses, ports, protocoles autorisés et interdits) ; les infrastructures complexes peuvent nécessiter l'installation de plusieurs pare-feux, chacun d'eux pouvant être paramétré avec des ACL différentes
- ☐ Définition des VLAN (liste des sous-réseaux virtuels du réseau interne avec pour chacun d'eux, sa finalité, son plan d'adressage et les flux éventuellement filtrés vers les VLAN voisins)
- ☐ Définition des règles de sauvegarde des données (fréquence des sauvegardes, leur type – incrémentales ou totales-, temps de rétention des données et principes d'externalisation des supports magnétiques)
- ☐ Liste des produits antivirus retenus (référence, positionnement –passerelle, serveur de messagerie, postes de travail-, principe de mise à jour)
- ☐ Liste des produits de chiffrement retenus (références, périmètres d'application, environnement de fonctionnement)
- ☐ Configuration d'un poste de travail dédié à du personnel extérieur (bridage physique – cadenas, verrou, etc.-, modification de la configuration –suppression de certains services du système, protection du BIOS, *auto-logon*, etc.-)
- ☐ Autre (à préciser) :

3.2.2 A l'usage des utilisateurs :

- ☐ Conseils sur le choix des mots de passe
- ☐ Règles de protection des PC portables (chiffrement obligatoire des données ou stockage sur un support externe, banalisation du contenu de la sacoche, arrimage du PC portable par un câble ou dépôt dans une armoire dès le retour de l'utilisateur dans l'organisation)
- ☐ Autre (à préciser) :

Reproduced with permission of the copyright owner. Further reproduction prohibited without permission.

3.3 Quelles sont les procédures de sécurité existantes dans l'organisation ?

3.3.1 A l'usage de la DSI :

- ☐ Procédure d'installation et de paramétrage du produit antivirus sur le serveur de messagerie
- ☐ Procédure d'installation et de paramétrage du produit antispam sur la passerelle de messagerie
- ☐ Autre (à préciser) :

3.3.2 A l'usage des utilisateurs :

- ☐ Guide d'utilisation du programme antivirus (fonctionnalités et instructions d'utilisation) ,
- ☐ Guide d'utilisation du produit de chiffrement (fonctionnalités, périmètre d'application, instructions d'utilisation)
- ☐ Guide d'utilisation d'un dispositif d'authentification forte (calculette, carte à puce, *token* USB)
- ☐ Autre (à préciser) :

4. Les solutions techniques et methodes de securité

4.1 Quelles sont les solutions techniques de sécurité existantes dans l'organisation ?

- ☐ Pare-feu (*firewall*)
- ☐ Proxy
- ☐ Zone démilitarisée (DMZ pour *DeMilitarized Zone*)
- ☐ Antivirus
- ☐ Antispam
- ☐ Système de détection ou de prévention d'intrusion (IDS pour *Intrusion Detection System* ou IPS pour *Intrusion Prevention System*)
- ☐ Réseau privé virtuel (VPN pour *Virtual Private Network*)
- ☐ Solution d'authentification unique (SSO pour *Single Sign-On*)
- ☐ Autre (à préciser) :

4.2 Quelles sont les méthodes de sécurité existantes dans l'organisation ?

- ☐ Contrôle d'URL
- ☐ Contrôle des messageries
- ☐ Authentification forte
- ☐ Détection/prévention d'intrusion distribuée (si coopération)
- ☐ Cryptographie
- ☐ Biométrie
- ☐ Stéganographie
- ☐ Autre (à préciser) :

5. Les audits de securité

5.1 Effectuez-vous des audits ponctuels (contrôles) pour vérifier si la politique de sécurité est correctement appliquée ?

- ☐ Aucun audit
- ☐ Vérification auprès d'une population ciblée de la bonne utilisation des logiciels de chiffrement mis à disposition et de l'absence de données « en clair » sur les PC portables
- ☐ Dans un environnement confidentiel, contrôle de la bonne application des règles et procédures correspondantes (dépôt des disques amovibles dans un coffre, fermeture des bureaux en cas d'absence, etc.)

Reproduced with permission of the copyright owner. Further reproduction prohibited without permission.

- ☐ Analyse de l'association compte/propriétaire pour détecter d'éventuelles utilisations de comptes par des personnes non autorisées
- ☐ Auprès du service informatique, inspection de l'état général de la salle des serveurs (les cartons vides et les listings inutiles sont des éléments majeurs de propagation d'incendie)
- ☐ Après de l'administrateur réseau, vérification de la non-utilisation de `telnet` pour l'administration des commutateurs, et de l'absence de mots de passe triviaux
- ☐ Autre (à préciser) :

5.2 Utilisez-vous un scanner de vulnérabilités (ou VDS pour *Vulnerability Detection System*) ?

- ☐ Oui
- ☐ Non
- ☐ Autre (à préciser) :

5.3 Pratiquez-vous des **tests d'intrusion** ?

- ☐ Oui
- ☐ Non
- ☐ Autre (à préciser) :

6. La surveillance du système d'information

6.1 Pratiquez-vous un examen des fichiers de journalisation (*logs*) ?

- ☐ Aucun
- ☐ Configuration du logiciel antivirus pour recevoir automatiquement un mail d'alerte à chaque détection de virus sur le réseau interne
- ☐ Filtrage des événements générés par les commutateurs pour faire ressortir les tentatives de connexion de postes de travail d'adresse MAC inconnue
- ☐ Réglage de l'audit par répertoire de manière à tracer uniquement les tentatives d'accès infructueuses à certaines arborescences choisies pour leur criticité
- ☐ Filtrage des *logs* de connexion de manière à faire ressortir les révocations de comptes de session (si un nombre d'essais de connexion maximum a été défini)
- ☐ Autre (à préciser) :

6.2 Si oui, cet examen des fichiers de journalisation (*logs*) est-il :

- ☐ Automatisé ?
- ☐ Manuel ?

6.3 Si oui, l'analyse des fichiers de journalisation (*logs*) est-elle réalisée :

- ☐ En temps réel ?
- ☐ Périodiquement (à préciser) :

7. Les tableaux de bord de la sécurité

7.1 Utilisez-vous un tableau de bord pour piloter la sécurité de votre système d'information ?

- ☐ Oui
- ☐ Non
- ☐ Autre (à préciser) :

Reproduced with permission of the copyright owner. Further reproduction prohibited without permission.

7.2 Si oui, quels indicateurs de sécurité suivez-vous ? Si non, quels indicateurs de sécurité vous paraîtraient-ils intéressants à suivre ?

7.2.1 Indicateurs organisationnels

- ☐ Nombre annuel d'utilisateurs ayant suivi une session de sensibilisation à la sécurité informatique
- ☐ Pourcentage de personnes satisfaites à ces séances de sensibilisation
- ☐ Suivi mensuel des dépenses relatives à la sécurité (permettant de piloter le budget alloué et de s'assurer qu'il ne sera pas dépassé)
- ☐ Autre (à préciser)

7.2.2 Indicateurs fonctionnels :

- ☐ Taux de disponibilité de chaque application critique de l'organisation
- ☐ Nombre mensuel de blocages (*ocends*) de chaque application critique
- ☐ Pourcentage de mots de passe triviaux détectés pour une application donnée
- ☐ Autre (à préciser)

7.2.3 Indicateurs opérationnels :

- ☐ Nombre mensuel de détections virales recensées sur le réseau interne de l'organisation
- ☐ Nombre journalier de *mails* non sollicités mis en quarantaine par le logiciel antispam
- ☐ Nombre mensuel de comptes révoqués (essais de connexion infructueux, pouvant révéler une tentative d'intrusion par usurpation de compte)
- ☐ Autre (à préciser)

7.3 Suivez-vous les incidents de sécurité par l'élaboration de « fiches d'incident de sécurité » ?

- ☐ Oui
- ☐ Non
- ☐ Autre (à préciser)

8. L'implication des utilisateurs

8.1 Comment informez-vous les utilisateurs sur la sécurité (méthodes et supports choisis) ?

- ☐ Regroupement des règles et procédures de sécurité dans des répertoires protégés ou une base documentaire dont les accès sont gérés selon le principe de besoin
- ☐ Diffusion des informations courantes via l'intranet sur des pages dédiées à la sécurité informatique
- ☐ Envoi de messages urgents par *mail* et messages « pop-up »
- ☐ Contact direct avec les utilisateurs
- ☐ Autres supports (plaquettes, affiches, séquences vidéo, etc.) :

8.2 Comment formez-vous les utilisateurs à la sécurité (thèmes abordés) ?

- ☐ Formation aux outils de chiffrement
- ☐ Formation à l'utilisation des PC portables et aux moyens de les sécuriser
- ☐ Formation à l'utilisation d'Internet dans l'organisation et sujets connexes (virus, *spam*, *phishing*, ingénierie sociale, etc.)
- ☐ Formation moins technique à l'attention de la hiérarchie, présentant la politique de sécurité de l'ensemble du SI de l'organisation
- ☐ Formations ciblées pour les informaticiens (protection des systèmes et réseaux, développement sécurisé, etc.)
- ☐ Autre (à préciser)

Reproduced with permission of the copyright owner. Further reproduction prohibited without permission.

9. Veille technologique et aspects legaux

9.1 Quels canaux de veille technologique exploitez-vous ?

- ☐ Les sites Web institutionnels et associatifs (DCSSI, CNIL, CLUSIF, etc.) donnant des informations d'ordre juridique et des tendances en matière de malveillance et de protection
- ☐ Les CERT (*Computer Emergency Response Team*) émettant régulièrement des alertes de sécurité et maintenant des bases de vulnérabilités sur les matériels et logiciels les plus courants (en France, on trouve le CERTA dédié à l'administration, le CERT-IST pour les secteurs de l'industrie, des services et du tertiaire, le CERT-RENATER pour l'enseignement et la recherche, le CERT-LEXSI à vocation commerciale)
- ☐ Les salons et revues spécialisés fournissant un panorama intéressant des problématiques et des technologies liées à la sécurité informatique
- ☐ Autre (à préciser) :

9.2 Avez-vous déjà eu recours à la législation existante en matière de sécurité informatique ?

- ☐ Protection de la vie privée (CNIL, loi Informatique et Libertés du 6 janvier 1978 modifiée par la loi du 6 août 2004)
- ☐ Protection de l'information : protection contre les atteintes directes au SI (articles spécifiques 323-1 à 323-4 du code pénal), protection des logiciels (droit d'auteur et propriété intellectuelle), protection contre le vol (article 311-1 du code pénal pour le vol de matériel, divers articles du code pénal ou du code de la propriété intellectuelle pour le vol de données informatiques, etc.)
- ☐ Lois de sécurité financière (loi « Sarbanes-Oxley », loi de sécurité financière LSF, recommandation « Bâle 2 »)
- ☐ Réglementation française des moyens cryptographiques (DCSSI)
- ☐ Autre (à préciser) :

10. La gestion du budget de securité

10.1 Existe-t-il un budget de sécurité dans l'organisation ?

- ☐ Non, la gestion de la sécurité est externalisée
- ☐ Non, les dépenses de sécurité sont imputées au budget de fonctionnement général de l'organisation
- ☐ Non, les dépenses de sécurité sont diluées dans le budget informatique et ne font l'objet d'aucune affectation analytique qui permette de les identifier
- ☐ Non, les dépenses de sécurité sont diluées dans le budget informatique mais font l'objet d'une affectation analytique qui permet de les identifier
- ☐ Oui, il existe un budget spécifique dédié à la sécurité dans l'organisation

10.2 Quelle est la politique pratiquée par l'organisation au regard des investissements ?

- ☐ Certains investissements sont imposés dans le cadre du recours à la sous-traitance (mise en place d'un VPN, utilisation d'outils de chiffrement spécifiques, etc.)
- ☐ Les investissements souhaités (logiciel antispam, système de signature unique, outil de gestion centralisée de la sécurité, etc.) doivent être justifiés par un calcul de retour sur investissement (ou ROI pour *Return Over Investment*)
- ☐ Si le ROI n'est pas calculable (ou pas exigé), les investissements souhaités doivent tout de même être justifiés par des critères qualitatifs ou une bonne argumentation

Reproduced with permission of the copyright owner. Further reproduction prohibited without permission.

☐ Aucune justification nécessaire
☐ Autre (à préciser) :

Partie IV. Votre opinion nous intéresse

1. Proposition d'un modele de securite pour les systemes d'information cooperatifs

1.1 Etes-vous d'accord avec les **propriétés de sécurité** suivantes pour les systèmes d'information coopératifs (à cocher dans l'affirmative) ?

☐ Confidentialité : la confidentialité des données est assurée par leur chiffrement lors de leur transit entre les partenaires de la coopération
☐ Authentification : l'authentification de l'utilisateur est garantie par le contrôle de l'accès au système d'information coopératif utilisé (annuaire LDAP, architecture PKI, etc.)
☐ Disponibilité : la disponibilité d'un service ou d'une ressource du système d'information coopératif est garantie par la limitation de ses défaillances (prévention, tolérance, élimination des fautes)
☐ Intégrité : l'intégrité des données est assurée par l'utilisation de techniques de sécurisation des communications et de chiffrement des données lors des transactions entre les partenaires de la coopération
☐ Non-répudiation : la non-répudiation d'une transaction est assurée par l'utilisation de certificats numériques (algorithmes de signature) par les différents partenaires de la coopération

1.2 Etes-vous d'accord avec les **invariants de sécurité** suivants (à cocher dans l'affirmative) ?

☐ Sécurité physique (ou sécurité des infrastructures matérielles) : un système d'information coopératif est sûr s'il est disponible et si son accès est contrôlé
☐ Sécurité organisationnelle (ou obligations imposées aux différents acteurs de l'organisation) : un système d'information coopératif est sûr s'il respecte la politique de sécurité définie par la DSI
☐ Sécurité logique (ou sécurité des données, applications et systèmes d'exploitation) : un système d'information coopératif est sûr s'il met en œuvre les critères de confidentialité, authentification, disponibilité, intégrité et non-répudiation décrits dans la question 1.1 ci-dessus

1.3 Pour les organisations utilisant un (ou plusieurs) système(s) d'information coopératif(s), quels **problèmes de sécurité** avez-vous rencontrés ? Comment les avez-vous résolus ?

2. Avez-vous des commentaires a formuler relativement à cette enquete de securité ?

Soumission par Email | Impression du Formulaire

Reproduced with permission of the copyright owner. Further reproduction prohibited without permission.