Sécurité des systèmes d'information

Quelle politique globale de gestion des risques ?

SEPTEMBRE 2002

LE CIGREF

Le Cigref, Club informatique des grandes entreprises françaises, existe depuis 1970. Sa finalité est la promotion de l'usage des systèmes d'information comme facteur de création de valeurs pour l'entreprise. Il constitue un lieu privilégié de rencontre et d'échange d'informations entre les responsables des grandes entreprises françaises ou européennes utilisatrices d'importants systèmes d'information. Ce partage d'expériences vise à faire émerger les meilleures pratiques. Chaque année, le Cigref réalise des études sur des sujets d'intérêt commun.

Rapports publiés par le Cigref en 2001-2002 :

Alignement stratégique du système d'information

Comment faire du système d'information un atout pour l'entreprise ?

Comment le contrôleur de gestion peut-il assister le DSI ?

E-learning et e-formation

Du radar à l'agenda des DSI. Rapport Introductif

E-procurement et places de marché

Quels enseignements tirer à l'issue du projet IMP ?

Gouvernance du système d'information

Problématiques et démarches

Internet dans l'entreprise

Panorama des usages

Nomenclature 2002

Les emplois-métiers du système d'information dans les grandes entreprises

XML, vers un format universel ?

Fiche technologique. 2e édition

Ces rapports peuvent être obtenus en se connectant sur le site web du Cigref : www.cigref.fr

PARTICIPANTS

Ce rapport est issu des travaux d'un groupe de réflexion du Cigref, dans le cadre du comité de pilotage « Urbanisme, architectures et nouvelles technologies » animé par Pascal Buffard (Axa) et Bertrand Amilhat (Manpower), avec la participation active des personnes et entreprises suivantes :

Anne-Elise Alberio, Crédit Agricole
Jean-Pierre Asun, Atofina
Pierre Bartaire, AP-HP
Nadir Belarbi, Danone
Antoine Beligné, PSA Peugeot Citroën
Pascal Boisgibault, RATP
Christian Bouvier, Cegetel
Monique Bureau, Maaf
Laurent Cabirol, CEA
Elisabeth Canat, Crédit Agricole
Pierre-Albert Carlier, LVMH
Jean-Louis Carton, MGEN
Francis Cauvé, Banque de France
Bernard Charpentier, Retraites Unies
Jean-Paul Charron, SNCF
Richard Chenuc, Informatique CDC (Caisse des Dépôts)
Brigitte Cohen, BNP Paribas
Philippe Copello, LVMH
François Coulomb, Air France
Alain Cudel, Amadeus
Gilbert de Mareschal, Lagardère
Stéphane Dogniaux, Snecma
Denis Dossantos, Altadis
Michel Dubar, Société Générale
Sven Dubois, LVMH
Jean-Michel Eberswiller, Gehis France (OCP)
Jean Eichelberger, Cie de Saint Gobain
Mojtaba Farhat Gehis, France (OCP)
Luc Fremaux, Groupe Vauban (Agirc)
Pascal Froment, EDF
Paul Olivier Gibert, AG2R
Marc Giraud, Essilor
Olivier Gonnet, GCA
Jean-François Gornet, EDF-Gaz de France
Christian Grard, Atica
Henri Guiheux, Scor
Dominique Guillaume, Framatome ANP
Jean-Jacques Hery, AG2R
Georges Le Du, Retraites Unies
Yves Le Duic, Crédit Agricole
Thierry Lesaffre, Crédit Lyonnais
Fabrice Leyglene, Altadis
Kim Leng Ly, Technip
Jean-François Lyet, TotalFinaElf
Gérard Margueritte, Framatome ANP
Hervé Martineau, La Poste
Eric Matoussowsky, La Française des Jeux
Patrick Mery, Cnav-TS
Cyril Moneron, Compagnie de Saint Gobain
Toai Nguyen-Huin, BNP Paribas
Sabine Odet, Air France
Thierry Parard, MGEN
Ludovic Petit, Cegetel
Frédéric Pfeffer, Médéric
Éric Pichon, Cogema
Éric Piskurski, Groupement des Mousquetaires
Martin Primke, Sodexho
Pierre Ragimbeau, RATP
Pierre-Pascal Regnault, TotalFinaElf
Alain Rémy, AG2R
Arnaud Sarrazin, RATP
Régis Sellier, EDF
Jean-Louis Szuba, EADS
Christiane Trognon, SNCF
Jean Vergnoux, Renault
Philippe Zanini, Mairie de Paris
Robert Zeitouni, Crédit Agricole

L'étude a été rédigée par Stéphane Rouhier, chargé de mission du Cigref.

SOMMAIRE

TABLE DES ILLUSTRATIONS

RÉSUMÉ

Une fonction sécurité arrivée à maturité

La majorité des grandes entreprises françaises[1] ont mis en place une fonction de responsable de la sécurité des systèmes d'information (RSSI), ce qui témoigne de l'importance du sujet et de la maturité croissante de la fonction.

La fonction RSSI reste encore principalement localisée au niveau groupe ou holding. Elle est encore assez peu développée au niveau des filiales et des métiers.

La plupart des responsables de la sécurité considèrent que la direction générale est désormais suffisamment sensibilisée aux risques liés aux systèmes d'information et que leur politique de sécurité est alignée avec la stratégie de l'entreprise[2].

Un modèle de gouvernance encore perfectible

La gouvernance de la sécurité, autrement dit le « qui fait quoi » et le « qui est responsable de quoi dans l'entreprise » est une notion vitale pour la pérennité du système d'information et la survie de l'entreprise.

Concernant la gouvernance, un effort de clarification doit être entrepris dans la répartition des rôles, en tenant compte de la culture et des spécificités de l'organisation, de manière à éviter qu'une même personne puisse être juge et parti et de manière à réduire les risques de dysfonctionnement dans l'organisation.

Une politique de sécurité orientée « gestion des risques »

Les préoccupations des DG en matière de sécurité du système d'information portent principalement sur deux aspects : la gestion des risques et le retour sur investissement.

Les responsables de la sécurité intègrent la dimension « gestion des risques » dans leurs pratiques mais ont encore des progrès à faire en matière de métrique de la rentabilité.

Pour les DSI, la question de la continuité du système d'information est un élément central pour répondre aux besoins des métiers.

[1] Les données statistiques contenues dans ce rapport sont extraites d'une enquête menée par le Cigref auprès de ses 115 membres en mai 2002.

[2] Sur les questions d'alignement stratégique, voir le rapport du Cigref « Alignement stratégique du système d'information », publié en septembre 2002.

Des menaces qui s'intensifient et se complexifient

Les personnes les plus citées comme étant à l'origine des menaces sont les salariés et les *hackers*. Les États ont parfois une influence en matière d'intelligence et de sécurité économique. Cette influence semble ici sous-estimée. De même, le rôle des concurrents comme source de menace semble sous-évalué.

Au palmarès des attaques subies en 2001 figurent en première ligne les attaques virales, les vols, les pannes internes et les erreurs d'utilisation.

Les entreprises ont tendance à utiliser plusieurs arguments pour justifier leur budget sécurité : principalement le discours de la gestion des risques, de la contrainte réglementaire et de l'apport *business*.

En dehors de l'indisponibilité de machines et de la perte de revenu liée à un processus *business* (par exemple un site de vente en ligne), les entreprises ont encore du mal à chiffrer leurs pertes.

Les normes et méthodes, un choix nécessaire et structurant

Choisir une norme ou une méthode d'analyse de risque ou d'organisation dans le domaine de la sécurité est un choix souvent structurant et de long terme pour l'entreprise en termes de coût, de ressources et d'organisation.

L'entreprise doit faire au préalable une analyse fine de ses besoins, de l'adéquation des méthodes existantes à ses besoins et de ses ressources disponibles.

Parmi les critères de choix à retenir, on peut citer : l'objectif de la méthode, le degré de couverture, Le caractère standard ou non, le caractère transversal au système d'information ou non, le niveau d'adaptation possible à l'organisation, la facilité de mise en œuvre, le coût, la maintenance de la méthode…

Le choix d'une méthode s'avère nécessaire mais pas suffisant. En effet, la méthode ne doit pas servir d'alibi ni masquer les insuffisances budgétaires, les erreurs techniques, les lacunes organisationnelles ou les défaillances humaines.

Les enjeux juridiques : risques et opportunités pour la DSI

Dans le cadre de ses activités sur la sécurité et des entretiens juridiques, le Cigref s'est intéressé à la responsabilité pénale du directeur des systèmes d'information. Il apparaît que, par le biais des mécanismes de délégation, la responsabilité pénale du DSI, voire du RSSI ou de l'administrateur de la messagerie, est de plus en plus évoquée.

Parmi les trois dossiers juridiques jugés prioritaires par les responsables de la sécurité et les DSI, on peut citer l'archivage et la conservation des données, la responsabilité des hébergeurs et des prestataires techniques, la gestion des données personnelles des clients. D'autres dossiers sont jugés également importants : la cybersurveillance des salariés, la signature électronique…

L'année 2001-2002 aura été marquée par plusieurs textes législatifs ayant des incidences sur la politique de sécurité de l'entreprise. Parmi ceux-ci, on peut citer :

- la loi sur la sécurité quotidienne du 15 novembre 2001, avec l'obligation faite aux opérateurs de télécommunication et aux fournisseurs d'accès à internet de conserver les données de connexion à des fins de police ;
- la convention du Conseil de l'Europe du 23 novembre 2001 sur la cybercriminalité qui devrait permettre une avancée en matière de coopération judiciaire et de poursuites pénales au niveau internationales ;
- le projet de loi du 30 janvier 2002, visant à transposer la directive communautaire du 24 octobre 1995 sur la protection des données à caractère personnel, qui va entraîner une refonte de la loi Informatique et Libertés de 1978 et renforcer les pouvoirs de la Cnil ;
- la loi du 4 mars 2002, relative aux droits des malades et à la qualité du système de santé, dont les articles L. 1110-4 et L. 1111-8 ont trait à la sécurité des systèmes d'information (cas d'utilisation de la carte professionnelle de santé et conditions d'agrément des hébergeurs) ;
- le décret du 18 avril 2002, relatif à l'évaluation et à la certification de la sécurité offerte par les produits et les systèmes des technologies de l'information ;

- l'arrêté du 31 mai 2002, relatif à la reconnaissance de la qualification des prestataires de certification électronique et à l'accréditation des organismes chargés de l'évaluation, permettant la mise en place d'un schéma d'accréditation volontaire dans le domaine des signatures électroniques.

Perspectives

Les entreprises sont passées d'une politique de sécurité basée sur la juxtaposition de briques hétérogènes à une politique de sécurité visant à l'optimisation des processus et à la rationalisation des investissements en sécurité.

Parmi les marges de progrès et les chantiers complexes non résolus, on peut citer la gestion de la sécurité dans un contexte international et la question de la persistance de l'efficacité de la sécurité dans le temps.

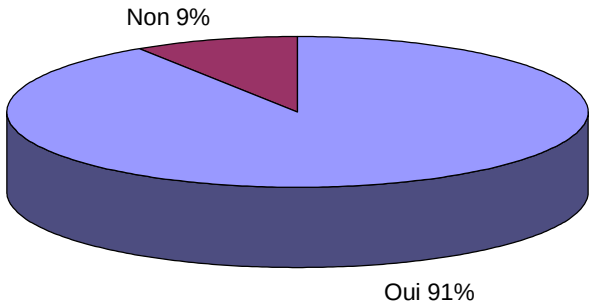
Pour une majorité des grandes entreprises interrogées, le budget sécurité va encore augmenter en 2003, mais pas sur l'ensemble des postes. Sont principalement concernés les services d'annuaires, les réseaux privés virtuels, le *monitoring* de la sécurité, les infrastructures à clé publique ou PKI, les outils de chiffrements et d'authentification, les outils de détection d'intrusion internes.

La sécurité étant actuellement un thème à la mode, il n'est pas exclu qu'il y ait à terme un risque de surinvestissement dans le domaine, à l'instar de ce qui s'est produit par le passé dans l'*e-business* ou les télécoms. Le Cigref met en garde contre des discours marketing parfois surgénérateurs de promesses mais également aussi contre un discours souvent trop alarmiste.

1. QUEL MODÈLE DE GOUVERNANCE POUR LA SÉCURITÉ ?

1.1 Organisation de la politique de sécurité

La fonction de responsable de la sécurité des systèmes d'information (RSSI) commence à se pérenniser au sein des grandes organisations. La plupart des grandes entreprises ont mis en place une fonction de responsable de la sécurité[3], ce qui témoigne de l'importance du sujet et de la maturité croissante de la fonction.



Source : Cigref 2002

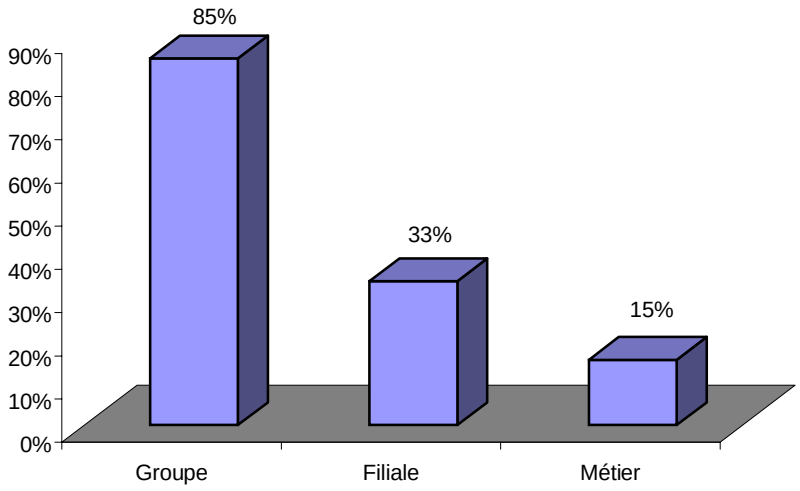
Figure 1 : Votre entreprise a-t-elle mis en place une fonction de responsable de la sécurité ?

La fonction RSSI reste encore principalement localisée au niveau groupe ou holding. Elle est encore assez peu développée au niveau des filiales et des métiers.

Ce sont les banques et assurances et les groupes décentralisés qui ont le plus mis en place des fonctions RSSI au niveau des filiales ou des métiers.

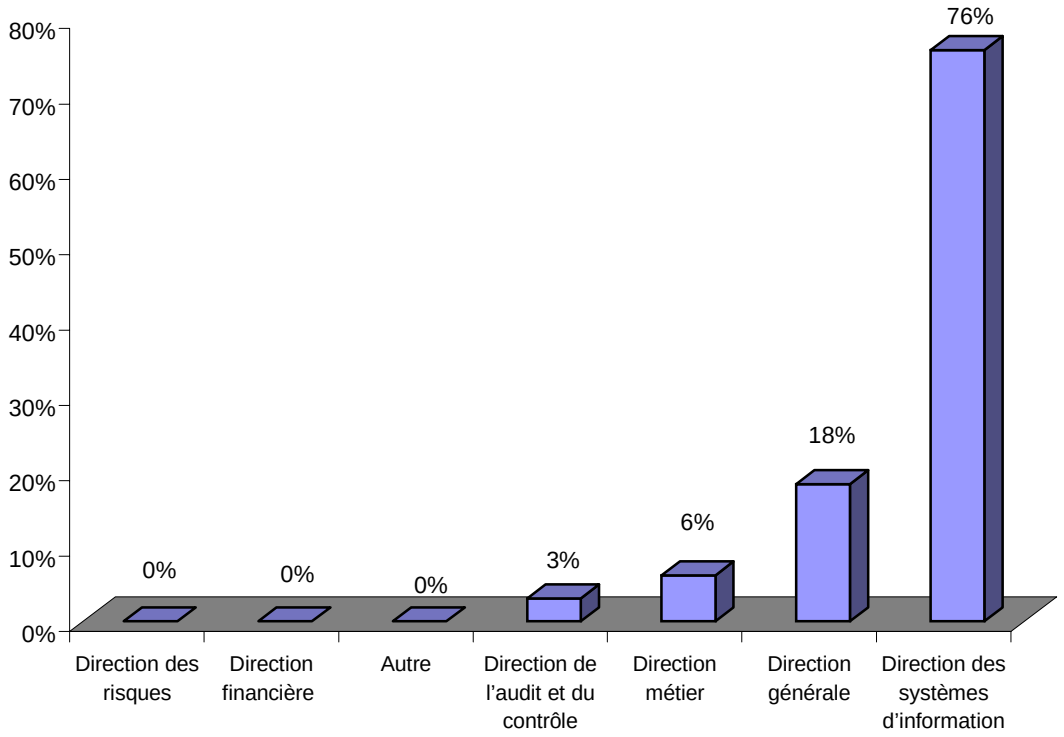
Le RSSI est principalement rattaché à la direction des systèmes d'information. Plus rarement, il peut être rattaché à la direction générale ou à une direction métier ou à la direction de l'audit. Ce mode d'organisation illustre bien à la fois la dimension technique et la nature transversale de la fonction.

[3] Voir note 1.



Source : Cigref 2002

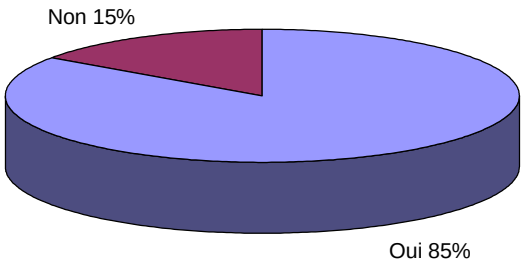
Figure 2 : Si oui, à quel niveau est le RSSI ?



Source : Cigref 2002

Figure 3 : Quel est le rattachement hiérarchique du RSSI ?

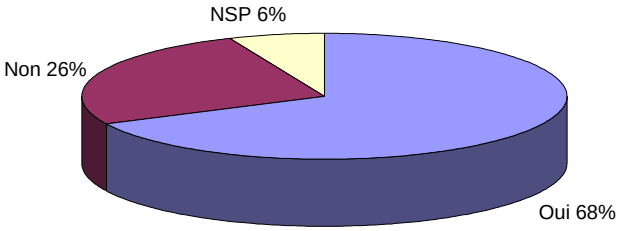
La majorité des entreprises interrogées ont mis en place une politique de sécurité formalisée par des règles, des processus et des schémas organisationnels. Plus la sécurité fait partie du cœur du métier de l'entreprise, mieux elle sera maîtrisée.



Source : Cigref 2002

Figure 4 : Votre entreprise a-t-elle mis en place une politique de sécurité ?

La plupart des responsables de la sécurité considèrent que leur politique de sécurité est alignée avec la stratégie du système d'information et avec la stratégie de l'entreprise[4].



Source : Cigref 2002

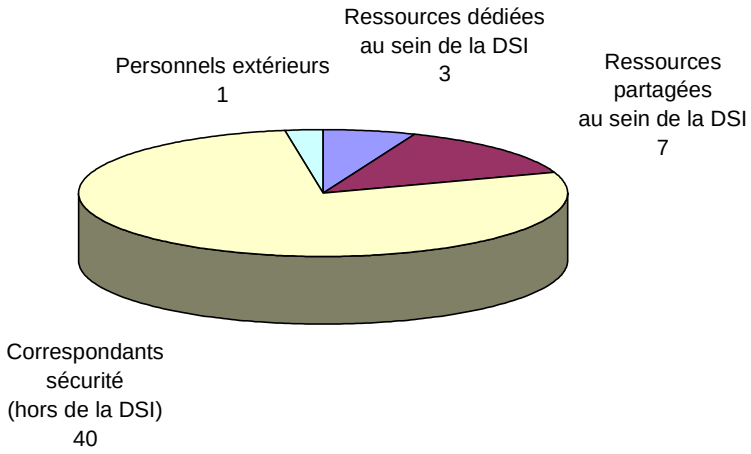
Figure 5 : Cette politique est-elle en relation avec la stratégie de l'entreprise ?

[4] Sur l'alignement, voir aussi le rapport du Cigref « Alignement stratégique du système d'information », paru en septembre 2002.

Les effectifs des équipes sécurité restent encore relativement faibles, en moyenne trois personnes dédiées au sein de la DSI, sept ressources partagées et surtout une quarantaine de correspondants sécurité. Ces chiffres sont à mettre en perspective avec un effectif moyen de 1 000 personnes au sein de la DSI et de 40 000 personnes au sein de l'entreprise.

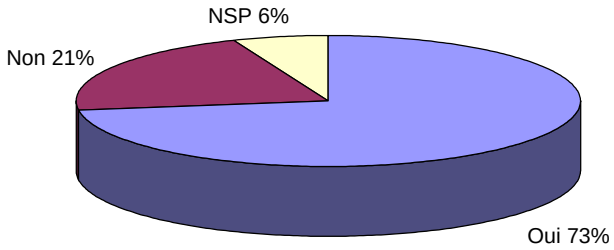
Ces chiffres illustrent l'importance des mécanismes de « relais » au sein de l'entreprise pour une mise en œuvre efficace de la politique de sécurité.

L'efficacité d'une politique de sécurité ne se mesure pas tant au budget investi ou au nombre de « divisions » sécurité mais dépend surtout de la sensibilité de l'écosystème aux menaces, du chaînage des responsabilités et de la culture de la sécurité des salariés de l'entreprise, des prestataires et des fournisseurs.



Source : Cigref 2002

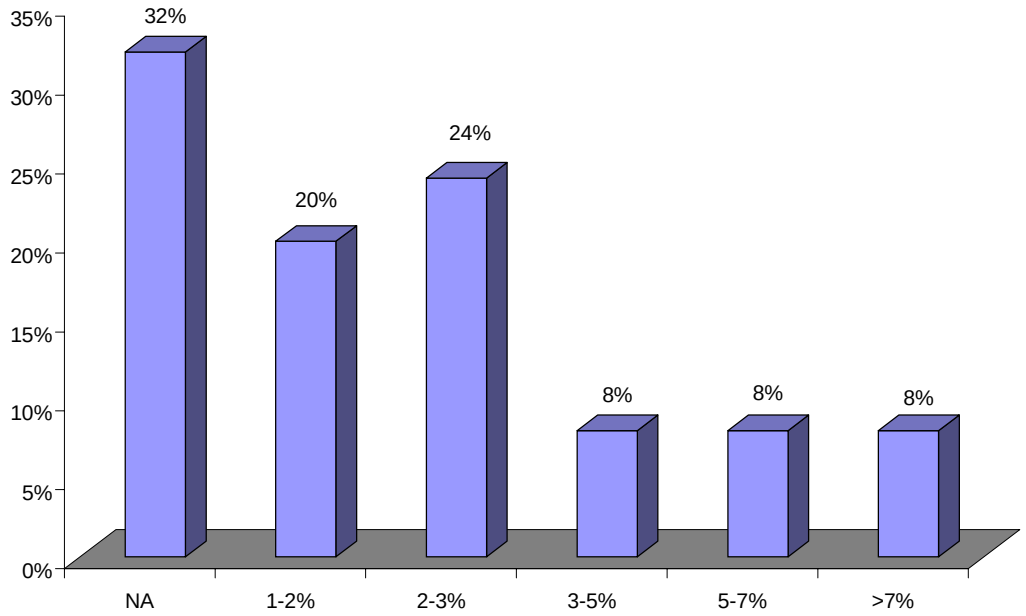
Figure 6 : Quelle est en moyenne la taille de votre équipe sécurité ?



Source : Cigref 2002

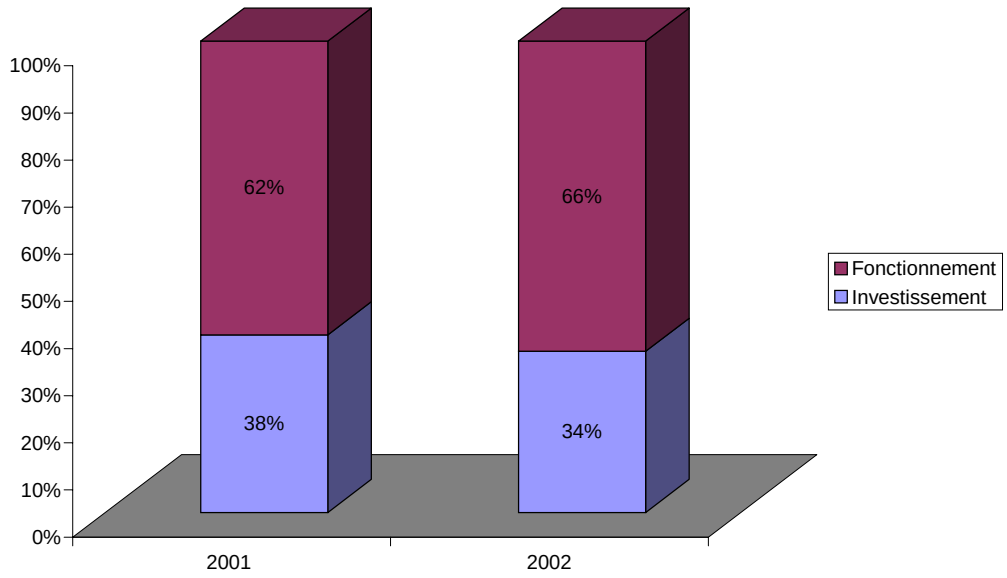
Figure 7 : Disposez-vous d'un budget spécifique pour la sécurité ?

La plupart des entreprises déclarent disposer d'une ligne budgétaire spécifique pour la sécurité, au moins en ce qui concerne le budget du groupe ou de la holding. Le budget moyen est de l'ordre de 1 à 3 % du budget informatique.



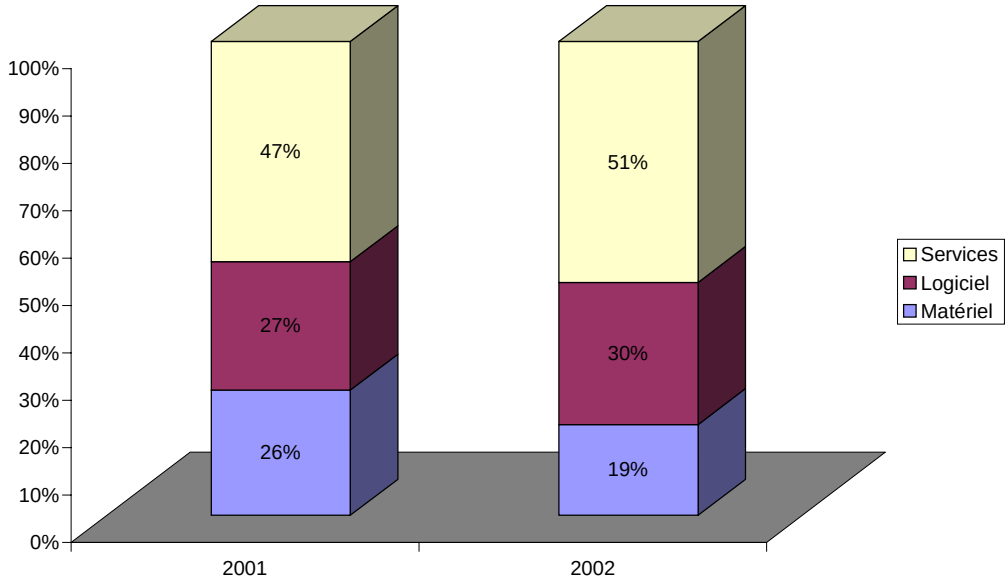
Source : Cigref 2002

Figure 8 : Quelle est la part de votre budget informatique consacrée à la sécurité en 2002 ? (en pour-cent, hors stockage)



Source : Cigref 2002

Figure 9 : Comment se répartit votre budget sécurité entre investissement et fonctionnement ?



Source : Cigref 2002

Figure 10 : Comment se répartit votre budget sécurité entre matériel, logiciel et services ?

En moyenne, les deux tiers du budget sécurité sont consacrés à des dépenses de fonctionnement. La diminution de la part liée à l'investissement montre l'arrivée à maturité de la fonction sécurité du système d'information. Mais l'investissement néanmoins reste plus important que sur d'autres segments du budget pour le système d'information.

La part des services représente en moyenne la moitié du budget sécurité des grandes entreprises françaises.

Les services comprennent les services de conseil, de formation, d'intégration, de support et de maintenance. Les dépenses liées aux services devraient rester stables en 2002-2003.

1.2 Quels rôles pour quels acteurs ?

La gouvernance de la sécurité, autrement dit le « qui fait quoi » et le « qui est responsable de quoi dans l'entreprise » est une notion vitale pour la pérennité du système d'information et la survie de l'entreprise.

Elle vise à garantir une politique de sécurité optimale dans le temps et dans l'espace. Elle repose sur un principe de séparation des tâches et s'articule selon trois axes :

- qui définit les règles ?
- qui les met en œuvre ?
- qui les contrôle ?

Dans la pratique, il peut y avoir parfois une certaine confusion des rôles et des genres. Une même personne peut remplir plusieurs rôles et intervenir à plusieurs niveaux : définition des règles, mise en œuvre et contrôle.

Un effort de clarification doit être entrepris dans la répartition des rôles, en tenant compte de la culture et des spécificités de l'organisation, de manière à éviter qu'une même personne puisse être « juge et parti » et de manière à réduire les risques de dysfonctionnement dans l'organisation[5].

Plusieurs démarches de gouvernance sont envisageables, chacune présentant ses avantages et ses inconvénients : la démarche par indicateurs, la démarche constituante, la démarche législative, la démarche par processus et la démarche structurelle. Les problèmes communs à l'ensemble des démarches étant l'application (*enforcement*) et la révision de la démarche dans le temps.

La définition des objectifs et des règles de sécurité est en général de la responsabilité du RSSI groupe, conjointement avec le DSI groupe et parfois la direction générale. Dans certaines organisations, on trouve des conseils de sécurité,

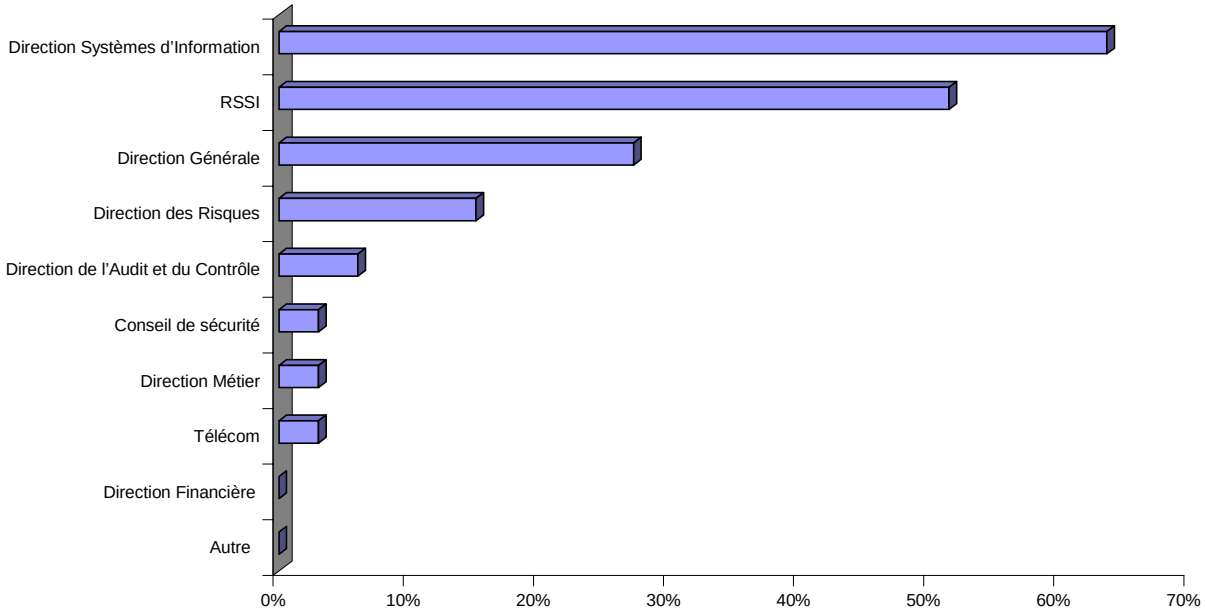
[5] Sur la gouvernance, voir le rapport du Cigref : « Gouvernance du système d'information », publié en septembre 2002.

structures *ad hoc* réunissant le RSSI, les directions métiers, la DG et le DSI, destinées à définir de manière conjointe les objectifs, les priorités et les ressources nécessaires à la mise en place de la politique de sécurité.

La mise en œuvre est souvent du ressort des DSI métiers et des correspondants sécurité présents dans les directions métiers. Pour cela, le RSSI groupe s'appuie généralement sur des fonctions relais tels les responsables télécoms, les administrateurs de messageries, les administrateurs de réseaux et systèmes, les responsables bureautiques, en définissant des « propriétaires » de l'information, des gestionnaires des droits.

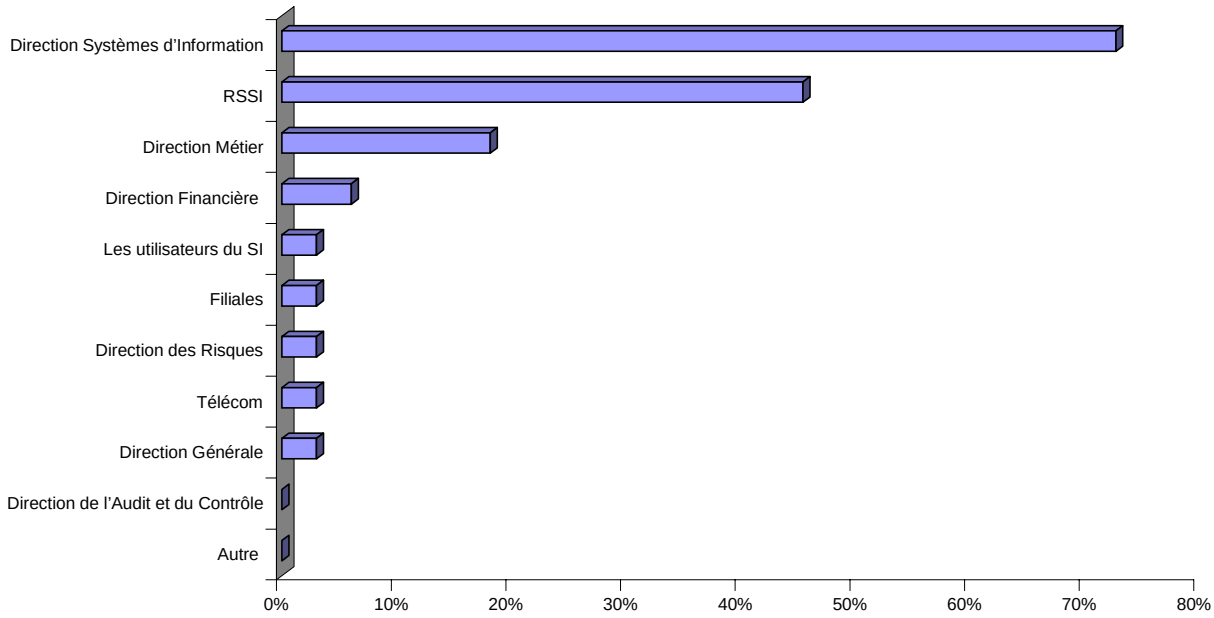
Le contrôle est effectué majoritairement par le contrôle interne, parfois avec l'aide d'un cabinet d'audit externe.

Les grandes entreprises font appel à des prestataires extérieurs plutôt en aval de leur politique de sécurité, lors de la phase d'audit et de contrôle.



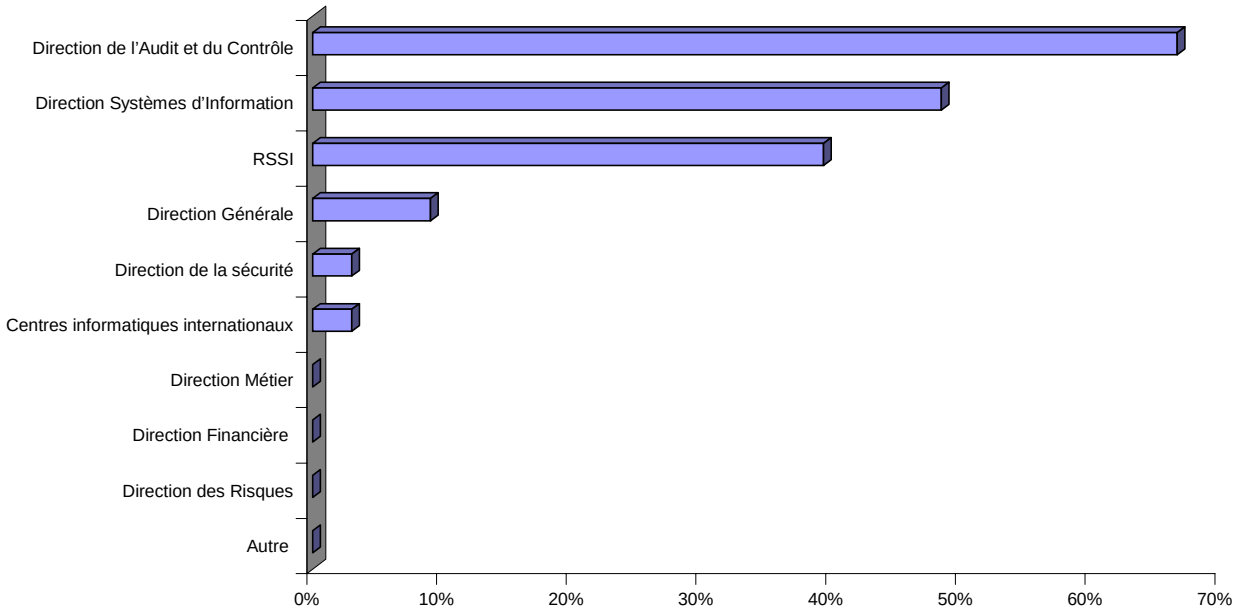
Source : Cigref 2002

Figure 11 : Qui définit les règles et les principes de votre politique de sécurité du système d'information ?



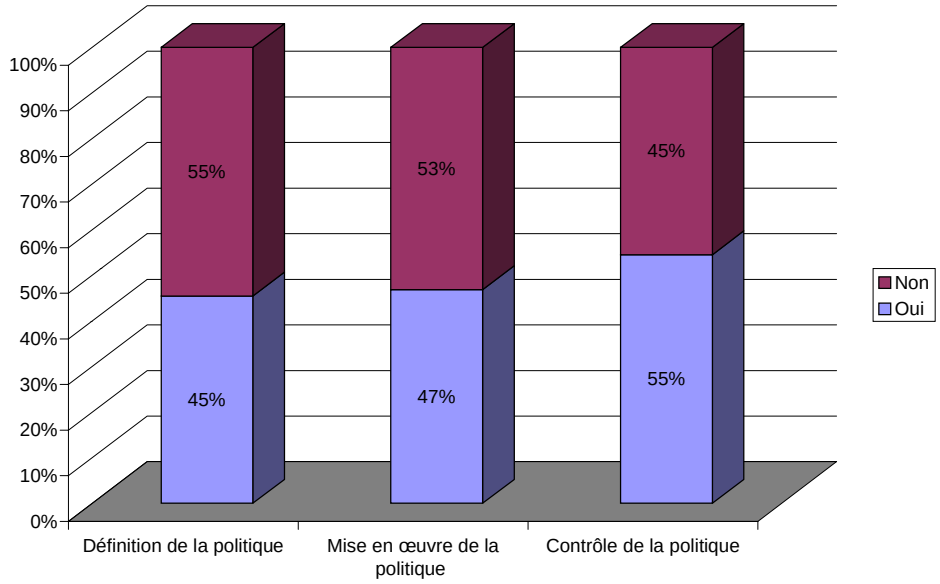
Source : Cigref 2002

Figure 12 : Qui met en œuvre la politique de sécurité du système d'information ?



Source : Cigref 2002

Figure 13 : Qui contrôle l'application de la politique de sécurité du système d'information ?



Source : Cigref 2002

Figure 14 : Faites-vous appel à un prestataire extérieur dans la définition, la mise en œuvre ou le contrôle de votre politique de sécurité ?

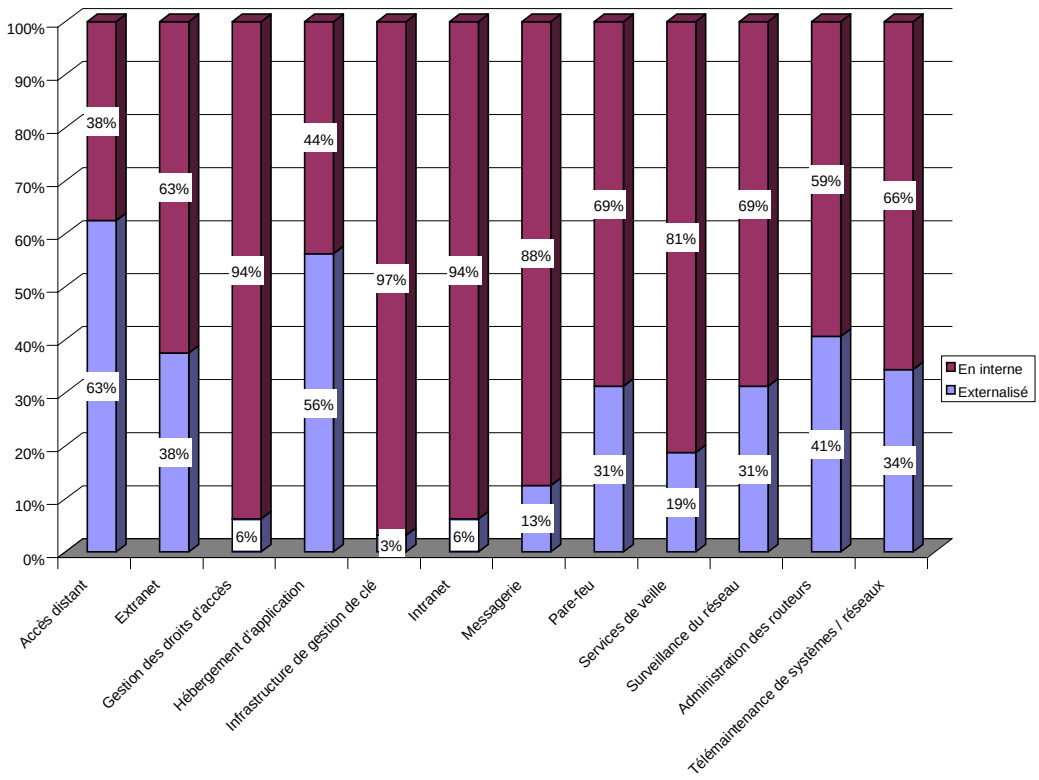
1.3 Quelle stratégie d'externalisation ?

Les grandes entreprises ont une stratégie d'externalisation, opportuniste mais relativement prudente en matière de sécurité. Le choix d'un prestataire doit s'accompagner d'une démarche de contrôle qualité.

Les principaux éléments gérés à l'extérieur sont les accès distants, les extranets, l'hébergement d'applications, l'administration de routeurs et des pare-feu, la télémaintenance des systèmes et du réseau.

La gestion des accès distants, des pare-feu, des routeurs et des extranets est majoritairement effectuée par les opérateurs. L'hébergement des applications et la fourniture de services de veille se fait surtout chez les SSII.

En revanche la gestion des droits d'accès, de la messagerie et des infrastructures à clé publique reste effectuée en interne.



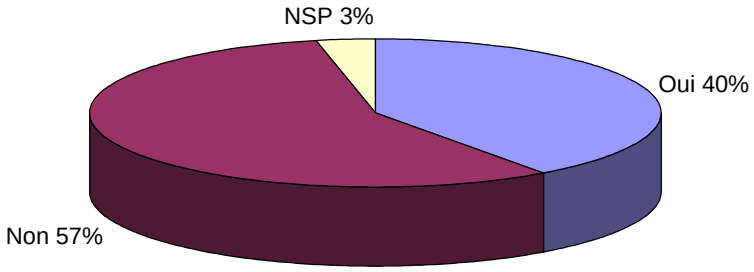
Source : Cigref 2002

Figure 15 : Quels sont les éléments de votre système d'information qui sont actuellement externalisés ?

Les critères de choix d'un prestataire de services de sécurité doivent notamment porter sur les points suivants :

- l'expérience du prestataire ;
- les compétences internes ;
- les technologies utilisées ;
- le délai de réaction ;
- le service de support ;
- la qualité de l'infrastructure de protection des serveurs de données ;
- les clauses contractuelles (l'engagement de résultat…) ;
- les services à valeur ajoutée (authentification, *monitoring*, gestion de bande passante) ;
- le partage des responsabilités légales ;
- etc.

La majorité des entreprises interrogées n'ont pas de nouveaux projets en matière d'externalisation. Pour les autres, parmi les nouveaux éléments susceptibles d'être externalisés, les entreprises citent l'administration des routeurs et des pare-feu, l'hébergement de site web et d'applications, la tierce maintenance applicative, la télémaintenance des systèmes et du réseau, la gestion des sauvegardes.



Source : Cigref 2002

Figure 16 : Envisagez-vous d'externaliser d'autres éléments ?

2. BILAN DES PRINCIPALES VULNÉRABILITÉS ET MENACES

2.1 Quelle sensibilité aux risques du système d'information ?

2.1.1 Des directions d'entreprise de plus en plus sensibilisées

La sécurité des services d'infrastructures, la sécurité des systèmes d'information et la sécurité de l'information font partie des préoccupations majeures des directeurs des systèmes d'information. Plusieurs facteurs sont à l'origine de cette prise de conscience :

- un facteur structurel, le développement d'internet ;
- un facteur conjoncturel, les attentats du 11 septembre ;
- un facteur exogène, le discours des fournisseurs ;
- un facteur endogène, la réalité du terrain dans les entreprises.

Le développement des nouveaux usages[6], l'ouverture du système d'information, l'explosion des attaques par internet, la multiplication des projets complexes de refonte de système d'information, l'essor de la mobilité intra et interentreprises et de l'accès distant, la mise en place d'architecture multi-tiers, l'arrivée des technologies sans fil, le développement des services de téléprocédure et de la télémaintenance sont autant de facteurs qui expliquent une prise en compte croissante de la dimension sécurité dans le management des systèmes d'information et la gestion de projets.

La majorité des responsables de la sécurité et des DSI des grandes entreprises interrogées par le Cigref considèrent que la direction générale est désormais suffisamment sensibilisée aux risques liés aux systèmes d'information.

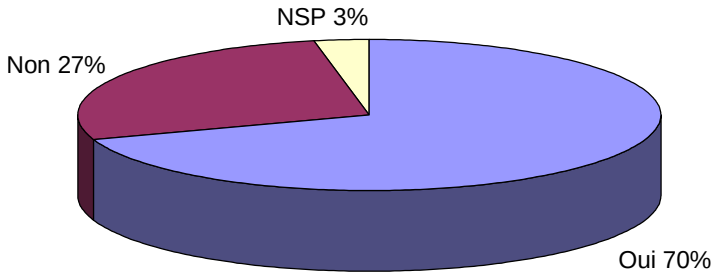
Inversement les préoccupations des DG en matière de sécurité portent principalement sur deux aspects :

- la gestion des risques ;
- le retour sur investissement.

On assiste donc à une convergence d'intérêt autour des approches de type *risk management*. En revanche les investissements en sécurité restent difficiles à justifier et restent perçus comme un poste à coût élevé.

[6] En particulier autour de la capitalisation de savoir-faire stratégiques métiers.

En l'espace de quelques années, on est passé d'un discours de la peur à un discours de la gestion des risques.



Source : Cigref 2002

Figure 17 : Estimez-vous que votre DG est suffisamment sensibilisée aux risques liés aux systèmes d'information ?

2.1.2 Comment justifier son budget sécurité ?

Une remarque préliminaire s'impose : est-il toujours nécessaire de justifier son budget ? La démarche est loin d'être simple en tout cas. Le budget sécurité n'est pas toujours isolé du reste du budget informatique.

Le budget sécurité est souvent visible au niveau de la holding pour répondre à des besoins fonctionnels (audit, conseil…).

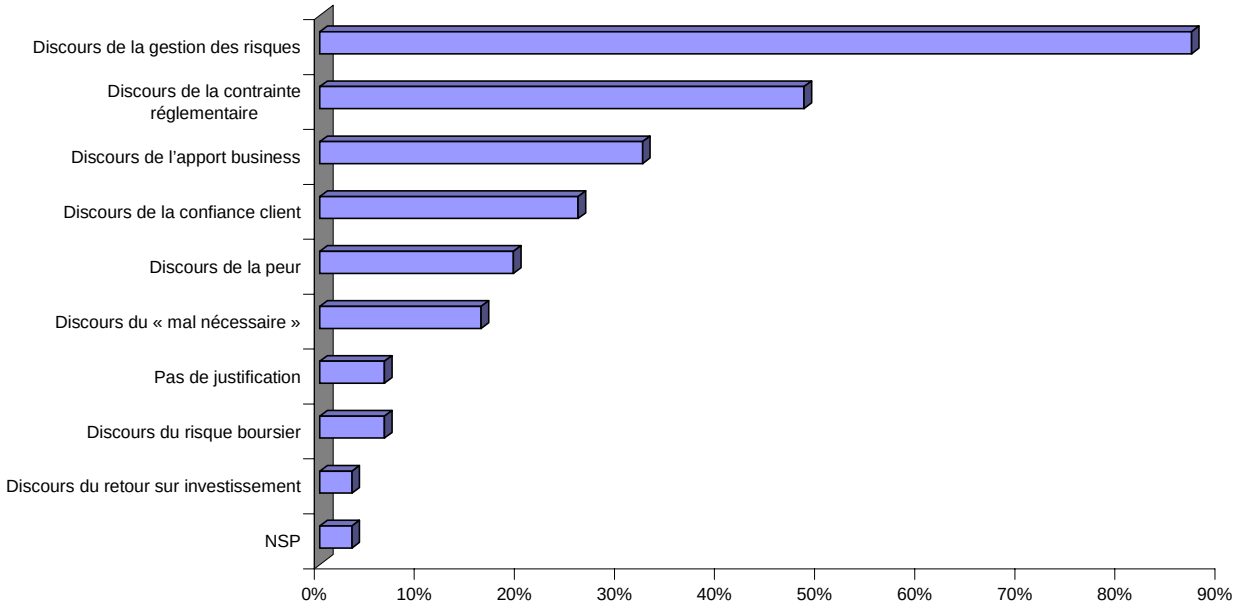
Au niveau d'une filiale ou d'un métier, là où les besoins sont plus opérationnels, le budget est souvent intégré dans des projets ou dans les budgets de production, d'exploitation ou de maintenance.

Les entreprises ne cherchent pas non plus forcément à le justifier, car la sécurité peut faire partie des dépenses d'infrastructures.

Les entreprises ont généralement tendance à utiliser plusieurs arguments, principalement le discours :

- de la gestion des risques ;
- de la contrainte réglementaire ;
- de l'apport *business*…

Les entreprises doivent chercher à formaliser davantage la métrique de rentabilité de leurs investissements sécurité, au moins sur les aspects qualitatifs et métiers.



Source : Cigref 2002

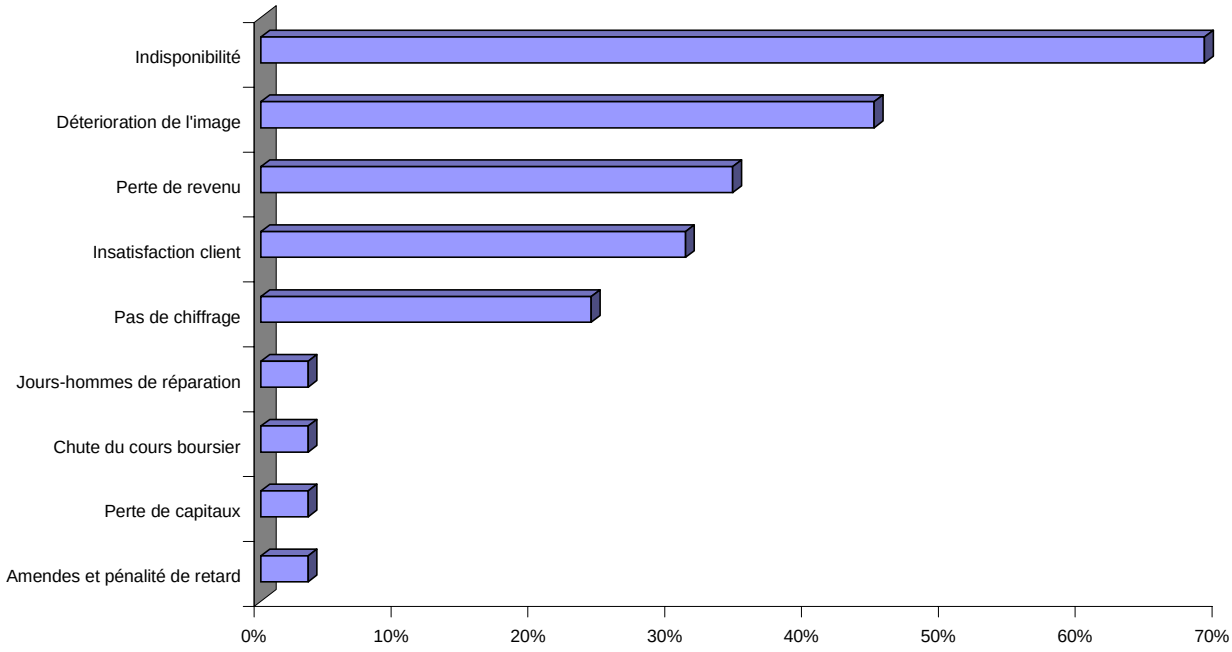
Figure 18 : Comment justifiez-vous votre budget sécurité ?

2.1.3 Comment chiffrer ses pertes ?

L'évaluation des pertes fait également partie des questions récurrentes.

Les entreprises ont souvent du mal à chiffrer leurs pertes dues à des attaques. De plus, même si elles tendent à se développer, les poursuites pénales sont encore loin d'être systématiques.

Le plus facile à chiffrer concerne l'indisponibilité d'une machine, la perte de revenu liée à un processus *business* (par exemple pour un site de vente en ligne). Le plus délicat à évaluer reste l'indisponibilité pour l'utilisateur, l'insatisfaction client, le lien entre l'attaque et la chute du cours boursier. Les directions métiers sont la plupart du temps associées à la démarche d'évaluation des préjudices en cas d'indisponibilité.



Source : Cigref 2002

Figure 19 : Comment évaluez-vous vos pertes dues à des défaillances du système de sécurité ?

Le tableau ci-dessous montre quelques exemples de coûts liés à une indisponibilité du système d'information. Le coût est d'autant plus élevé que le système d'information est au cœur du processus métier de l'entreprise (courtage, carte bancaire…).

Métier	Industrie	Coût d'une heure de panne
Courtage	Finance	$ 6,450,000
Carte de crédit	Finance	$ 2,600,000
Pay per view	Média	$ 150,000
Home Shopping	Distribution	$ 113,000
VPC	Distribution	$ 90,000
Réservation aérienne	Transport	$ 90,000
Vente de tickets	Media	$ 69,000
Livraisons	Transport	$ 28,000
Distributeurs	Finance	$ 14,500

Source : Fiber Channel Association

Figure 20 : Perte liée à une indisponibilité.

Analyse par année

Year	Worldwide Economic Impact ($ US Billion)
2001	13.2
2000	17.1
1999	12.1
1998	6.1
1997	3.3
1996	1.8
1995	0.5

Analyse par incident

Year	Code Name	Worldwide Economic Impact ($ US Billions)	Cyber Quake Rating
2001	Nimda	0.635	0.73
2001	Code Red(s)	2.62	2.99
2001	Sircam	1.15	1.31
2000	LoveBug	8.75	10.00
1999	Melissa	1.10	1.26
1999	Explorer	1.02	1.17

Source : Computer Economics

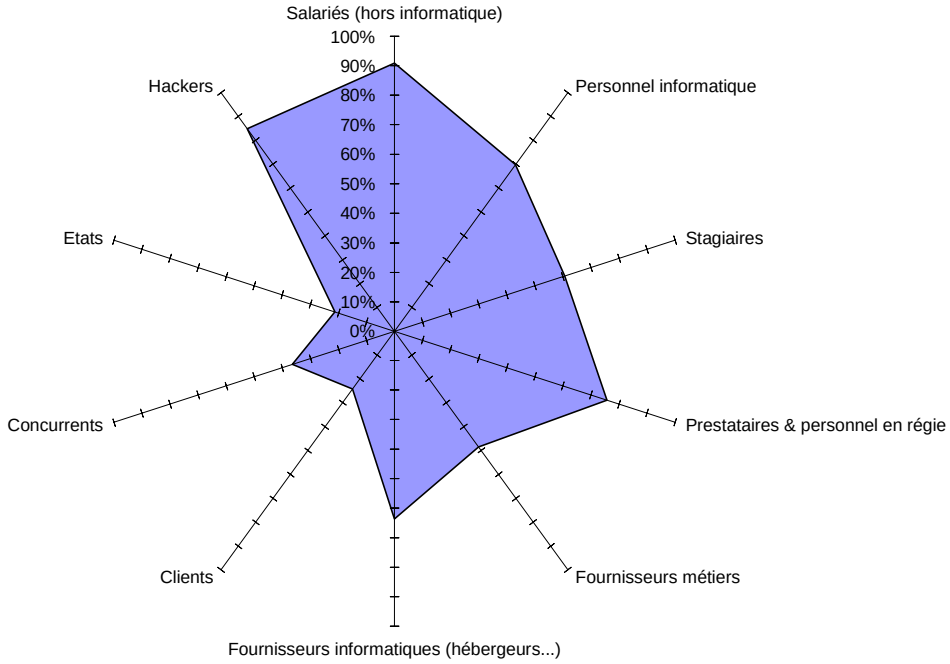
Figure 21 : Perte liée à une attaque virale.

2.2 Comment évaluer ses risques ?

2.2.1 À l'origine des menaces : *salariés et* hackers

Les personnes les plus citées comme étant à l'origine des menaces sont les salariés et les *hackers*. Les États ont parfois une influence en matière d'intelligence et de sécurité économique. Cette influence semble ici sous-estimée. De même, le rôle des concurrents comme source de menace semble sous-évalué. Inversement, les résultats montrent que l'on a tendance à surestimer le risque lié aux stagiaires et aux fournisseurs informatiques.

Les salariés sont à l'origine des vols, des pannes internes, des erreurs d'utilisation, tandis que les *hackers* sont souvent les instigateurs des attaques virales, des attaques internet, des dénis de service... Les concurrents peuvent jouer un rôle dans les campagnes de désinformation.



Source : Cigref 2002

Figure 22 : Selon vous, d'où viennent les principales menaces ?

2.2.2 La principale menace : les attaques virales

Les responsables de la sécurité sont aujourd'hui confrontés aux enjeux suivants :

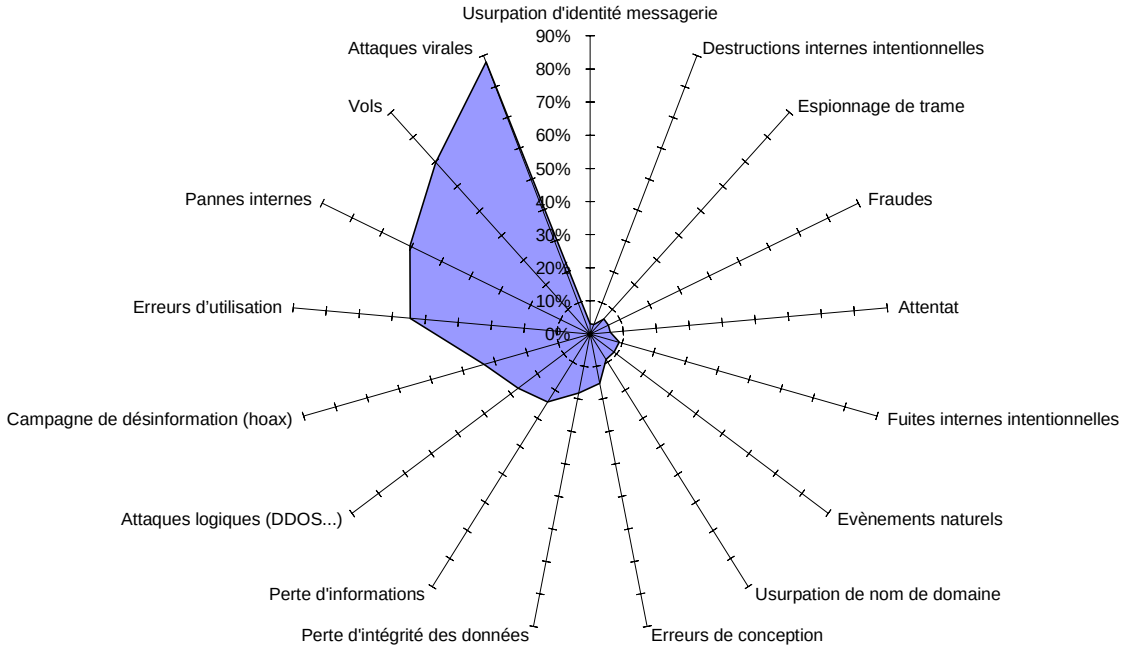
- complexité des systèmes d'information ;
- complexification des attaques ;
- prolifération des attaques.

Les principales zones de fragilité perçues par les RSSI se situent autour de l'accès à internet, des applications critiques, de l'accès distant, de l'intranet et des annuaires. Les chiffres issus des enquêtes annuelles du Cigref, du Clusif et du CSI (Computer Security Institute) du FBI, concordent.

Au palmarès des attaques subies en 2001 figurent en première ligne les attaques virales, les vols, les pannes internes et les erreurs d'utilisation.

Viennent ensuite les campagnes de désinformation (canulars ou *hoaxes*), les attaques par déni de service (DOS et DDOS), les pertes d'information et les pertes d'intégrité de données. Les fraudes, l'espionnage de trames et les destructions intentionnelles restent peu mentionnés.

Il faut nuancer le propos par deux remarques : il s'agit des attaques connues et déclarées par les RSSI. Or l'on sait très bien qu'il y a en fait beaucoup plus d'attaques non détectées : seules 10 % des attaques seraient connues des victimes.

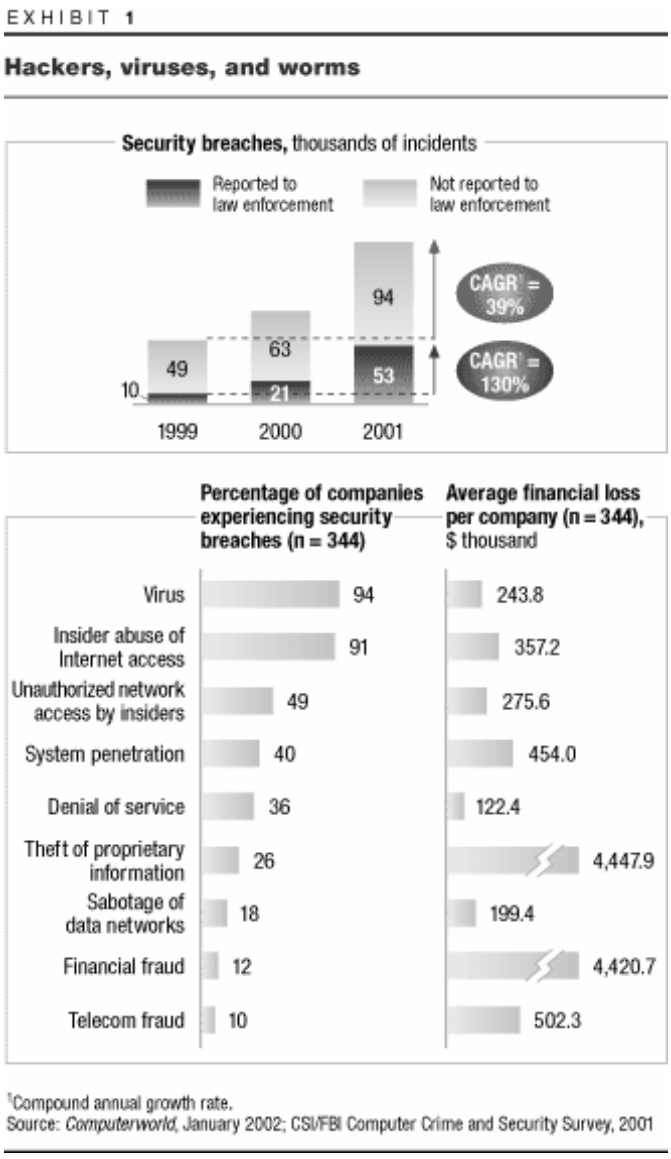


Source : Cigref 2002

Figure 23 : Quelles atteintes à la sécurité avez-vous subies en 2001-2002 ?

Les résultats de l'enquête menée chaque année par le CSI et le FBI auprès des grandes entreprises, agences gouvernementales, et universités américaines permettent de dégager plusieurs tendances significatives :

- les attaques les plus fréquentes ne sont pas nécessairement les plus coûteuses ;
- les attaques les plus fréquentes restent les attaques virales et celles commises via les connections internet ;
- les attaques les plus coûteuses sont les vols d'informations, les fraudes financières et les fraudes sur les autocommutateurs ;
- le nombre d'attaques déclarées aux autorités judiciaires tend à augmenter.



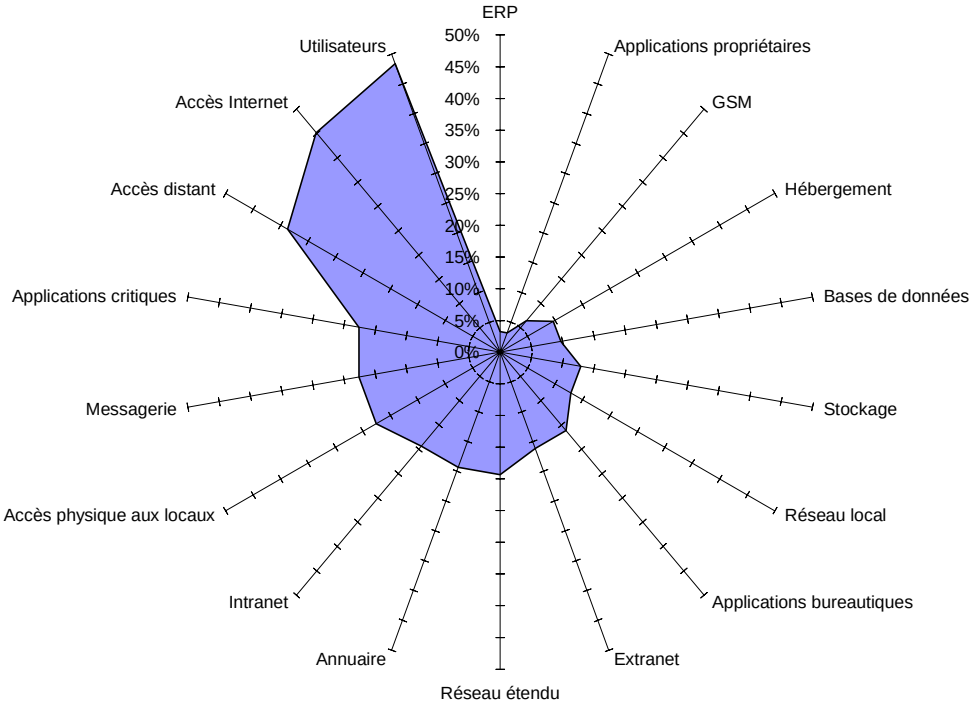
Source : CSI/FBI

Figure 24 : Évolution des attaques et des pertes financières des entreprises américaines (1999-2001).

Parmi les zones de fragilité citées par les responsables de la sécurité, on peut mentionner en premier lieu l'utilisateur qui constitue encore le « maillon faible » de la politique de sécurité.

Viennent ensuite les infrastructures d'accès à internet, d'accès distant puis les applications critiques et la messagerie.

Les bastions jugés les plus solides semblent être les applications propriétaires, les GSM, l'hébergement, les bases de données, le stockage.



Source : Cigref 2002

Figure 25 : Quelle(s) partie(s) de votre système d'information jugez-vous la plus fragile ?

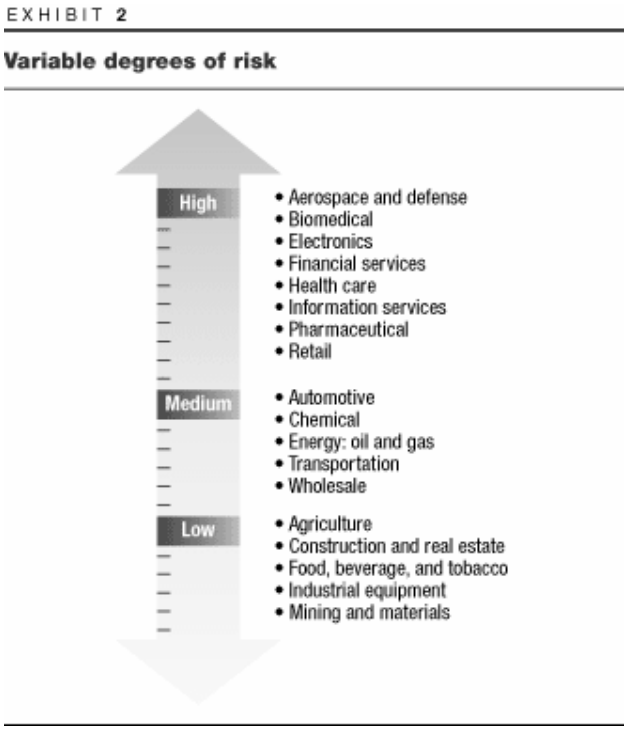
2.3 Comment gérer ses risques ?

La cartographie des risques internes et externes liés au système d'information est une démarche préalable indispensable dans le cadre d'une politique de sécurité.

Les risques liés au système d'information peuvent revêtir une multitude de formes. Ce sont en effet à la fois :

- des risques internes et externes ;
- des risques matériels et immatériels ;
- des risques organisationnels, humains, juridiques, techniques ;
- des risques liés aux personnes, aux procédures, aux protocoles et aux matériels ;
- des risques prévisibles ou imprévisibles ;
- des risques maîtrisables ou non.

Les risques varient également selon le secteur d'activité de l'entreprise, sa taille, son image de marque et son degré de dépendance vis-à-vis de son système d'information.



Source : McKinsey

Figure 26 : Degré d'exposition au risque du système d'information par secteur d'activité.

Les risques liés au système d'information sont désormais des risques identifiés au même titre que les autres risques de l'entreprise (risque métier, risque social, risque environnemental, risque pays…).

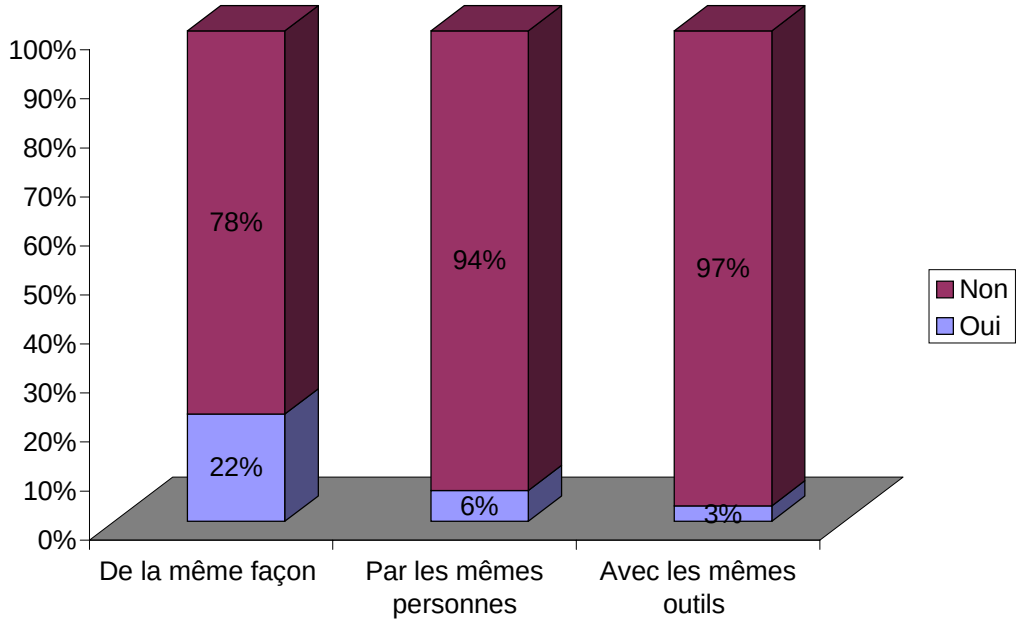
Mais le risque système d'information n'est pas encore traité de la même façon, par les mêmes personnes et avec les mêmes outils que les autres risques de l'entreprise.

Le RSSI doit se rapprocher du *risk manager* lorsqu'il existe ou en tout cas chercher à développer une culture de *risk management*.

Certains secteurs, le secteur bancaire notamment, pour des raisons de réglementation sectorielle et de règles prudentielles, commencent néanmoins à développer des passerelles entre les risques opérationnels (système d'information…) et les risques métiers (risques de crédit…).

Le Comité de Bâle a proposé pour le secteur bancaire, en 2001, une prise en compte des profils de risques individuels pour le calcul d'un nouveau ratio Cooke. Pour mémoire, l'accord de 1988 définissait un niveau de fonds propres minimum égal à 8 % des actifs pondérés détenus par un établissement.

Ce taux de 8 % n'a pas été modifié, en revanche les modalités de détermination de l'assiette font l'objet d'une refonte complète avec la prise en compte des notations externes, la reconnaissance des systèmes de notations internes, la prise en compte non seulement des risques de crédit mais aussi des risques opérationnels, et une reconnaissance plus importante des techniques de réduction des risques. Le nouveau système doit entrer en vigueur en 2005.



Source : Cigref 2002

Figure 27 : Comment gérez-vous les risques liés au système d'information par rapport aux autres risques de l'entreprise ?

La « cyndinique », ou science du risque, discipline développée par l'École des Mines, permet apporter une grille d'analyse utile pour déterminer les vulnérabilités d'une organisation face à une agression sur son patrimoine informationnel. On constate souvent que les vulnérabilités se produisent suite à l'apparition de déficits d'ordre culturels, organisationnels ou managériaux.

Parmi les déficits culturels, on peut citer la culture de l'infaillibilité, la culture du simplisme, l'absence de communication, la culture du nombrilisme. Au titre des déficits

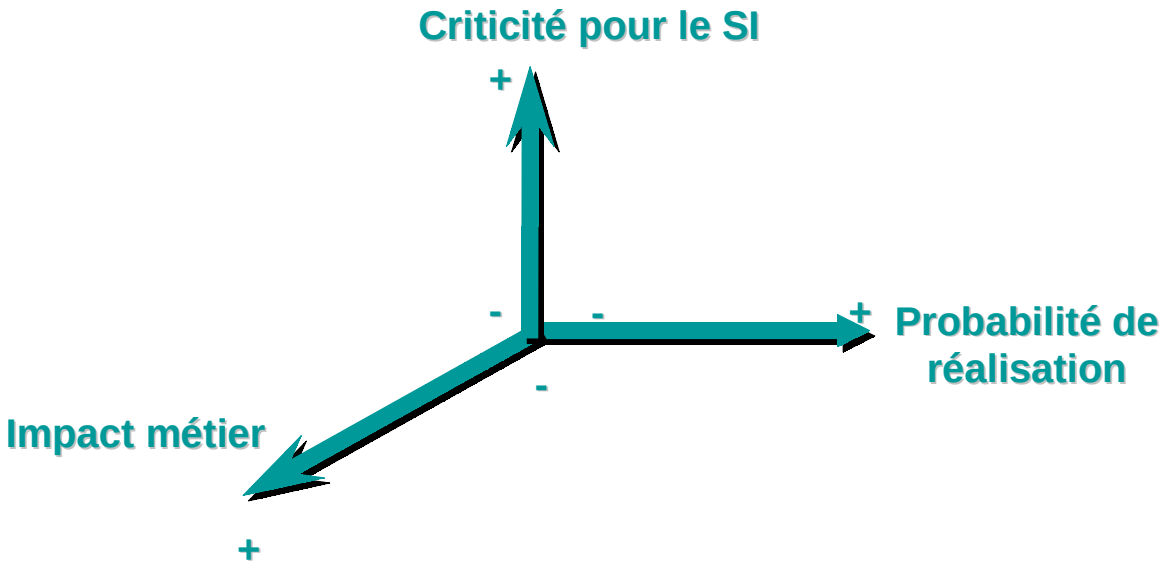
organisationnels figurent la subordination de la sécurité de l'information à d'autres fonctions de gestion créatrices de risques (marketing…), la dilution des responsabilités. Parmi les déficits managériaux, on peut citer l'absence d'un système de retour d'expérience, l'absence d'une méthode de sécurité de l'information dans l'organisation, l'absence d'un programme de formation, l'absence de planification des situations de crise.

Le RSSI peut s'appuyer également sur des méthodes d'analyse de risques (Marion, Melisa, Mehari, Ebios…) pour identifier le risque, le résoudre, le couvrir, le réduire ou le transférer.

Une politique de gestion des risques implique de cartographier les risques, de les classer par degré de fréquence et de gravité, et de décider de la façon dont le risque doit être géré.

Les risques peuvent être classés selon plusieurs axes :

- la criticité pour le système d'information ;
- la probabilité de réalisation ;
- l'impact sur les métiers.



Source : Cigref 2002

Figure 28 : Classification des risques.

Une politique de gestion des risques revient à choisir entre quatre options :

- accepter le risque ;
- gérer le risque ;
- transférer le risque ;
- rejeter le risque.

.

	Actes non volontaires		**Actes volontaires**	
	Utilisateur non privilégié	*Utilisateur privilégié*	*Utilisateur non privilégié*	*Utilisateur privilégié*
Externe	Risque faible	Risque faible à moyen	Risque faible à moyen	Risque élevé
Interne	Risque faible à moyen	Risque moyen	Risque élevé	?

Source : Computer Associates

Figure 29 : Exemple de matrice de gestion des risques.

L'objectif d'une politique de gestion des risques est de préserver le patrimoine de l'organisation afin d'assurer la bonne continuation de son activité, ce qui suppose de définir les domaines dans lesquels il sera nécessaire de prendre des mesures, d'identifier les moyens à mettre en œuvre, de les traduire en moyens techniques, organisationnels, humains et de fournir les moyens de pilotage.

L'analyse des risques a pour objectif de réduire le volume initial du risque et d'aboutir à un risque résiduel.

L'analyse des risques doit se faire selon trois axes :

- les ressources ;
- les menaces ;
- les vulnérabilités.

La démarche à suivre est la suivante :

- identifier et valoriser le patrimoine de l'entreprise ;
- identifier et valoriser les ressources critiques de l'entreprise ;
- définir les propriétés et les responsabilités ;

- identifier les menaces ;
- définir les priorités ;
- définir la méthode ;
- définir les moyens.

L'identification et l'évaluation de la valeur du patrimoine informationnel de l'entreprise est vital dans une démarche de *risk management*.

En conclusion, la politique de gestion des risques intervient en amont de la politique de sécurité mais ne doit pas priver l'entreprise d'une réflexion sur les processus, les personnes et les outils.

Une démarche de *risk management* ne constitue qu'une partie d'une politique globale de sécurité.

3. LE CHOIX DES NORMES, OUTILS ET MÉTHODES

3.1 Les normes et méthodes : une démarche indispensable ?

L'abondance des normes et méthodes est souvent source de confusion et d'embarras. Pourtant le choix d'une ou plusieurs normes et méthodes d'organisation ou d'évaluation de la sécurité s'avère indispensable pour mettre en place une politique de sécurité cohérente, homogène et efficace au sein d'une entreprise, *a fortiori* lorsqu'il s'agit d'un groupe décentralisé, multi-métiers, et international.

Selon Intrinsec, la norme (qui peut être organisationnelle ou technique) a un objet souvent très vaste, s'appuie généralement sur des concepts ou des notions générales. Le champ d'application de chaque concept doit alors être précisé, pour que la norme puisse être appliquée efficacement.

La méthode est un moyen d'arriver efficacement à un résultat souhaité, précis. Ce souhait étant souvent formulé dans une norme, on voit que souvent la méthode sera l'outil utilisé pour satisfaire à une norme.

3.1.1 Pourquoi choisir une norme et une méthode ?

Le choix d'une norme ou d'une méthode de sécurité présente un certain nombre d'avantages :

- obtenir une vision globale et cohérente de la sécurité ;
- fournir un référentiel et des concepts communs à tous les acteurs, permettant les audits de ce référentiel ;
- fournir un cadre commun pour gérer les risques ;
- proposer des parades adaptées aux risques ;
- améliorer la sensibilisation des utilisateurs ;
- prendre en compte la sécurité dans la gestion des projets ;
- favoriser la démarche qualité ;
- éventuellement faire baisser le coût des assurances.

3.1.2 Typologie des normes et méthodes

On peut dresser plusieurs typologies des normes et méthodes de sécurité des systèmes d'information. À titre d'exemple, on citera la classification construite par la DCSSI (Direction centrale de la sécurité des systèmes d'information) et celle élaborée par Intrinsec.

La DCSSI distingue d'un côté les « catalogues SSI » et de l'autre les « méthodes SSI ».

Le terme « catalogue SSI » est employé pour tous les recueils de mesures, d'exigences, de vulnérabilités ou autres éléments sans démarche méthodologique. Parmi ceux-ci, on peut citer :

- les bonnes pratiques et mesures de sécurité : IT Baseline Protection Manual (BSI allemand), ISO 17799, ISO 13335, ACSI 33 (DSD australien), CM 5515 (Otan) ;
- la politique de sécurité : PSI (DCSSI), ISPME (CSE canadien), RFC 1244 (IETF)...
- les catalogues pour l'évaluation de produits :TCSEC (DoD américain), ITSEC (CEE), ISO 15408…
- les catalogues spécifiques : sécurité des réseaux : MG-1 (CSE canadien), sécurité des sites : RFC 2196 (IEFT), sécurité des interconnexions : AC35-D/1027 (OTAN), modèle de maturité SSI : SSE-CMM (ISSEA) ;

Le terme de « méthode SSI » désigne quant à lui les démarches de sécurité reposant sur une méthode. Parmi celles-ci, on peut citer :

- les méthodes contribuant à la gestion du risque SSI : Ebios (DCSSI), Marion, Mehari (Clusif), MV3 (CF6), Cramm (CCTA anglais), Ninah (XP CONSEIL), Risk Management Guide, MG-2 (CSE canadien), SP800-30 (NIST), IAM (NSA), Buddy System (Countermeasures Corp.)...
- les méthodes d'audit ou contrôle interne SSI : Massia (DGA), ERSI (Forum des compétences), IPAK (CSI), SP800-26 (NIST)...
- les méthodes d'intégration de la SSI dans les projets : DSIS (DCSSI), Incas (Clusif), Orion (Cersiat)...
- les méthodes globales incluant des aspects SSI : Cobit…
- les guides de rédaction : Feros, SSRS, SP800-18…
- les autres méthodes : Domaines spécifiques : Messedi, Muse…

Le cabinet de conseil Intrinsec distingue quant à lui d'un côté les normes et de l'autre les méthodes

Parmi les normes, on peut distinguer :

- les normes internationales organisationnelles : les GMITS, Guidelines for the management of IT Security, (ISO/IEC TR 13335) la norme ISO/IEC 17799 (Code of practice for information security management) en phase de révision, issu de la norme britannique BS 7799 Part 1 – 1999 ;
- les normes internationales techniques : la norme ISO/IEC 15408 (Evaluation criteria for IT security) (cette norme est tirée des « *common criteria* »), ISO/IEC WD 15947 (norme en cours de discussion, portant sur le cadre des détections d'intrusions) ;
- les normes internationales de diagnostic et de qualité : ISO/IEC 19011 (Audit), ISO 9004 (Qualité) ;
- les normes nationales organisationnelles : BS 7799-1 (Code of practice for information security management, élaborée par le British Standard Institute, à l'origine de la norme ISO/IEC 17799) ;
- les normes nationales d'évaluation : BS 7799-2 (Specification for information security management systems, élaborée par le British Standard Institute).

Parmi les méthodes, on peut citer :

- les méthodes françaises : Marion, Mehari, Melisa ;
- les méthodes étrangères : Cobit, Cramm 4.

Enfin, dans le cadre des critères communs ITSEC, la DCSSI a développé différentes méthodes, utilisées principalement dans les ministères :

- politique de sécurité interne (PSI) ;
- développement de systèmes d'information sécurisés (DSIS) ;
- expression des besoins et identification des objectifs de sécurité (Ebios) ;
- fiche d'expression rationnelle des objectifs de sécurité (Feros) des systèmes d'information ;
- Réalisation des objectifs de sécurité par le choix des Fonctions (Roscof) ;
- guides d'aide à la rédaction des fournitures pour l'évaluation (Garde).

Le schéma ci-dessous dresse le panorama des méthodes développées et normalisées à travers le monde en matière de sécurité soit par les gouvernements et les associations ou les entreprises.

Source : DCSSI

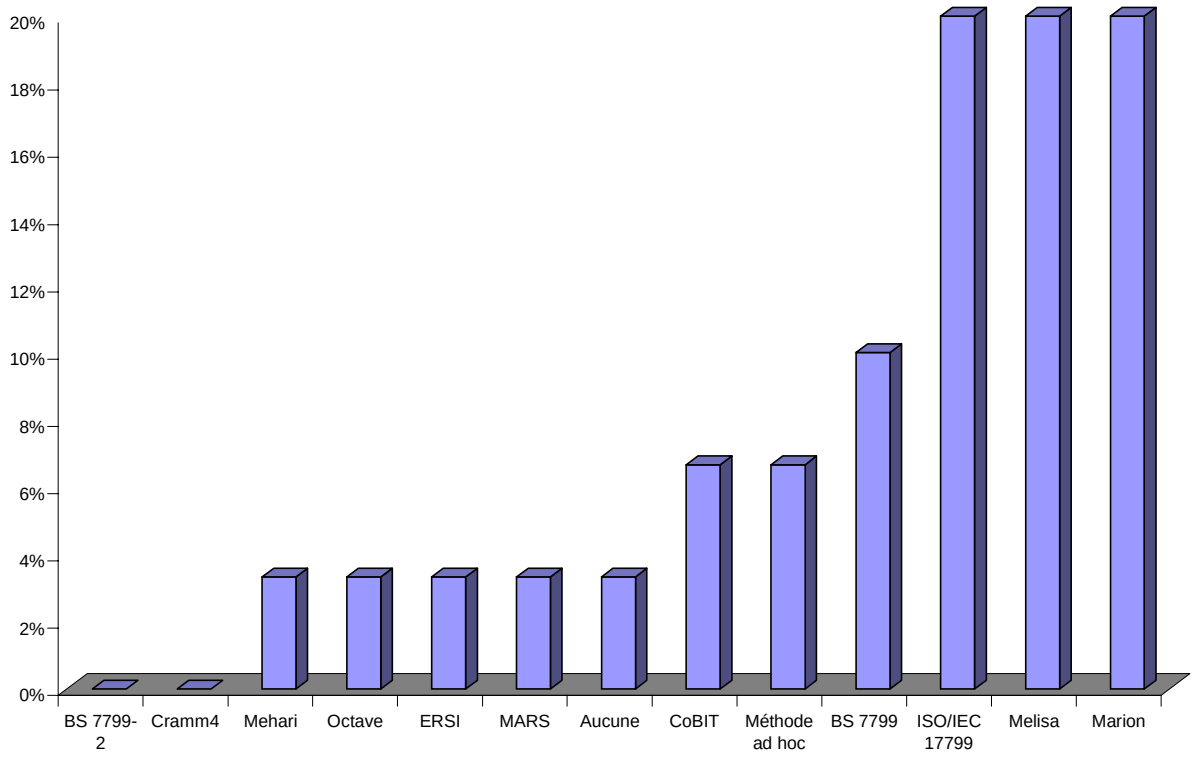
Figure 30 : Cartographie des principales méthodes SSI dans le monde.

3.1.3 Quelle norme et méthode choisir ?

La majorité des entreprises interrogées déclarent utiliser au moins une norme ou une méthode pour la définition, la mise en œuvre ou le contrôle de leur politique de sécurité.

Parmi les normes et méthodes les plus fréquemment utilisées on peut citer Marion, Melisa et ISO/IEC 17799 / BS 7799.

Certaines entreprises préfèrent au contraire développer une méthodologie *ad hoc*, plus spécifique, donc mieux adaptée à leurs besoins mais aussi plus difficile à entretenir et à faire évoluer.



Source : Cigref 2002

Figure 31 : Quelles normes et méthodes d'organisation et d'évaluation de la sécurité du système d'information utilisez-vous ?

Retenir une norme ou une méthode est un choix souvent structurant et de long terme pour l'entreprise concernant le coût, les ressources et l'organisation.

L'entreprise doit faire au préalable une analyse fine de ses besoins, de l'adéquation des méthodes existantes à ses besoins et de ses ressources disponibles.

Parmi les critères de choix à retenir, on peut citer :

- l'objectif de la méthode ;
- le niveau d'abstraction ;
- le degré de couverture par domaine ;
- le caractère standard ou non de la méthode ;
- le caractère récent ou non de la méthode ;
- le caractère stable ou non de la méthode ;
- le caractère transversal au système d'information ou non de la méthode (cf. Cobit) ;
- le degré de diffusion de la méthode ;
- le niveau de souplesse et d'adaptation possible ;

- l'« auditabilité » de la méthode ;
- la facilité de mise en œuvre ;
- le coût d'acquisition ;
- le coût de déploiement ;
- le coût d'entretien ;
- l'implication de l'organisme dans la maintenance de la méthode.

Le choix d'une méthode s'avère nécessaire mais pas suffisant. En effet, la méthode ne doit pas servir d'alibi ni masquer les insuffisances budgétaires, les erreurs techniques, les lacunes organisationnelles ou les défaillances humaines.

On peut parfaitement combiner une norme et une méthode entre elles. Par exemple, il est possible de concilier des méthodes de type Mehari, Cramm et Cobit avec des normes plus générales comme ISO/IEC 17799 ou BS 7799-2000 Part 2.

Dans un cadre international, il est préférable de suivre une seule norme internationale pour assurer la sécurité de son système d'information de façon cohérente dans tous les pays. Il ne semble pas nécessaire pour autant d'imposer une méthode unique à l'ensemble des filiales de l'entreprise.

L'un des enjeux actuels en matière de normalisation au sein de l'ISO est de « transformer » des méthodes ou normes nationales en normes ISO internationales (cf. le cas de la BS 7799).

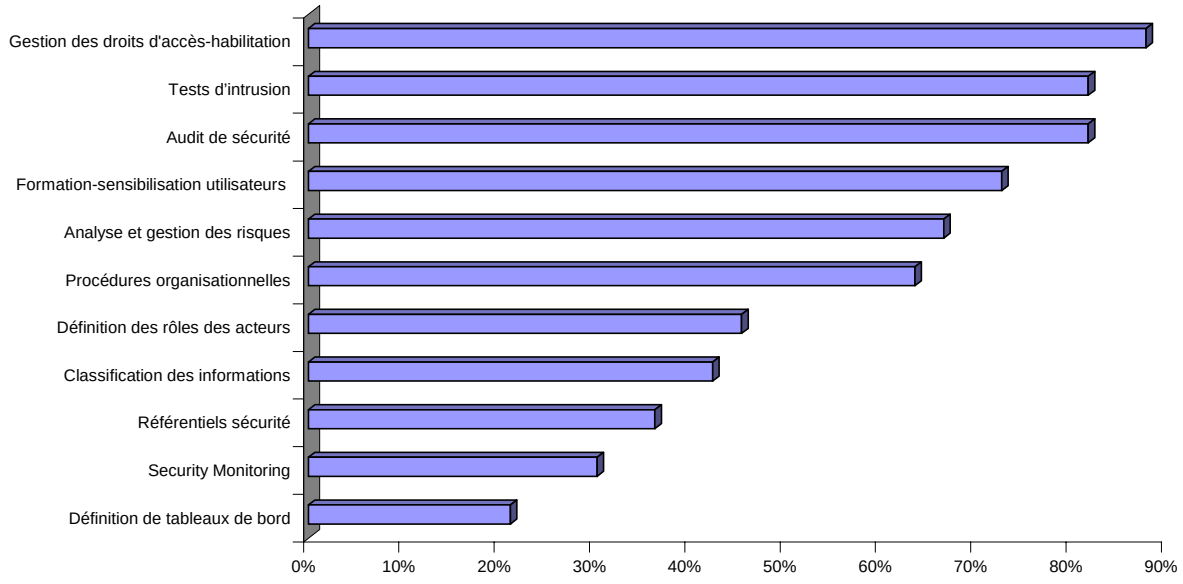
Le Cigref soutient à ce propos le Clusif dans sa démarche de normalisation de la méthode Mehari et de compatibilité avec les normes BS 7799 et ISO/IEC 17799.

3.2 Les principaux éléments d'une politique de sécurité

3.2.1 Quelle politique de sécurité ?

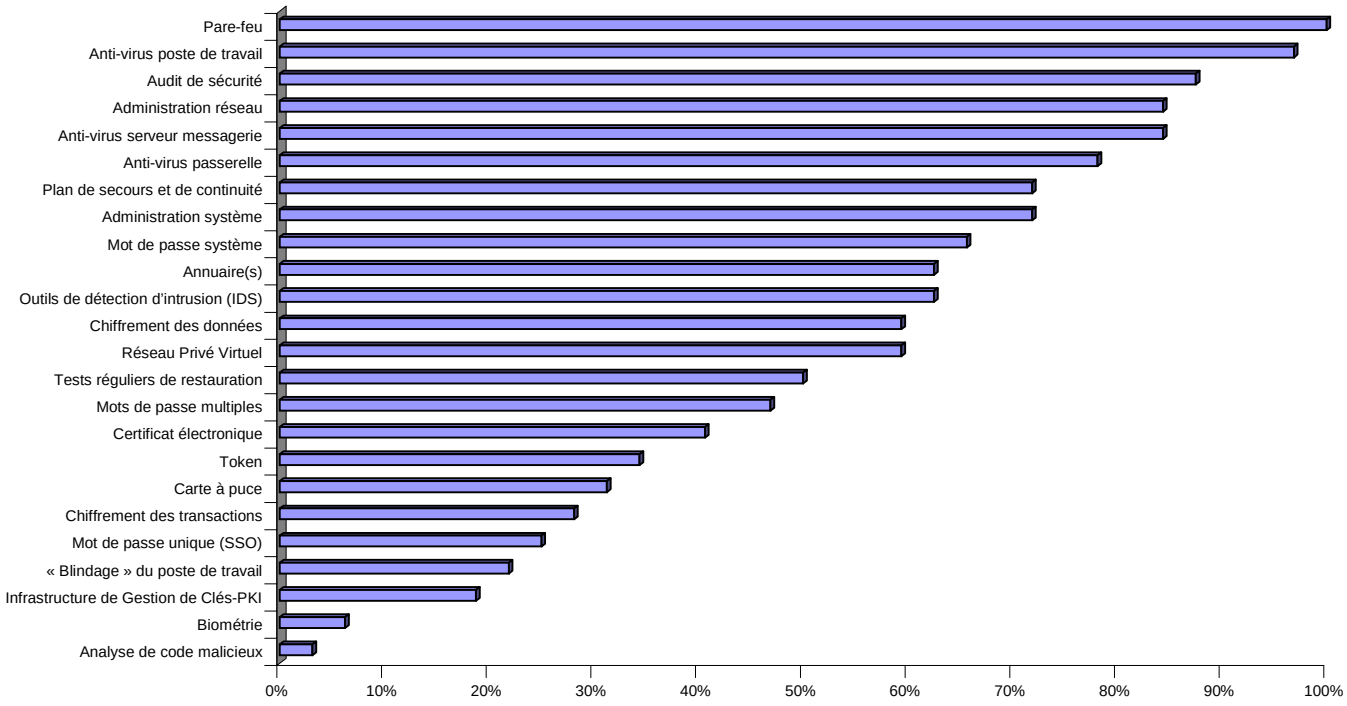
La politique de sécurité doit prévoir un schéma organisationnel de sécurité, s'appuyer sur des normes, des processus, des personnes et combiner plusieurs outils. Parmi les moyens employés, on peut citer :

- la protection par les règles (classifier l'information) ;
- la protection par les outils (chiffrement…) ;
- la protection par les contrats (clauses, obligations, SLA…) ;
- la protection par l'identification (tatouage, marquage, copyright) ;
- la protection par le dépôt (marques, brevets, droit d'auteur) ;
- la protection par l'assurance (polices, exclusions…).



Source : Cigref 2002

Figure 32 : Parmi les éléments suivants, quels sont ceux utilisés dans votre politique de sécurité ?



Source : Cigref 2002

Figure 33 : Quels outils utilisez-vous ? (plusieurs réponses possibles).

La sécurité exige une protection en profondeur, à plusieurs niveaux, tant en interne qu'en externe.

Le panorama des solutions actuelles montre une approche insuffisamment intégrée, un manque de cohérence dans la capacité d'administration et de *monitoring* de la sécurité, une pénurie d'experts sur le marché.

3.2.2 Quelques recommandations

Sans nécessairement considérer cela comme un guide des bonnes pratiques, on peut d'ores et déjà extraire des réunions du groupe sécurité du Cigref un certain nombre de grands principes :

- le principe de précaution ;
- le principe de coopération ;
- le principe d'économie ;
- le principe de séparation des pouvoirs.,

On peut également formuler un certain nombre de recommandations :

- la désignation de « propriétaires » métiers de l'information ;
- la délégation des droits ;
- le développement de moyens de surveillance ;
- l'existence d'une cellule de crise ;
- la définition ou l'actualisation d'un plan de continuité ou de reprise ;
- la présence d'un comité de sécurité informatique ;
- la prise en compte des aspects organisationnels ;
- la prise en compte de la législation en vigueur ;
- la sensibilisation des acteurs.

L'OCDE a rendu public en juillet 2002 ses nouvelles lignes directrices en matière de sécurité des systèmes d'information. Ce document constitue une réactualisation des travaux de 1992. L'organisation a identifié neuf principes fondamentaux en matière de sécurité :

- sensibilisation ;
- responsabilité ;
- réaction ;
- éthique ;
- démocratie ;
- évaluation des risques ;
- conception et mise en œuvre de la sécurité ;
- gestion de la sécurité ;
- réévaluation.

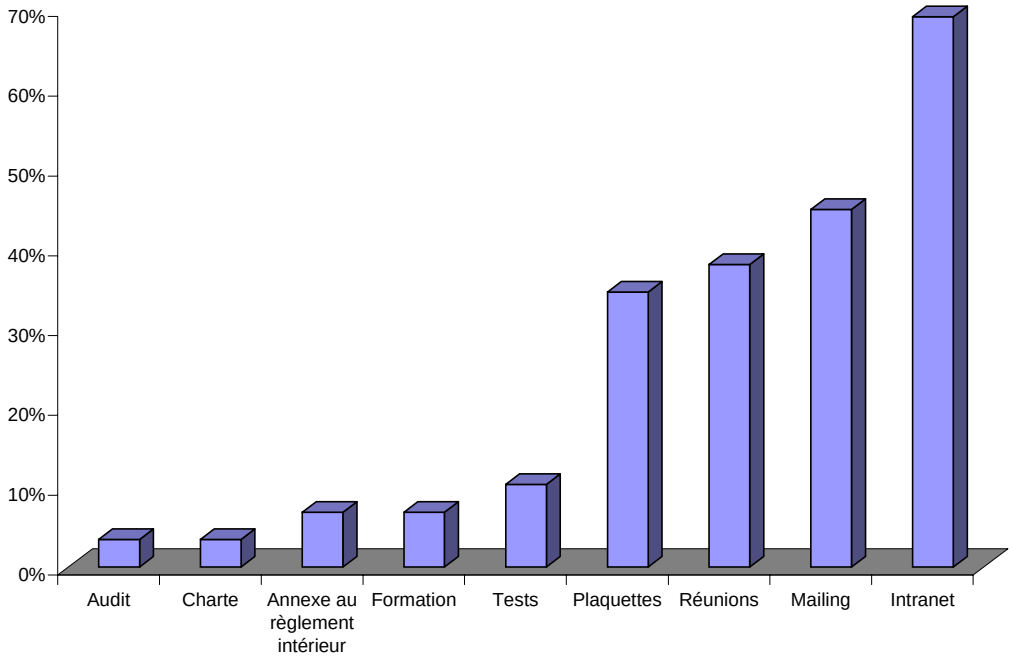
3.3 L'importance de la sensibilisation

La sécurité est d'autant plus efficace qu'elle est « admise » « diffuse » et par l'ensemble des acteurs de l'entreprise. L'utilisateur, le client, l'administrateur sont tous potentiellement à des degrés divers les « maillons faibles » du système d'information.

Une politique de sensibilisation s'impose avec des « piqûres de rappel » fréquentes, de manière à garantir un niveau de sécurité optimal dans le temps.

Parmi les outils de sensibilisation utilisés on peut citer les intranets, le courrier électronique, les réunions, les plaquettes d'information.

De manière plus résiduelle, les entreprises utilisent les tests et audits et peuvent avoir recours à des annexes au règlement intérieur ainsi qu'à des chartes.



Source : Cigref 2002

Figure 34 : Quels outils utilisez-vous pour sensibiliser vos utilisateurs ?

3.4 Mettre en place un pilotage

Le management global de la sécurité doit s'appuyer fortement sur la notion de pilotage. La mise en place de tableaux de bord constitue un instrument clé du pilotage et du suivi de la sécurité.

La pratique des tableaux de bord de sécurité reste encore peu développée dans les grandes entreprises françaises (cf. figure 30).

Deux approches du tableau de bord peuvent être retenues :

- une approche descendante : indicateurs de type stratégique et de suivi du référentiel de sécurité ;
- une approche ascendante : indicateurs opérationnels synthétisant les pratiques efficaces et les données faciles à collecter.

La mise en place d'un tableau de bord est encore loin d'être systématique au sein des grandes entreprises. La culture de *reporting* doit être renforcée. Mais il est vrai que les indicateurs restent difficiles ou trop nombreux à définir, à collecter et à entretenir. De plus il existe un décalage entre les outils disponibles sur le marché et ce que les responsables de la sécurité veulent mesurer. Les indicateurs internes doivent être complétés par des indicateurs externes sur l'image, la visibilité et la notoriété de l'entreprise.

L'historique est un élément déterminant pour la pertinence d'un tableau de bord. Enfin le facteur humain est essentiel à la fois en amont pour l'alimentation du tableau de bord et en aval pour l'interprétation des résultats.

4. LA MONTÉE EN PUISSANCE DES ENJEUX JURIDIQUES

4.1 La responsabilité pénale du DSI

Les personnes interrogées sont également de plus en plus conscientes de la responsabilité pénale des acteurs en cas d'attaques ou de sinistralité. Au premier rang, la responsabilité pénale du PDG ou de la direction générale apparaît[7].

Par le biais des mécanismes de délégation, la responsabilité pénale du directeur des systèmes d'information, voire du RSSI ou de l'administrateur messagerie est de plus en plus évoquée.

La personne qui reçoit la délégation doit avoir la compétence, l'autorité et les moyens nécessaires pour exercer cette délégation.

Les biens informatiques peuvent en effet être soit l'objet d'une fraude, soit le moyen d'une fraude. Parmi les atteintes, on peut citer :

- Les atteintes aux données : l'information n'est pas protégée en tant que tel, c'est le support qui est protégé. Les atteintes sont protégées par la législation concernant le droit d'auteur, le brevet, les bases de données, le secret défense nationale, le secret professionnel et le secret des correspondances. Elles sont réprimées par le Code pénal.
- Les atteintes aux systèmes : les atteintes peuvent être matérielles (vol, écoute, sabotage) ou immatérielles (intrusion, cyberterrorisme). Ces atteintes sont sanctionnées par la loi Godfrain[8] et par le Code pénal.
- Les atteintes aux personnes : les atteintes peuvent être liées au traitement non autorisé de fichiers des données nominatives (loi du 16/12/92), à l'escroquerie et l'abus de confiance.

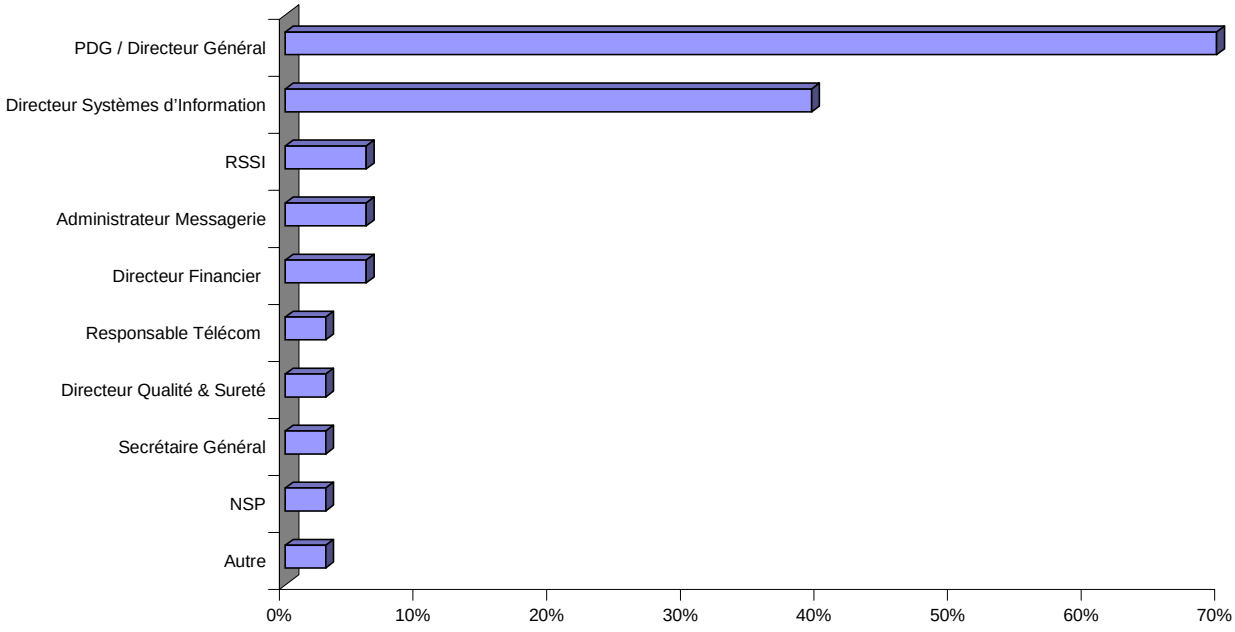
Le délit de manquement à la sécurité du système d'information, mentionné à l'article 226-17 du nouveau Code pénal, autrement dit « le fait de procéder ou de faire procéder à des traitements automatisés d'information nominatives sans prendre toutes les précautions utiles pour préserver la sécurité de ces informations et notamment empêcher qu'elles ne soient déformées, endommagées ou communiquées à des tiers non

[7] Sur la responsabilité pénale du DSI et les enjeux juridiques liés au SI, voir aussi le rapport « Intelligence juridique » du Cigref à paraître fin 2002..
[8] La loi Godfrain permet à l'entreprise de se protéger contre les tentatives d'intrusion.

autorisés, est puni de 5 ans d'emprisonnement et de 304 898 euros (2 MF) d'amende. »

Les obligations légales du DSI doivent porter *a minima* sur :

- la déclaration des fichiers et traitement de données nominatives à la Cnil ;
- l'information des salariés et du comité d'entreprise sur les mesures de surveillance et les limites d'utilisation des outils de type internet, messagerie…



Source : Cigref 2002

Figure 35 : Selon vous, qui est responsable pénalement en cas de préjudice ?

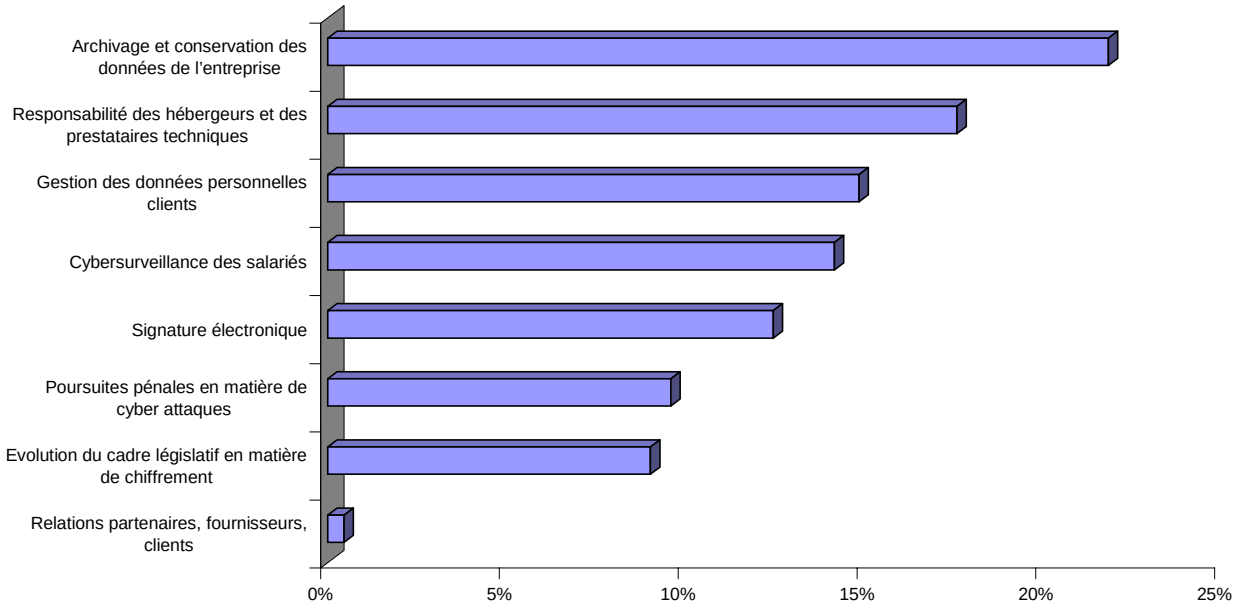
Un DSI ou un RSSI ne peuvent être inculpés du seul fait qu'une attaque informatique n'a pu être repoussée. Le DSI a ici une obligation de moyens et non de résultat. L'essentiel est de montrer que l'on a pris les mesures nécessaires pour protéger le système d'information et ses données.

4.2 Les enjeux juridiques liés à la sécurité

On assiste par ailleurs à une montée en puissance des enjeux juridiques liés à la sécurité des systèmes d'information.

Parmi les trois dossiers juridiques jugés prioritaires par les responsables de la sécurité et les DSI, on peut citer l'archivage et la conservation des données, la responsabilité des hébergeurs et des prestataires techniques, la gestion des données personnelles clients.

D'autres dossiers sont jugés également importants : la cybersurveillance des salariés, la signature électronique…



Source : Cigref 2002

Figure 36 : Quels sont les dossiers juridiques que vous jugez prioritaires pour votre entreprise en matière de sécurité ?

4.2.1 La protection des données à caractère personnel

Le Cigref a déjà évoqué, dans son précédent rapport sur la sécurité, la directive européenne du 24/10/95 sur la protection des données à caractère personnel. Les nouveautés introduites par la directive portent sur :

- l'allégement des formalités de déclaration et de contrôle *a priori* des traitements automatisés de données à caractère personnel ;
- la suppression de toute distinction entre traitements selon qu'il s'agit de traitements publics ou privés ;
- l'accroissement des pouvoirs de contrôle *a posteriori* du fonctionnement des fichiers et des traitements mis en œuvre ;
- l'énumération limitative des traitements (publics ou privés) qui, en raison de leur finalité ou des risques particuliers que leur mise en œuvre est susceptible de présenter, feront l'objet d'une autorisation préalable ;
- le renforcement des mesures d'information des personnes concernées sur la finalité des traitements et sur leurs droits (droit d'opposition à toute utilisation à des fins de prospection commerciale, droit d'opposition en cas de revente ou de cession) ;
- le renforcement du dispositif de garanties prévues en matière de flux transfrontaliers de données hors d'Europe. Ce principe est assorti de dérogations notamment lorsque le destinataire des données présente des garanties suffisantes (contrat assorti de clauses types).

L'avantage de cette directive est qu'elle permet la mise en place d'un régime européen harmonisé en matière de gestion des données à caractère personnel et qu'elle offre un cadre légal sécurisé pour le transfert des données vers un pays tiers offrant un niveau de protection équivalent (principe du « *safe harbour* »).

L'efficacité de ce dispositif de transfert n'est toutefois qu'apparente, de nombreuses dérogations étant prévues. Ainsi, alors même que la protection n'est pas adéquate, les données pourront être transférées si :

- la personne a consenti au transfert de ses données dans un pays n'offrant pas un niveau de protection adéquate ;
- le transfert est nécessaire à la réalisation d'un contrat entre la personne concernée et le responsable du traitement ;

- le transfert est nécessaire à l'exécution d'un contrat ou de mesures pré-contractuelles, dans l'intérêt de la personne concernée, entre le maître du fichier et un tiers.

Avec retard, la directive est en cours de transposition en France avec le projet de loi qui a fait l'objet d'un 1er vote à l'Assemblée nationale le 30 janvier 2002. Ce projet de loi vise à rénover la loi Informatique et Libertés de 1978.

Lors des discussions parlementaires, les députés ont introduit des dispositions nouvelles portant sur :

- les *cookies* : l'utilisateur doit être informé de manière claire et complète des finalités du *cookie* et des moyens de s'y opposer. L'accès à un service web ne peut être subordonné à l'acceptation d'un *cookie.*
- le droit des héritiers sur les données à caractère personnel de leurs parents décédés.
- les dérogations concernant le traitement des données à des fins de journalisme.
- le renforcement des pénalités et des pouvoirs de sanction de la Cnil.
- le renforcement du contrôle des enregistrements visuels de vidéosurveillance dans les lieux publics.

4.2.2 La cybersurveillance des salariés : un principe admis mais encadré

La cybersurveillance pose la problématique des usages mixtes des nouvelles technologies de l'information et de la communication (NTIC) et de l'équilibre entre vie privée et vie professionnelle au sein de l'entreprise. Le principe de la cybersurveillance sur le lieu de travail est admis, moyennant le respect des principes suivants :

- l'information préalable des salariés ;
- la discussion collective avec les instances représentatives du personnel ;
- le principe de proportionnalité.

La cybersurveillance comprend le contrôle des accès à internet, l'usage de la messagerie, l'usage des fichiers de journalisation, la place des NTIC dans le cadre du dialogue social et pose enfin la question du rôle de l'administrateur du réseau.

En matière de contrôle des accès à internet, la Cnil rappelle dans son 22e rapport d'activité que, lorsqu'une entreprise met en place un dispositif de contrôle individuel, le traitement automatisé des informations nominatives doit être déclaré à la Cnil et la durée de conservation des données doit être précisée.

Le dossier de déclaration doit comporter l'indication et la date à laquelle les instances représentatives du personnel ont été consultées.

Pour le contrôle de l'usage de la messagerie, lorsqu'une entreprise met en place un dispositif de contrôle individuel poste par poste du fonctionnement de la messagerie, là aussi le traitement automatisé des informations nominatives doit être déclaré à la Cnil et la durée de conservation des données doit être précisée. Le dossier de déclaration doit comporter l'indication et la date à laquelle les instances représentatives du personnel ont été consultées.

Pour les fichiers de journalisation, la mise en oeuvre d'un logiciel d'analyse (applicatifs et systèmes) permettant de collecter des informations personnelles poste par poste, destiné à contrôler l'activité des utilisateurs doit être déclarée à la Cnil.

Par ailleurs la sécurité doit être renforcée dans le cas d'une utilisation des NTIC par les instances représentatives du personnel.

Enfin, en ce qui concerne le rôle des administrateurs réseaux : l'accès aux informations relatives aux utilisateurs sur le disque dur du poste de travail n'est pas contraire à la loi de 1978, ni l'utilisation de logiciels de télémaintenance. En revanche aucune exploitation à des fins autres que celles liées au bon fonctionnement et à la sécurité des applications ne peut être opérée.

Le Cigref soutient la Cnil dans sa proposition de publier un bilan annuel « informatique et libertés » et de créer une fonction de délégué à la protection des données mais s'interroge cependant sur les conditions de mise en œuvre opérationnelles de cette fonction. À qui faut-il attribuer cette mission (au RSSI, à une instance représentative du personnel, à une direction métier), avec quels moyens et quelle autorité ?

4.2.3 La signature électronique

L'Union européenne a mis en place un cadre juridique communautaire sur la signature électronique, avec la directive adopté le 13 décembre 1999. Cette directive énonce les principes suivants :

- équivalence avec une signature manuscrite sous certaines conditions (art 5.1) ;
- non-discrimination (art 5.2) ;

- mise en place de certificat qualifié et de Prestataire de service de certification qualifié (annexes 1 et 2) ;
- dispositif sécurisé de création de signature (annexe 3) ;
- pas d'accréditation obligatoire préalable à l'activité de prestataire de service de certification (PSC) (art 3.1) mais les États membres peuvent mettre en place un schéma d'accréditation volontaire (art 3.2) et émettre des exigences supplémentaires pour l'utilisation des signatures électroniques dans le secteur public (art 3.7).

On peut noter qu'il existe des différences de vocabulaire entre le texte communautaire et les textes français de transposition :

- la « signature électronique avancée » au niveau communautaire s'appelle la « signature électronique sécurisée » en français.
- l'« accréditation » des PSC s'appelle la « qualification » des PSC en français.

La France a transposé cette directive avec la loi du 13 mars 2000, les décrets du 30 mars 2001 (et du 18 avril 2002, décret relatif à l'évaluation et à la certification de la sécurité offerte par les produits et les systèmes des technologies de l'information). Dernièrement, en vertu de l'article 3.2 de la directive, la France a mis en place un schéma d'accréditation volontaire avec l'arrêté du 31 mai 2002 (arrêté relatif à la reconnaissance de la qualification des prestataires de certification électronique et à l'accréditation des organismes chargés de l'évaluation).

Le schéma français d'accréditation est basé sur une structure de validation à deux étages. Au sommet de l'édifice, se trouve le Cofrac (Comité français d'accréditation, association loi 1901) qui accrédite les organismes qualificateurs (appelés « centres d'accréditation » dans l'arrêté) qui certifient à leur tour les prestataires de services de certification (PSC), lesquels délivrent aux clients finaux les certificats.

L'arrêté du 31 mai 2002 comprend deux chapitres. Le premier chapitre traite de l'accréditation des organismes qui procèdent à l'évaluation des prestataires de services de certification électronique en vue de reconnaître leur qualification. Parmi les points intéressants on peut citer :

- les critères demandés par le centre d'accréditation au PSC pour son accréditation : statuts de l'organisme ; noms et qualités des dirigeants ; description des procédures et des moyens mis en oeuvre par l'organisme… ;

- la durée de l'accréditation : l'accréditation est accordée pour une durée de deux ans, renouvelable ;
- la publicité des informations : la liste des organismes accrédités est accessible au public, sur un site internet, et tenue à jour.

Le second chapitre traite de la reconnaissance de la qualification des prestataires de services de certification électronique. Parmi les points intéressants on peut citer :

- le prestataire de services de certification est tenu de fournir aux organismes d'accréditation qu'il a choisis tous les éléments nécessaires au bon accomplissement de la procédure d'évaluation.
- l'évaluation est effectuée par l'organisme d'accréditation aux frais du prestataire de services de certification.
- les rapports d'évaluation sont communiqués par les organismes accrédités à la direction centrale de la sécurité des systèmes d'information si celle-ci le demande.
- lorsqu'il reconnaît la qualification d'un prestataire, l'organisme accrédité délivre une attestation qui décrit les prestations de services couvertes par la qualification ainsi que la durée, qui ne peut excéder un an,

Sur le papier, le schéma français de qualification est *a priori* séduisant. Il s'appuie sur le Cofrac, organisme incontournable en matière d'accréditation, sur une structure de validation à deux étages, sur une indépendance entre les organismes certificateurs et les PSC, sur un dispositif d'information vis-à-vis du public et sur des attestations à durée de vie limitée, ce qui devrait rassurer les clients finaux.

Dans la pratique, le succès du schéma dépendra *in fine* de la souplesse et de l'efficacité du dispositif (rapidité d'instruction des dossiers…), de l'étendue de la qualification demandée (quid d'une qualification de certains services fonctionnels uniquement ?), de la volonté et de la capacité financière de prestataires de service de certification à se faire qualifier et à s'engager sur le marché et enfin de l'adhésion des clients finaux.

4.2.4 La convention du Conseil de l'Europe sur la cybercriminalité

La convention de Budapest du 23 novembre 2001 est le premier texte international conçu pour lutter contre un fléau transfrontalier complexe et grandissant : la cybercriminalité.

La convention a été signée par 26 États membres du Conseil de l'Europe et les 4 États non membres ayant participé à son

élaboration (Canada, Japon, Afrique du Sud et États-Unis). Ce traité contraignant pourra ultérieurement être ouvert à d'autres États non membres sur invitation du comité des ministres. Elle entrera en vigueur après sa ratification par 5 États, dont au moins 3 États membres du Conseil de l'Europe.

Selon les propos de Guy de Vel, directeur général des affaires juridiques du Conseil de l'Europe, « le texte ne vise que les enquêtes pénales spécifiques et n'a pas pour vocation la mise en place d'un régime de surveillance électronique générale ».

4.2.4.1 Les principales dispositions de la convention

Le texte se compose de quatre chapitres :

Le chapitre premier traite de la terminologie et donne une définition commune des termes « système informatique », « données informatiques », « fournisseur de service » et « données relatives au trafic ».

Le chapitre 2 traite des mesures à prendre au niveau national en matière de droit pénal matériel, de droit procédural, de compétence.

Le chapitre 3 traite des mécanismes de coopération internationale, les principes généraux en matière d'extradition et d'entraide, les dispositions spécifiques en matière de mesures provisoires, de pouvoirs d'investigation et la mise en place d'un réseau 24/7.

Le chapitre 4 traite des clauses finales (signature, entrée en vigueur, adhésion, application territoriale, effets de la convention, réserves…)

Le traité poursuit un triple objectif :

- établir des définitions communes de certaines infractions pénales en matière d'utilisation des nouvelles technologies ;
- définir des moyens d'enquêtes et de poursuites pénales ;
- définir des moyens de communication internationale.

Les infractions pénales visées sont :

- celles commises contre la confidentialité, l'intégralité et la disponibilité des données ou systèmes informatiques (telles que la propagation de virus) ;
- les infractions informatiques (telles que fraudes et faux virtuels) ;

- les infractions se rapportant au contenu (telles que la possession et la distribution intentionnelles de pornographie enfantine) ;
- les infractions liées aux atteintes à la propriété intellectuelle et aux droits connexes.

Il vise également à faciliter la conduite des enquêtes pénales en milieu informatique par un certain nombre de compétences procédurales telles que :

- la conservation des données stockées ;
- la conservation et la divulgation rapide des données relatives au trafic ;
- la perquisition des systèmes et la saisie de données informatiques ;
- la collecte en temps réel des données relatives au trafic et l'interception de données relatives au contenu.

Ces dispositions sont soumises aux conditions légales des pays signataires mais doivent respecter les droits de l'homme et l'application du principe de proportionnalité.

4.2.4.2 Commentaires

Le texte ne se substitue pas à la législation en vigueur mais se superpose. Des mécanismes de règlements des différends sont prévus. Des clauses de réserve sont prévues sur les dossiers sensibles (pédophilie).

Le texte permet d'envisager une atténuation de l'effet territorial et une harmonisation des pratiques dans certains domaines tels que la qualification des infractions, la procédure et les mécanismes de coopération.

Des compléments sont attendus, notamment un protocole incriminant la propagande raciste et xénophobe à travers les réseaux informatiques.

La convention pourrait avoir un impact en droit interne sur deux aspects :

- le volet coopération : la convention jouera sur les conventions existantes, en élargissant les thèmes traités dans les conventions bilatérales ;
- le volet intégration : la convention aura un impact sur les dispositifs répressifs (peu de changement sur la loi Godfrain, mais cela pourrait impacter au niveau de la conservation et la restitution des données, donc sur la LSQ.

5. PERSPECTIVES

5.1 Quelles sont les priorités des entreprises pour 2003 ?

Les entreprises sont passées d'une politique de sécurité basée sur la juxtaposition de briques hétérogènes à une politique de sécurité visant à l'optimisation des processus et à la rationalisation des investissements en sécurité.

Parmi les priorités citées par les entreprises pour les douze prochains mois, on peut évoquer la réactualisation des plans de secours, la refonte de la politique de sécurité, la sensibilisation des utilisateurs, la sécurisation des sites internet, intranet, extranet, le déploiement de solutions de détection d'intrusion. La réactualisation des plans de secours met en évidence l'impact de la continuité du système d'information pour les besoins métiers.

Source : Cigref 2002

Figure 37 : Quelles sont vos trois priorités dans le domaine de la sécurité pour les 12 prochains mois ?

Ont également été citées comme priorités, par un faible nombre d'entreprises :

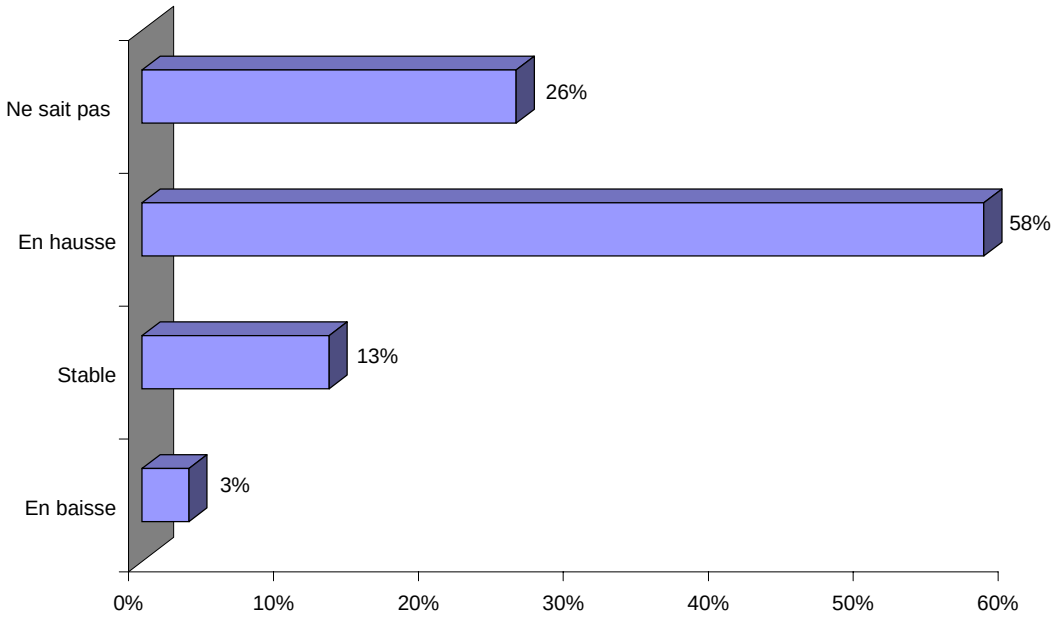
- signature électronique ;
- renforcement de la sécurité logique ;
- amélioration des plans de continuité ;
- mise en place de plans d'actions sécurité spécifique ;
- sécurisation des accès distants ;
- sécurisation du poste de travail ;
- sécurisation de la messagerie ;
- cadre légal d'action des administrateurs de réseaux ;
- amélioration de la disponibilité des systèmes ;
- développement sécurisé ;
- mise en place d'une organisation autour de la sécurité ;
- harmonisation de la politique au niveau groupe ;
- sécurisation n-tiers ;
- tableaux de bord ;
- télétransmission des paiements.

5.2 Un budget sécurité en augmentation

Pour une majorité des grandes entreprises interrogées, le budget de la sécurité va encore augmenter en 2003, mais pas sur l'ensemble des postes.

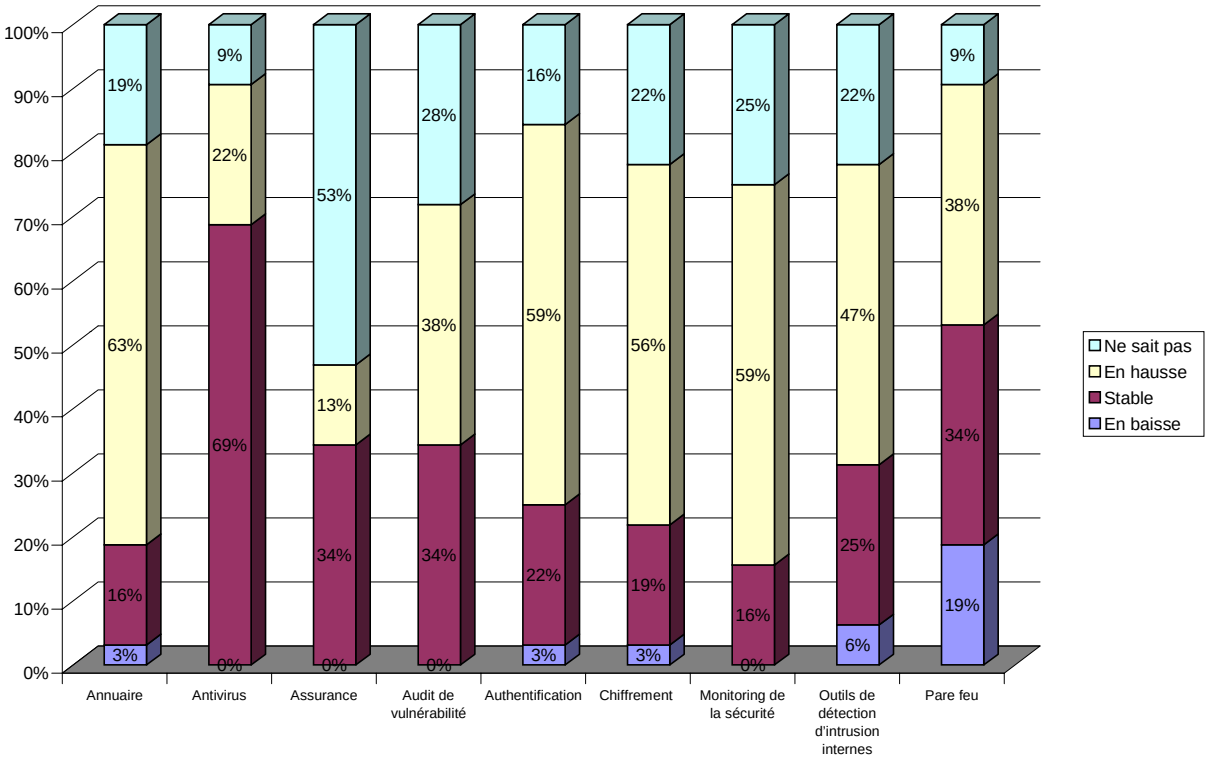
Les principaux postes en augmentation seront les services d'annuaires, les réseaux privés virtuels, le *monitoring* de la sécurité, les infrastructures à clé publique ou PKI, les outils de chiffrements et d'authentification, les outils de détection d'intrusions internes.

Les postes de dépense stables concernent les anti-virus, les tests d'intrusion externes, les services de conseil, de formation, d'intégration, de support.



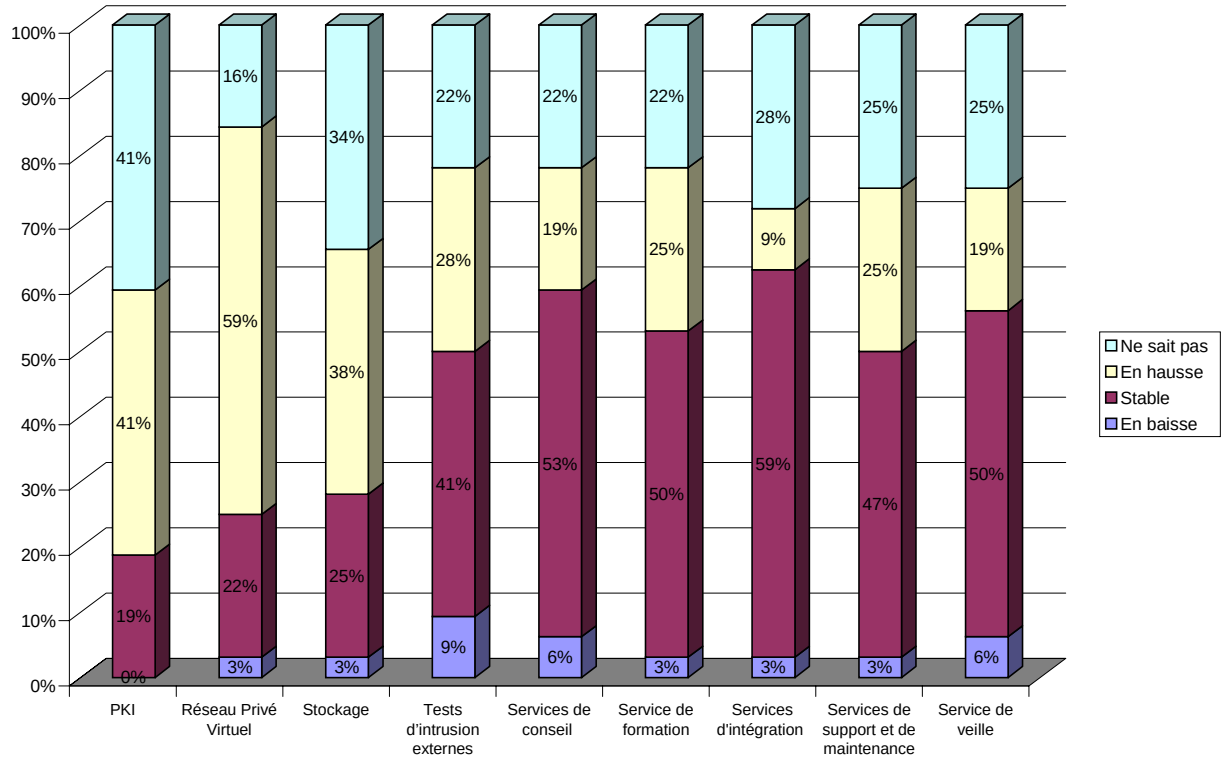
Source : Cigref 2002

Figure 38 : Évolution des budgets de sécurité.



Source : Cigref 2002

Figure 39 : Évolution des budgets par type de poste (1/2).



Source : Cigref 2002

Figure 40 : Évolution des budgets par type de poste (2/2).

5.3 Les marges de progrès

Un certain nombre de questions restent cependant sans réponse. Parmi les dossiers complexes, on peut citer la refonte et le test régulier des plans de secours. La gestion de la sécurité dans un contexte international et la question de la persistance de l'efficacité de la sécurité dans le temps méritent également toute l'attention des entreprises.

La gestion de la sécurité dans un contexte international et multi-culturel

La gestion de la sécurité dans un contexte international fait émerger les problématiques suivantes :

- choix de méthodes ;
- vitesse de déploiement ;
- choix des fournisseurs ;
- disparité de régimes juridiques ;

- hétérogénéité de niveau de sécurité ;
- disparité de budget et de *reporting* ;
- différence de sensibilité et de culture sécurité.

La gestion de la sécurité dans le temps

La persistance de l'efficacité de la sécurité dans le temps suppose notamment que celle-ci reste une priorité dans l'agenda des DG et des DSI. Cela implique également une meilleure traçabilité des attaques. Cela suppose aussi des outils de mesures et de pilotage plus performants, une prise en compte plus fine des nouveaux usages. L'un des aspects clés réside cependant dans l'efficacité des actions de sensibilisation et une métrique plus fine de la rentabilité.

5.4 Conclusion

La mise en place d'une démarche « sécurité » a des impacts à plusieurs niveaux dans l'entreprise.

Tout d'abord la politique de sécurité implique une réflexion en amont et de manière transversale sur le mode de management, la refonte des processus et les nouveaux usages (gestion de projets, processus métiers, processus informatiques, chartes comportementales…).

Ensuite la politique de sécurité doit prendre en compte la dimension de la gestion des ressources humaines et de la gestion des connaissances (évolution des métiers et gestion des connaissances, gestion des ressources internes et externes, politique de rémunération…).

Enfin la politique de sécurité doit s'intéresser à l'architecture technique et fonctionnelle du système d'information.

La politique de sécurité doit s'appuyer sur un ensemble de grands principes, au nombre desquels on peut citer :

- le principe de précaution ;
- le principe de coopération ;
- le principe d'économie ;
- le principe de décentralisation ;
- le principe de séparation des pouvoirs.

La politique de sécurité doit être globale, autrement dit gérer la sécurité du contenu et du contenant, développer une approche de type *risk management*, évaluer les risques techniques, juridiques, organisationnels et humains, associer l'ensemble

des acteurs de l'entreprise (DG, DRH, métiers...), prendre en compte la sécurité des partenaires et des fournisseurs.

Enfin la politique de sécurité doit être permanente, c'est-à-dire être en mesure de prendre en compte la composante sécurité dans tous les projets métiers, gérer les anciens et nouveaux collaborateurs, gérer les changements de périmètre de l'entreprise (fusion - acquisition, vente par appartement).

La sécurité étant actuellement un thème à la mode, il n'est pas exclu qu'il y ait à terme un risque de surinvestissement dans le domaine, à l'instar de ce qui s'est produit par le passé dans l'e-business ou les télécoms. Le Cigref met en garde contre des discours marketing parfois générateurs de promesses non tenables mais également aussi contre un discours souvent trop alarmiste.

Annexe 1 : Sites web

CERT

www.cert.org

Clusif

www.clusif.asso.fr

Conseil de l'Europe

www.coe.int

CNIL

www.cnil.fr

Computer Security Institute

www.gocsi.com

Global Business Dialogue on Electronic Commerce

www.gbde.org

OCDE

www.ocde.org

Riskwatch

www.riskwatch.com/

SANS Institute

www.sans.org

Annexe 2 : Décret du 18 avril 2002

Décret no 2002-535 du 18 avril 2002 relatif à l'évaluation et à la certification de la sécurité offerte par les produits et les systèmes des technologies de l'information.

Art. 1er. - La sécurité offerte par des produits ou des systèmes des technologies de l'information, au regard notamment de leur aptitude à assurer la disponibilité, l'intégrité ou la confidentialité de l'information traitée face aux menaces dues en particulier à la malveillance peut être certifiée dans les conditions prévues au présent décret.

Les administrations de l'État recourent, dans la mesure du possible et en fonction de leurs besoins de sécurité, à des produits ou des systèmes des technologies de l'information certifiés suivant la procédure prévue au présent décret.

Chapitre Ier

Procédure d'évaluation et de certification.

Section 1

Évaluation

Art. 2. - Une évaluation en vue de la certification prévue à l'article 1er est effectuée à la demande d'un commanditaire qui adresse à la direction centrale de la sécurité des systèmes d'information un dossier d'évaluation. Le dossier comporte notamment la description du système de sécurité à évaluer, les dispositions prévues pour lui conférer sa pleine efficacité ainsi que le programme de travail prévisionnel permettant une évaluation.

Dès réception de ce dossier, la direction centrale de la sécurité des systèmes d'information si elle estime que les objectifs de sécurité ne sont pas définis de manière pertinente au regard des normes, prescriptions techniques ou règles de bonne pratique applicables au moment où commence l'évaluation, notifie au commanditaire qu'elle ne pourra pas en l'état du dossier procéder à la certification envisagée.

Art. 3. - Le commanditaire de l'évaluation choisit un ou plusieurs centres d'évaluation, agréés dans les conditions prévues au chapitre II, pour procéder à celle-ci. Avant le début des travaux, il détermine avec chacun de ces centres :

a) Le produit ou le système à évaluer ainsi que les objectifs de sécurité ;

b) Les conditions de protection de la confidentialité des informations qui seront traitées dans le cadre de l'évaluation ;

c) Le coût et les modalités de paiement de l'évaluation ;

d) Le programme de travail et les délais prévus pour l'évaluation.

Le commanditaire est tenu d'assurer la mise à la disposition des centres d'évaluation qu'il a choisis et de la direction centrale de la sécurité des systèmes d'information, si elle en fait la demande, de tous les éléments nécessaires au bon accomplissement de leurs travaux, le cas échéant après accord des fabricants concernés.

Art. 4. - Le commanditaire peut décider à tout moment de mettre fin à une évaluation.

Il est décidé entre les parties du dédommagement éventuellement dû au centre d'évaluation.

Art. 5. - La direction centrale de la sécurité des systèmes d'information veille à la bonne exécution des travaux d'évaluation. Elle peut à tout moment demander à assister à ces travaux ou à obtenir des informations sur leur déroulement.

Art. 6. - Au terme des travaux d'évaluation, chaque centre remet un rapport d'évaluation au commanditaire et à la direction centrale de la sécurité des systèmes d'information. Ce rapport est un document confidentiel dont les informations sont couvertes par le secret industriel et commercial.

Section 2

Certification

Art. 7. - Le commanditaire et la direction centrale de la sécurité des systèmes d'information valident les rapports d'évaluation en liaison avec le centre d'évaluation intervenant. Lorsque l'ensemble des rapports prévus a été validé, la direction centrale de la sécurité des systèmes d'information élabore un rapport de certification dans un délai d'un mois. Ce rapport, qui précise les caractéristiques des objectifs de sécurité proposés, conclut soit à la délivrance d'un certificat, soit au refus de la certification.

Le rapport de certification peut comporter tout avertissement que ses rédacteurs estiment utile de mentionner pour des raisons de sécurité. Il est, au choix du commanditaire, communiqué ou non à des tiers ou rendu public.

Art. 8. - Le certificat est délivré par le Premier ministre.

Il atteste que l'exemplaire du produit ou du système soumis à évaluation répond aux caractéristiques de sécurité spécifiées. Il atteste également que l'évaluation a été conduite conformément aux règles et normes en vigueur, avec la compétence et l'impartialité requises.

Art. 9. - La direction centrale de la sécurité des systèmes d'information peut passer, après avis du comité directeur de la certification, des accords de reconnaissance mutuelle avec des organismes étrangers homologues, ayant leur siège en dehors des États membres de la Communauté européenne.

Ces accords peuvent prévoir que les certificats délivrés par les organismes étrangers cosignataires, dans le cadre de procédures comparables à celle prévue au présent chapitre, sont reconnus comme ayant la même valeur que les certificats délivrés en application du présent décret. La reconnaissance mutuelle des certificats peut être limitée à un niveau d'assurance déterminé.

Sans préjudice des règles régissant la certification des dispositifs sécurisés de création de signature électronique mentionnées au 2o du II de l'article 3 du décret du 30 mars 2001 susvisé, le Premier ministre reconnaît aux certificats délivrés par les organismes ayant leur siège dans un Etat membre de la Communauté européenne, dans le cadre de procédures comparables présentant des garanties équivalentes, la même valeur qu'aux certificats délivrés en application du présent décret.

Chapitre II

Agrément des centres d'évaluation

Art. 10. - Les centres d'évaluation chargés de procéder à l'évaluation prévue au présent décret sont agréés dans les conditions fixées par le présent chapitre.

Art. 11. - I. - La demande d'agrément est formulée auprès de la direction centrale de la sécurité des systèmes d'information. Cette demande précise le domaine dans lequel l'organisme demandeur entend exercer son activité.

II. - L'organisme demandeur doit faire la preuve :

a) De sa conformité aux critères de qualité selon les règles et normes d'accréditation en vigueur ;

b) De son aptitude à appliquer les critères d'évaluation en vigueur et la méthodologie correspondante ainsi qu'à assurer la confidentialité requise par l'évaluation ;

c) De sa compétence technique à conduire une évaluation.

La conformité mentionnée au a et l'aptitude mentionnée au b sont attestées par une accréditation délivrée par une instance reconnue dans les conditions prévues à l'article R. 115-6 du code de la consommation ou délivrée par une instance étrangère équivalente.

La compétence technique mentionnée au c est appréciée par la direction centrale de la sécurité des systèmes d'information, notamment à partir des moyens, des ressources et de l'expérience du centre d'évaluation.

Art. 12. - L'agrément est délivré par le Premier ministre, après avis du comité directeur de la certification.

Il peut énoncer les obligations particulières auxquelles est soumis le centre d'évaluation.

Il est valable pour une durée de deux ans renouvelable.

Art. 13. - Lorsqu'un centre d'évaluation situé hors du territoire national ou d'un autre Etat membre de la Communauté européenne a déjà fait l'objet d'un agrément par les autorités de son pays d'installation dans le cadre d'une procédure homologue, le Premier ministre peut, après avis du comité directeur de la certification, le déclarer agréé au titre du présent décret. Cet agrément, qui est accordé pour une durée de deux ans renouvelable, peut être limité à un niveau d'assurance déterminé.

Lorsqu'un centre d'évaluation situé dans un État membre de la Communauté européenne a déjà fait l'objet d'un agrément par les autorités de cet État dans le cadre d'une procédure équivalente, le Premier ministre, après avis du comité directeur de la certification, le déclare agréé au titre du présent décret.

Art. 14. - La direction centrale de la sécurité des systèmes d'information peut s'assurer à tout moment que les centres d'évaluation continuent à satisfaire aux critères au vu desquels ils ont été agréés.

Lorsqu'un centre ne satisfait plus aux exigences mentionnées à l'article 11 ou qu'il manque aux obligations fixées par la décision d'agrément, l'agrément peut être retiré par le Premier ministre, après avis du comité directeur de la certification. Le retrait ne peut être prononcé qu'après que le représentant du centre d'évaluation a été mis à même de faire valoir ses observations devant le comité directeur de la certification.

Chapitre III

Comité directeur de la certification en sécurité des technologies de l'information

Art. 15. - Le comité directeur de la certification en sécurité des technologies de l'information a notamment pour mission :

a) De formuler des avis ou des propositions sur la politique de certification, sur les règles et normes utilisées pour les procédures d'évaluation et de certification et sur les guides techniques mis à la disposition du public ;

b) D'émettre un avis sur la délivrance et le retrait des agréments aux centres d'évaluation ;

c) D'examiner, à des fins de conciliation, tout litige relatif aux procédures d'évaluation organisées par le présent décret qui lui est soumis par les parties ;

d) D'émettre un avis sur les accords de reconnaissance mutuelle conclus avec des organismes étrangers en application de l'article 9.

La mission prévue au c ci-dessus peut être déléguée par le comité à l'un de ses membres, elle comporte obligatoirement l'audition des parties.

Art. 16. - Le comité directeur de la certification en sécurité des technologies de l'information est présidé par le secrétaire général de la défense nationale ou son représentant. Outre son président, il comprend :

a) Un représentant du ministre de la justice ;

b) Un représentant du ministre de l'intérieur ;

c) Un représentant du ministre des affaires étrangères ;

d) Un représentant du ministre de la défense ;

e) Un représentant du ministre chargé de l'industrie ;

f) Un représentant du ministre chargé de l'économie ;

g) Un représentant du ministre chargé de l'emploi ;

h) Un représentant du ministre chargé de la santé ;

i) Un représentant du ministre chargé de l'éducation nationale ;

j) Un représentant du ministre chargé de la communication ;

k) Un représentant du ministre chargé de la réforme de l'État ;

l) Un représentant du ministre chargé des transports ;

m) Un représentant du ministre chargé ; de la recherche.

Lorsque le comité directeur examine des questions concernant les dispositifs de création et de vérification de signature électronique, tels que définis à l'article 1er du décret du 30 mars 2001 susvisé, il comprend en outre douze personnalités qualifiées nommées pour trois ans par arrêté du Premier ministre.

Le secrétariat du comité directeur est assuré par la direction centrale de la sécurité des systèmes d'information.

Art. 17. - Le comité directeur se réunit sur convocation de son président qui en fixe l'ordre du jour.

Le président peut inviter tout expert ou personne qualifiée dont la participation aux débats lui paraît nécessaire.

Le comité rend compte de ses travaux au Premier ministre.

Art. 18. - La direction centrale de la sécurité des systèmes d'information fait annuellement rapport au comité directeur de la certification de l'activité qu'elle exerce dans le cadre de la mise en oeuvre du présent décret.

Chapitre IV

Dispositions diverses et transitoires.

Art. 19. - Dans la partie « Sécurité et défense nationale » du paragraphe 2 de l'annexe au décret no 97-1184 du 19 décembre 1997 susvisé, il est ajouté, à la suite du tableau relatif au décret no 2001-143 du 15 février 2001, les mots et le tableau suivants :

« Décret no 2002-535 du 18 avril 2002 » relatif à l'évaluation et à la certification de la sécurité offerte par les produits et les systèmes des technologies de l'information.

Vous pouvez consulter le tableau dans le JO

n° 92 du 19/04/2002 page 6944 à 6946

Art. 20. - Le décret du 30 mars 2001 susvisé est ainsi modifié :

I. - Le 1° du II de l'article 3 est remplacé par les dispositions suivantes :

« 1° Soit par le Premier ministre, dans les conditions prévues par le décret no 2002-535 du 18 avril 2002 relatif à l'évaluation et à la certification de la sécurité offerte par les produits et les systèmes des technologies de l'information. La délivrance du certificat de conformité est rendue publique. »

II. - L'article 4 est remplacé par les dispositions suivantes :

« Art. 4. - La mise en oeuvre des procédures d'évaluation et de certification prévues au 1° du II de l'article 3 est assurée dans les conditions prévues par le décret no 2002-535 du 18 avril 2002 relatif à l'évaluation et à la certification de la sécurité offerte par les produits et les systèmes des technologies de l'information. »

III. - Au premier alinéa de l'article 5, les mots : « l'arrêté » sont remplacés par les mots : « le décret ».

IV. - Au deuxième alinéa de l'article 7, les mots : « selon des règles définies par arrêté du Premier ministre » sont supprimés.

V. - Au premier alinéa du II de l'article 9, les mots : « par des organismes publics désignés par arrêté du Premier ministre et agissant sous l'autorité des services du Premier ministre chargés de la sécurité des systèmes d'information » sont remplacés par les mots : « par la direction centrale de la sécurité des systèmes d'information ».

Art. 21. - Les certificats et les agréments des centres d'évaluation délivrés avant la date d'entrée en vigueur du présent décret, en application des dispositions de l'avis du Premier ministre relatif à la délivrance de certificats pour la sécurité offerte par les produits informatiques vis-à-vis de la malveillance, publié au Journal officiel de la République française du 1er septembre 1995, sont reconnus comme délivrés au titre du présent décret.

Art. 22. - Le présent décret est applicable :

a) En Nouvelle-Calédonie et en Polynésie française, en tant qu'il concerne la signature électronique ;

b) Dans les îles Wallis et Futuna et à Mayotte.

Art. 23. - Les dispositions du présent décret pourront être ultérieurement modifiées par décret, à l'exception :

a) Du premier alinéa des articles 8 et 12, du deuxième alinéa de l'article 14 et de l'article 19 dont la modification s'effectuera, le cas échéant, dans les conditions prévues à l'article 2 du décret du 15 janvier 1997 susvisé ;

b) De l'article 20.

Art. 24. - Le présent décret sera publié au Journal officiel de la République française.

Fait à Paris, le 18 avril 2002.

Annexe 3 : Arrêté du 31 mai 2002

Accréditation des organismes qui procèdent à l'évaluation des prestataires de services de certification électronique en vue de reconnaître leur qualification.

Art. 1er. - Le Comité français d'accréditation (COFRAC), association déclarée le 4 mai 1994, ainsi que les organismes d'accréditation signataires de l'accord européen multilatéral pris dans le cadre de la coordination européenne des organismes d'accréditation, sont chargés d'accréditer les organismes qui procèdent à l'évaluation des prestataires de services de certification électronique en vue de reconnaître leur qualification. Ils sont nommés ci-après centres d'accréditation.

Art. 2. - La demande d'accréditation, adressée par un organisme à un centre d'accréditation, doit comprendre les éléments suivants :

1. Les statuts de l'organisme, son règlement intérieur et tous autres textes régissant son fonctionnement ;

2. Les noms et qualités des dirigeants de l'organisme et des membres de son conseil d'administration ou des organes en tenant lieu ;

3. Les noms et les qualifications des personnels de l'organisme prenant part à la procédure d'évaluation ;

4. La description des activités de l'organisme, de sa structure et de ses moyens techniques ;

5. Les comptes des deux exercices précédents ;

6. La description des procédures et des moyens qui seront mis en oeuvre par l'organisme pour évaluer les prestataires de certification électronique en vue de reconnaître leur qualification, compte tenu des normes ou prescriptions techniques en vigueur.

L'organisme demandeur doit en outre signaler au centre d'accréditation les liens éventuels qu'il a avec des prestataires de services de certification électronique. En ce cas, il doit préciser les mesures qu'il compte mettre en oeuvre pour éviter tout conflit d'intérêts.

Art. 3. - Le centre d'accréditation instruit la demande d'accréditation. Il peut solliciter tous renseignements complémentaires de l'organisme demandeur. Il peut demander à effectuer des vérifications dans les locaux de l'organisme demandeur. A l'issue de l'instruction, le centre d'accréditation prend une décision motivée qu'il notifie à l'organisme

demandeur et dont il adresse copie à la direction centrale de la sécurité des systèmes d'information. Lorsqu'il accorde l'accréditation, le centre d'accréditation peut soumettre l'organisme bénéficiaire à des obligations particulières.

Art. 4. - L'accréditation est accordée pour une durée de deux ans. Elle peut être renouvelée pour une durée identique, à la demande de l'organisme bénéficiaire, après que le centre d'accréditation a vérifié que celui-ci remplit toujours l'ensemble des conditions requises. Les organismes accrédités informent le centre d'accréditation de tout changement par rapport aux éléments communiqués dans le dossier de demande d'accréditation. Le centre d'accréditation peut s'assurer à tout moment que les organismes continuent à satisfaire aux critères au vu desquels ils ont été accrédités. Lorsqu'un organisme ne satisfait plus aux conditions d'accréditation ou manque aux obligations fixées dans la décision d'accréditation, le retrait d'accréditation peut être prononcé par le centre d'accréditation après que le représentant de l'organisme concerné a été mis à même de présenter ses observations.

Art. 5. - Le centre d'accréditation met à la disposition du public, notamment sur un site internet, la liste des organismes accrédités. Cette liste est tenue à jour.

Reconnaissance de la qualification des prestataires de services de certification électronique

Art. 6. - Un prestataire de services de certification électronique qui demande à être reconnu comme qualifié choisit un ou plusieurs organismes accrédités pour procéder à l'évaluation des services qu'il propose. Le prestataire est tenu de fournir aux organismes qu'il a choisis tous les éléments nécessaires au bon accomplissement de la procédure d'évaluation.

Art. 7. - L'évaluation est effectuée par l'organisme aux frais du prestataire de services de certification. Son objet est notamment de vérifier que les services offerts par le prestataire respectent en tous points les exigences fixées par l'article 6 du décret du 30 mars 2001 susvisé ainsi que les normes, prescriptions techniques et règles de bonne pratique applicables en matière de certification électronique. A l'issue de la procédure d'évaluation, l'organisme accrédité établit un rapport qui est notifié au prestataire afin que celui-ci puisse, le cas échéant, formuler des observations sur son contenu.

Art. 8. - Les rapports d'évaluation sont communiqués par les organismes accrédités à la direction centrale de la sécurité des systèmes d'information si celle-ci le demande.

Art. 9. - L'organisme accrédité reconnaît ou non la qualification du prestataire de services de certification électronique au vu du rapport d'évaluation et des éventuelles observations du prestataire. Lorsqu'il reconnaît la qualification d'un prestataire, l'organisme accrédité délivre une attestation qui décrit les prestations de services couvertes par la qualification ainsi que la durée, qui ne peut excéder un an, pendant laquelle l'attestation est valable. Les prestataires dont la qualification est reconnue communiquent à toute personne qui en fait la demande une copie de l'attestation délivrée par l'organisme accrédité.

Art. 10. - La directrice générale de l'industrie, des technologies de l'information et des postes est chargée de l'exécution du présent arrêté, qui sera publié au Journal officiel de la République française.

Annexe 4 : Convention du 23 novembre 2001 sur la cybercriminalité

Série des Traités européens - n° 185

CONVENTION SUR LA CYBERCRIMINALITÉ

Budapest, 23.XI.2001

Préambule

Les États membres du Conseil de l'Europe et les autres États signataires.

Considérant que le but du Conseil de l'Europe est de réaliser une union plus étroite entre ses membres.

Reconnaissant l'intérêt d'intensifier la coopération avec les autres États parties à la Convention.

Convaincus de la nécessité de mener, en priorité, une politique pénale commune destinée à protéger la société de la criminalité dans le cyberespace, notamment par l'adoption d'une législation appropriée et par l'amélioration de la coopération internationale.

Conscients des profonds changements engendrés par la numérisation, la convergence et la mondialisation permanente des réseaux informatiques.

Préoccupés par le risque que les réseaux informatiques et l'information électronique soient utilisés également pour commettre des infractions pénales et que les preuves de ces infractions soient stockées et transmises par le biais de ces réseaux.

Reconnaissant la nécessité d'une coopération entre les États et l'industrie privée dans la lutte contre la cybercriminalité, et le besoin de protéger les intérêts légitimes dans l'utilisation et le développement des technologies de l'information.

Estimant qu'une lutte bien menée contre la cybercriminalité requiert une coopération internationale en matière pénale accrue, rapide et efficace.

Convaincus que la présente Convention est nécessaire pour prévenir les actes portant atteinte à la confidentialité, à l'intégrité et à la disponibilité des systèmes informatiques, des réseaux et des données, ainsi que l'usage frauduleux de tels systèmes, réseaux et données, en assurant l'incrimination de ces comportements, tels que décrits dans la présente Convention, et l'adoption de pouvoirs suffisants pour permettre une lutte efficace contre ces infractions pénales, en en facilitant la détection, l'investigation et la poursuite, tant au plan national qu'au niveau international, et en prévoyant des dispositions matérielles en vue d'une coopération internationale rapide et fiable.

Gardant à l'esprit la nécessité de garantir un équilibre adéquat entre les intérêts de l'action répressive et le respect des droits de l'homme fondamentaux, tels que garantis dans la Convention de sauvegarde des Droits de l'Homme et des Libertés fondamentales du Conseil de l'Europe (1950), dans le Pacte international relatif aux droits civils et politiques des Nations Unies (1966), ainsi que dans d'autres conventions internationales applicables en matière de droits de l'homme, qui réaffirment le droit à ne pas être inquiété pour ses opinions, le droit à la liberté d'expression, y compris la liberté de rechercher, d'obtenir et de communiquer des informations et des idées de toute nature, sans considération de frontière, ainsi que le droit au respect de la vie privée.

Conscients également du droit à la protection des données personnelles, tel que spécifié, par exemple, par la Convention de 1981 du Conseil de l'Europe pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel.

Considérant la Convention des Nations Unies relative aux droits de l'enfant (1989) et la Convention de l'Organisation internationale du travail sur les pires formes de travail des enfants (1999).

Tenant compte des conventions existantes du Conseil de l'Europe sur la coopération en matière pénale, ainsi que d'autres traités similaires conclus entre les États membres du Conseil de l'Europe et d'autres États, et soulignant que la présente Convention a pour but de les compléter en vue de rendre plus efficaces les enquêtes et les procédures pénales portant sur des infractions pénales en relation avec des systèmes et des données informatiques, ainsi que de permettre la collecte des preuves électroniques d'une infraction pénale.

Se félicitant des récentes initiatives destinées à améliorer la compréhension et la coopération internationales aux fins de la lutte contre la criminalité dans le cyberespace, notamment des actions menées par les Nations Unies, l'OCDE, l'Union européenne et le G8.

Rappelant les Recommandations du Comité des Ministres n° R (85) 10 concernant l'application pratique de la Convention européenne d'entraide judiciaire en matière pénale relative aux commissions rogatoires pour la surveillance des télécommunications, n° R (88) 2 sur des mesures visant à combattre la piraterie dans le domaine du droit d'auteur et des droits voisins, n° R (87) 15 visant à réglementer l'utilisation de données à caractère personnel dans le secteur de la police, n° R (95) 4 sur la protection des données à caractère personnel dans le domaine des services de télécommunication, eu égard notamment aux services téléphoniques, et n° R (89) 9 sur la criminalité en relation avec l'ordinateur, qui indique aux législateurs nationaux des principes directeurs pour définir certaines infractions informatiques, ainsi que n° R (95) 13 relative aux problèmes de procédure pénale liés à la technologie de l'information.

Eu égard à la Résolution n° 1, adoptée par les ministres européens de la Justice lors de leur 21e Conférence (Prague, 10 et 11 juin 1997), qui recommande au Comité des Ministres de soutenir les activités concernant la cybercriminalité menées par le Comité européen pour les problèmes criminels (CDPC) afin de rapprocher les législations pénales nationales et de permettre l'utilisation de moyens d'investigation efficaces en matière d'infractions informatiques, ainsi qu'à la Résolution n° 3, adoptée lors de la 23e Conférence des ministres européens de la Justice (Londres, 8 et 9 juin 2000), qui encourage les parties aux négociations à poursuivre leurs efforts afin de trouver des solutions permettant au plus grand nombre d'États d'être parties à la Convention et qui reconnaît la nécessité de disposer d'un mécanisme rapide et efficace de coopération internationale qui tienne dûment compte des exigences spécifiques de la lutte contre la cybercriminalité.

Prenant également en compte le plan d'action adopté par les chefs d'État et de gouvernement du Conseil de l'Europe à l'occasion de leur 2e Sommet (Strasbourg, 10 et 11 octobre 1997) afin de trouver des réponses communes au développement des nouvelles technologies de l'information, fondées sur les normes et les valeurs du Conseil de l'Europe.

Sont convenus de ce qui suit :

Chapitre I – Terminologie

Article 1 – Définitions

Aux fins de la présente Convention,

a l'expression « système informatique » désigne tout dispositif isolé ou ensemble de dispositifs interconnectés ou apparentés, qui assure ou dont un ou plusieurs éléments assurent, en exécution d'un programme, un traitement automatisé de données ;

b l'expression « données informatiques » désigne toute représentation de faits, d'informations ou de concepts sous une forme qui se prête à un traitement informatique, y compris un programme de nature à faire en sorte qu'un système informatique exécute une fonction ;

c l'expression « fournisseur de services » désigne :

i toute entité publique ou privée qui offre aux utilisateurs de ses services la possibilité de communiquer au moyen d'un système informatique, et

ii toute autre entité traitant ou stockant des données informatiques pour ce service de communication ou ses utilisateurs.

d « données relatives au trafic » désigne toutes données ayant trait à une communication passant par un système informatique, produites par ce dernier en tant qu'élément de la chaîne de communication, indiquant l'origine, la destination, l'itinéraire, l'heure, la date, la taille et la durée de la communication ou le type de service sous-jacent.

Chapitre II – Mesures à prendre au niveau national

Section 1 – Droit pénal matériel

Titre 1 – Infractions contre la confidentialité, l'intégrité et la disponibilité des données et systèmes informatiques

Article 2 – Accès illégal

Chaque Partie adopte les mesures législatives et autres qui se révèlent nécessaires pour ériger en infraction pénale, conformément à son droit interne, l'accès intentionnel et sans droit à tout ou partie d'un système informatique. Une Partie peut exiger que l'infraction soit commise en violation des mesures de sécurité, dans l'intention d'obtenir des données informatiques ou dans une autre intention délictueuse, ou soit en relation avec un système informatique connecté à un autre système informatique.

Article 3 – Interception illégale

Chaque Partie adopte les mesures législatives et autres qui se révèlent nécessaires pour ériger en infraction pénale, conformément à son droit interne, l'interception intentionnelle et sans droit, effectuée par des moyens techniques, de données informatiques, lors de transmissions non publiques, à destination, en provenance ou à l'intérieur d'un système informatique, y compris les émissions électromagnétiques provenant d'un système informatique transportant de telles données informatiques. Une Partie peut exiger que l'infraction soit commise dans une intention délictueuse ou soit en relation avec un système informatique connecté à un autre système informatique.

Article 4 – Atteinte à l'intégrité des données

1 Chaque Partie adopte les mesures législatives et autres qui se révèlent nécessaires pour ériger en infraction pénale, conformément à son droit interne, le fait, intentionnel et sans droit, d'endommager, d'effacer, de détériorer, d'altérer ou de supprimer des données informatiques.

2 Une Partie peut se réserver le droit d'exiger que le comportement décrit au paragraphe 1 entraîne des dommages sérieux.

Article 5 – Atteinte à l'intégrité du système

Chaque Partie adopte les mesures législatives et autres qui se révèlent nécessaires pour ériger en infraction pénale, conformément à son droit interne, l'entrave grave, intentionnelle et sans droit, au fonctionnement d'un système informatique, par l'introduction, la transmission, l'endommagement, l'effacement, la détérioration, l'altération ou la suppression de données informatiques.

Article 6 – Abus de dispositifs

1 Chaque Partie adopte les mesures législatives et autres qui se révèlent nécessaires pour ériger en infraction pénale, conformément à son droit interne, lorsqu'elles sont commises intentionnellement et sans droit :

a la production, la vente, l'obtention pour utilisation, l'importation, la diffusion ou d'autres formes de mise à disposition :

i d'un dispositif, y compris un programme informatique, principalement conçu ou adapté pour permettre la commission de l'une des infractions établies conformément aux articles 2 à 5 ci-dessus ;

ii d'un mot de passe, d'un code d'accès ou de données informatiques similaires permettant d'accéder à tout ou partie d'un système informatique,

dans l'intention qu'ils soient utilisés afin de commettre l'une ou l'autre des infractions visées par les articles 2 à 5; et

b la possession d'un élément visé aux paragraphes a.i ou ii ci-dessus, dans l'intention qu'il soit utilisé afin de commettre l'une ou l'autre des infractions visées par les articles 2 à 5. Une Partie peut exiger en droit interne qu'un certain nombre de ces éléments soit détenu pour que la responsabilité pénale soit engagée.

2 Le présent article ne saurait être interprété comme imposant une responsabilité pénale lorsque la production, la vente, l'obtention pour utilisation, l'importation, la diffusion ou d'autres formes de mise à disposition mentionnées au paragraphe 1 du présent article n'ont pas pour but de commettre une infraction établie conformément aux articles 2 à 5 de la présente Convention, comme dans le cas d'essai autorisé ou de protection d'un système informatique.

3 Chaque Partie peut se réserver le droit de ne pas appliquer le paragraphe 1 du présent article, à condition que cette réserve ne porte pas sur la vente, la distribution ou toute autre mise à disposition des éléments mentionnés au paragraphe 1.a.ii du présent article.

Titre 2 – Infractions informatiques

Article 7 – Falsification informatique

Chaque Partie adopte les mesures législatives et autres qui se révèlent nécessaires pour ériger en infraction pénale, conformément à son droit interne, l'introduction, l'altération, l'effacement ou la suppression intentionnels et sans droit de données informatiques, engendrant des données non authentiques, dans l'intention qu'elles soient prises en compte ou utilisées à des fins légales comme si elles étaient authentiques, qu'elles soient ou non directement lisibles et intelligibles. Une Partie peut exiger une intention frauduleuse ou une intention délictueuse similaire pour que la responsabilité pénale soit engagée.

Article 8 – Fraude informatique

Chaque Partie adopte les mesures législatives et autres qui se révèlent nécessaires pour ériger en infraction pénale, conformément à son droit interne, le fait intentionnel et sans droit de causer un préjudice patrimonial à autrui :

a par toute introduction, altération, effacement ou suppression de données informatiques ;

b par toute forme d'atteinte au fonctionnement d'un système informatique,

dans l'intention, frauduleuse ou délictueuse, d'obtenir sans droit un bénéfice économique pour soi-même ou pour autrui.

Titre 3 – Infractions se rapportant au contenu

Article 9 – Infractions se rapportant à la pornographie enfantine

1 Chaque Partie adopte les mesures législatives et autres qui se révèlent nécessaires pour ériger en infraction pénale, conformément à son droit interne, les comportements suivants lorsqu'ils sont commis intentionnellement et sans droit :

a la production de pornographie enfantine en vue de sa diffusion par le biais d'un système informatique ;

b l'offre ou la mise à disposition de pornographie enfantine par le biais d'un système informatique ;

c la diffusion ou la transmission de pornographie enfantine par le biais d'un système informatique ;

d le fait de se procurer ou de procurer à autrui de la pornographie enfantine par le biais d'un système informatique ;

e la possession de pornographie enfantine dans un système informatique ou un moyen de stockage de données informatiques.

2 Aux fins du paragraphe 1 ci-dessus, le terme « pornographie enfantine » comprend toute matière pornographique représentant de manière visuelle :

a un mineur se livrant à un comportement sexuellement explicite ;

b une personne qui apparaît comme un mineur se livrant à un comportement sexuellement explicite ;

c des images réalistes représentant un mineur se livrant à un comportement sexuellement explicite.

3 Aux fins du paragraphe 2 ci-dessus, le terme « mineur » désigne toute personne âgée de moins de 18 ans. Une Partie peut toutefois exiger une limite d'âge inférieure, qui doit être au minimum de 16 ans.

4 Une Partie peut se réserver le droit de ne pas appliquer, en tout ou en partie, les paragraphes 1, alinéas d. et e, et 2, alinéas b. et c.

Titre 4 – Infractions liées aux atteintes à la propriété intellectuelle et aux droits connexes

Article 10 – Infractions liées aux atteintes à la propriété intellectuelle et aux droits connexes

1 Chaque Partie adopte les mesures législatives et autres qui se révèlent nécessaires pour ériger en infraction pénale, conformément à son droit interne, les atteintes à la propriété intellectuelle, définies par la législation de ladite Partie, conformément aux obligations que celle-ci a souscrites en application de l'Acte de Paris du 24 juillet 1971 portant révision de la Convention de Berne pour la protection des œuvres littéraires et artistiques, de l'Accord sur les aspects commerciaux des droits de propriété intellectuelle et du traité de l'OMPI sur la propriété intellectuelle, à l'exception de tout droit moral conféré par ces conventions, lorsque de tels actes sont commis délibérément, à une échelle commerciale et au moyen d'un système informatique.

2 Chaque Partie adopte les mesures législatives et autres qui se révèlent nécessaires pour ériger en infraction pénale, conformément à son droit interne, les atteintes aux droits connexes définis par la législation de ladite Partie, conformément aux obligations que cette dernière a souscrites en application de la Convention internationale pour la protection des artistes interprètes ou exécutants, des producteurs de phonogrammes et des organismes de radiodiffusion (Convention de Rome), de l'Accord relatif aux aspects commerciaux des droits de propriété intellectuelle et du Traité de l'OMPI sur les interprétations et exécutions, et les phonogrammes, à l'exception de tout droit moral conféré par ces conventions, lorsque de tels actes sont commis délibérément, à une échelle commerciale et au moyen d'un système informatique.

3 Une Partie peut, dans des circonstances bien délimitées, se réserver le droit de ne pas imposer de responsabilité pénale au titre des paragraphes 1 et 2 du présent article, à condition que d'autres recours efficaces soient disponibles et qu'une telle réserve ne porte pas atteinte aux obligations internationales incombant à cette Partie en application des instruments internationaux mentionnés aux paragraphes 1 et 2 du présent article.

Titre 5 – Autres formes de responsabilité et de sanctions

Article 11 – Tentative et complicité

1 Chaque Partie adopte les mesures législatives et autres qui se révèlent nécessaires pour ériger en infraction pénale, conformément à son droit interne, toute complicité lorsqu'elle est commise intentionnellement en vue de la perpétration d'une des infractions établies en application des articles 2 à 10 de la présente Convention, dans l'intention qu'une telle infraction soit commise.

2 Chaque Partie adopte les mesures législatives et autres qui se révèlent nécessaires pour ériger en infraction pénale, conformément à son droit interne, toute tentative intentionnelle de commettre l'une des infractions établies en application des articles 3 à 5, 7, 8, 9.1.a et c de la présente Convention.

3 Chaque Partie peut se réserver le droit de ne pas appliquer, en tout ou en partie, le paragraphe 2 du présent article.

Article 12 – Responsabilité des personnes morales

1 Chaque Partie adopte les mesures législatives et autres qui se révèlent nécessaires pour que les personnes morales puissent être tenues pour responsables des infractions établies en

application de la présente Convention, lorsqu'elles sont commises pour leur compte par toute personne physique, agissant soit individuellement, soit en tant que membre d'un organe de la personne morale, qui exerce un pouvoir de direction en son sein, fondé :

a sur un pouvoir de représentation de la personne morale ;

b sur une autorité pour prendre des décisions au nom de la personne morale ;

c sur une autorité pour exercer un contrôle au sein de la personne morale.

2 Outre les cas déjà prévus au paragraphe 1 du présent article, chaque Partie adopte les mesures qui se révèlent nécessaires pour s'assurer qu'une personne morale peut être tenue pour responsable lorsque l'absence de surveillance ou de contrôle de la part d'une personne physique mentionnée au paragraphe 1 a rendu possible la commission des infractions établies en application de la présence Convention pour le compte de ladite personne morale par une personne physique agissant sous son autorité.

3 Selon les principes juridiques de la Partie, la responsabilité d'une personne morale peut être pénale, civile ou administrative.

4 Cette responsabilité est établie sans préjudice de la responsabilité pénale des personnes physiques ayant commis l'infraction.

Article 13 – Sanctions et mesures

1 Chaque Partie adopte les mesures législatives et autres qui se révèlent nécessaires pour que les infractions pénales établies en application des articles 2 à 11 soient passibles de sanctions effectives, proportionnées et dissuasives, comprenant des peines privatives de liberté.

2 Chaque Partie veille à ce que les personnes morales tenues pour responsables en application de l'article 12 fassent l'objet de sanctions ou de mesures pénales ou non pénales effectives, proportionnées et dissuasives, comprenant des sanctions pécuniaires.

Section 2 – Droit procédural

Titre 1 – Dispositions communes

Article 14 – Portée d'application des mesures du droit de procédure

1 Chaque Partie adopte les mesures législatives et autres qui se révèlent nécessaires pour instaurer les pouvoirs et procédures prévus dans la présente section aux fins d'enquêtes ou de procédures pénales spécifiques.

2 Sauf disposition contraire figurant à l'article 21, chaque Partie applique les pouvoirs et procédures mentionnés dans le paragraphe 1 du présent article :

a aux infractions pénales établies conformément aux articles 2 à 11 de la présente Convention ;

b à toutes les autres infractions pénales commises au moyen d'un système informatique ; et

c à la collecte des preuves électroniques de toute infraction pénale.

3 a Chaque Partie peut se réserver le droit de n'appliquer les mesures mentionnées à l'article 20 qu'aux infractions ou catégories d'infractions spécifiées dans la réserve, pour autant que l'éventail de ces infractions ou catégories d'infractions ne soit pas plus réduit que celui des infractions auxquelles elle applique les mesures mentionnées à l'article 21.

Chaque Partie envisagera de limiter une telle réserve de manière à permettre l'application la plus large possible de la mesure mentionnée à l'article 20.

b Lorsqu'une Partie, en raison des restrictions imposées par sa législation en vigueur au moment de l'adoption de la présente Convention, n'est pas en mesure d'appliquer les mesures visées aux articles 20 et 21 aux communications transmises dans un système informatique d'un fournisseur de services :

i qui est mis en œuvre pour le bénéfice d'un groupe d'utilisateurs fermé, et

ii qui n'emploie pas les réseaux publics de télécommunication et qui n'est pas connecté à un autre système informatique, qu'il soit public ou privé,

cette Partie peut réserver le droit de ne pas appliquer ces mesures à de telles communications. Chaque Partie envisagera de limiter une telle réserve de manière à permettre l'application la plus large possible de la mesure mentionnée aux articles 20 et 21.

Article 15 – Conditions et sauvegardes

1 Chaque Partie veille à ce que l'instauration, la mise en œuvre et l'application des pouvoirs et procédures prévus dans la présente section soient soumises aux conditions et sauvegardes prévues par son droit interne, qui doit assurer une protection adéquate des droits de l'homme et des libertés, en particulier des droits établis conformément aux obligations que celle-ci a souscrites en application de la Convention de sauvegarde des Droits de l'Homme et des Libertés fondamentales du Conseil de l'Europe (1950) et du Pacte international relatif aux droits civils et politiques des Nations Unies (1966), ou d'autres instruments internationaux applicables concernant les droits de l'homme, et qui doit intégrer le principe de la proportionnalité.

2 Lorsque cela est approprié, eu égard à la nature de la procédure ou du pouvoir concerné, ces conditions et sauvegardes incluent, entre autres, une supervision judiciaire ou d'autres formes de supervision indépendante, des motifs justifiant l'application ainsi que la limitation du champ d'application et de la durée du pouvoir ou de la procédure en question.

3 Dans la mesure où cela est conforme à l'intérêt public, en particulier à la bonne administration de la justice, chaque Partie examine l'effet des pouvoirs et procédures dans cette section sur les droits, responsabilités et intérêts légitimes des tiers.

Titre 2 – Conservation rapide de données informatiques stockées

Article 16 – Conservation rapide de données informatiques stockées

1 Chaque Partie adopte les mesures législatives et autres qui se révèlent nécessaires pour permettre à ses autorités compétentes d'ordonner ou d'imposer d'une autre manière la conservation rapide de données électroniques spécifiées, y compris des données relatives au trafic, stockées au moyen d'un système informatique, notamment lorsqu'il y a des raisons de penser que celles-ci sont particulièrement susceptibles de perte ou de modification.

2 Lorsqu'une Partie fait application du paragraphe 1 ci-dessus, au moyen d'une injonction ordonnant à une personne de conserver des données stockées spécifiées se trouvant en sa possession ou sous son contrôle, cette Partie adopte les mesures législatives et autres qui se révèlent nécessaires pour obliger cette personne à conserver et à protéger l'intégrité desdites données pendant une durée aussi longue que nécessaire, au maximum de quatre-vingt-dix jours, afin de permettre aux autorités compétentes d'obtenir leur divulgation. Une Partie peut prévoir qu'une telle injonction soit renouvelée par la suite.

3 Chaque Partie adopte les mesures législatives et autres qui se révèlent nécessaires pour obliger le gardien des données ou une autre personne chargée de conserver celles-ci à garder le secret sur la mise en œuvre desdites procédures pendant la durée prévue par son droit interne.

4 Les pouvoirs et procédures mentionnés dans le présent article doivent être soumis aux articles 14 et 15.

Article 17 – Conservation et divulgation partielle rapides de données relatives au trafic

1 Afin d'assurer la conservation des données relatives au trafic, en application de l'article 16, chaque Partie adopte les mesures législatives et autres qui se révèlent nécessaires :

a pour veiller à la conservation rapide de ces données relatives au trafic, qu'un seul ou plusieurs fournisseurs de services aient participé à la transmission de cette communication ; et

b pour assurer la divulgation rapide à l'autorité compétente de la Partie, ou à une personne désignée par cette autorité, d'une quantité suffisante de données relatives au trafic pour permettre l'identification par la Partie des fournisseurs de services et de la voie par laquelle la communication a été transmise.

2 Les pouvoirs et procédures mentionnés dans le présent article doivent être soumis aux articles 14 et 15.

Titre 3 – Injonction de produire

Article 18 – Injonction de produire

1 Chaque Partie adopte les mesures législatives et autres qui se révèlent nécessaires pour habiliter ses autorités compétentes à ordonner :

a à une personne présente sur son territoire de communiquer les données informatiques spécifiées, en sa possession ou sous son contrôle, qui sont stockées dans un système informatique ou un support de stockage informatique ; et

b à un fournisseur de services offrant des prestations sur le territoire de la Partie, de communiquer les données en sa possession ou sous son contrôle relatives aux abonnés et concernant de tels services.

2 Les pouvoirs et procédures mentionnés dans le présent article doivent être soumis aux articles 14 et 15.

3 Aux fins du présent article, l'expression « données relatives aux abonnés » désigne toute information, sous forme de données informatiques ou sous toute autre forme, détenue par un fournisseur de services et se rapportant aux abonnés de ses services, autres que des données relatives au trafic ou au contenu, et permettant d'établir :

a le type de service de communication utilisé, les dispositions techniques prises à cet égard et la période de service ;

b l'identité, l'adresse postale ou géographique et le numéro de téléphone de l'abonné, et tout autre numéro d'accès, les données concernant la facturation et le paiement, disponibles sur la base d'un contrat ou d'un arrangement de services ;

c toute autre information relative à l'endroit où se trouvent les équipements de communication, disponible sur la base d'un contrat ou d'un arrangement de services.

Titre 4 – Perquisition et saisie de données informatiques stockées

Article 19 – Perquisition et saisie de données informatiques stockées

1 Chaque Partie adopte les mesures législatives et autres qui se révèlent nécessaires pour habiliter ses autorités compétentes à perquisitionner ou à accéder d'une façon similaire :

a à un système informatique ou à une partie de celui-ci ainsi qu'aux données informatiques qui y sont stockées ; et

b à un support du stockage informatique permettant de stocker des données informatiques

sur son territoire.

2 Chaque Partie adopte les mesures législatives et autres qui se révèlent nécessaires pour veiller à ce que, lorsque ses autorités perquisitionnent ou accèdent d'une façon similaire à un système informatique spécifique ou à une partie de celui-ci, conformément au paragraphe 1.a, et ont des raisons de penser que les données recherchées sont stockées dans un autre système informatique ou dans une partie de celui-ci situé sur son territoire, et que ces données sont légalement accessibles à partir du système initial ou disponibles pour ce système initial, lesdites autorités soient en mesure d'étendre rapidement la perquisition ou l'accès d'une façon similaire à l'autre système.

3 Chaque Partie adopte les mesures législatives et autres qui se révèlent nécessaires pour habiliter ses autorités compétentes à saisir ou à obtenir d'une façon similaire les données informatiques pour lesquelles l'accès a été réalisé en application des paragraphes 1 ou 2. Ces mesures incluent les prérogatives suivantes :

a saisir ou obtenir d'une façon similaire un système informatique ou une partie de celui-ci, ou un support de stockage informatique ;

b réaliser et conserver une copie de ces données informatiques ;

c préserver l'intégrité des données informatiques stockées pertinentes ;

d rendre inaccessibles ou enlever ces données informatiques du système informatique consulté.

4 Chaque Partie adopte les mesures législatives et autres qui se révèlent nécessaires pour habiliter ses autorités compétentes à ordonner à toute personne connaissant le fonctionnement du système informatique ou les mesures appliquées pour protéger les données informatiques

qu'il contient de fournir toutes les informations raisonnablement nécessaires, pour permettre l'application des mesures visées par les paragraphes 1 et 2.

5 Les pouvoirs et procédures mentionnés dans cet article doivent être soumis aux articles 14 et 15.

Titre 5 – Collecte en temps réel de données informatiques

Article 20 – Collecte en temps réel des données relatives au trafic

1 Chaque Partie adopte les mesures législatives et autres qui se révèlent nécessaires pour habiliter ses autorités compétentes :

a à collecter ou enregistrer par l'application de moyens techniques existant sur son territoire, et

b à obliger un fournisseur de services, dans le cadre de ses capacités techniques existantes :

i à collecter ou à enregistrer par l'application de moyens techniques existant sur son territoire, ou

ii à prêter aux autorités compétentes son concours et son assistance pour collecter ou enregistrer,

en temps réel, les données relatives au trafic associées à des communications spécifiques transmises sur son territoire au moyen d'un système informatique.

2 Lorsqu'une Partie, en raison des principes établis de son ordre juridique interne, ne peut adopter les mesures énoncées au paragraphe 1.a, elle peut à la place, adopter les mesures législatives et autres qui se révèlent nécessaires pour assurer la collecte ou l'enregistrement en temps réel des données relatives au trafic associées à des communications spécifiques transmises sur son territoire par l'application de moyens techniques existant sur ce territoire.

3 Chaque Partie adopte les mesures législatives et autres qui se révèlent nécessaires pour obliger un fournisseur de services à garder secrets le fait que l'un quelconque des pouvoirs prévus dans le présent article a été exécuté ainsi que toute information à ce sujet.

4 Les pouvoirs et procédures mentionnés dans le présent article doivent être soumis aux articles 14 et 15.

Article 21 – Interception de données relatives au contenu

1 Chaque Partie adopte les mesures législatives et autres qui se révèlent nécessaires pour habiliter ses autorités compétentes en ce qui concerne un éventail d'infractions graves à définir en droit interne :

a à collecter ou à enregistrer par l'application de moyens techniques existant sur son territoire, et

b à obliger un fournisseur de services, dans le cadre de ses capacités techniques :

i à collecter ou à enregistrer par l'application de moyens techniques existant sur son territoire, ou

ii à prêter aux autorités compétentes son concours et son assistance pour collecter ou enregistrer,

en temps réel, les données relatives au contenu de communications spécifiques sur son territoire, transmises au moyen d'un système informatique.

2 Lorsqu'une Partie, en raison des principes établis dans son ordre juridique interne, ne peut adopter les mesures énoncées au paragraphe 1.a, elle peut à la place adopter les mesures législatives et autres qui se révèlent nécessaires pour assurer la collecte ou l'enregistrement en temps réel des données relatives au contenu de communications spécifiques transmises sur son territoire par l'application de moyens techniques existant sur ce territoire.

3 Chaque Partie adopte les mesures législatives et autres qui se révèlent nécessaires pour obliger un fournisseur de services à garder secrets le fait que l'un quelconque des pouvoirs prévus dans le présent article a été exécuté, ainsi que toute information à ce sujet.

4 Les pouvoirs et procédures mentionnés dans le présent article doivent être soumis aux articles 14 et 15.

Section 3 – Compétence

Article 22 – Compétence

1 Chaque Partie adopte les mesures législatives et autres qui se révèlent nécessaires pour établir sa compétence à l'égard de toute infraction pénale établie conformément aux articles 2 à 11 de la présente Convention, lorsque l'infraction est commise :

a sur son territoire ; ou

b à bord d'un navire battant pavillon de cette Partie ; ou

c à bord d'un aéronef immatriculé selon les lois de cette Partie ; ou

d par un de ses ressortissants, si l'infraction est punissable pénalement là où elle a été commise ou si l'infraction ne relève de la compétence territoriale d'aucun Etat.

2 Chaque Partie peut se réserver le droit de ne pas appliquer, ou de n'appliquer que dans des cas ou des conditions spécifiques, les règles de compétence définies aux paragraphes 1.b à 1.d du présent article ou dans une partie quelconque de ces paragraphes.

3 Chaque Partie adopte les mesures qui se révèlent nécessaires pour établir sa compétence à l'égard de toute infraction mentionnée à l'article 24, paragraphe 1, de la présente Convention, lorsque l'auteur présumé de l'infraction est présent sur son territoire et ne peut être extradé vers une autre Partie au seul titre de sa nationalité, après une demande d'extradition.

4 La présente Convention n'exclut aucune compétence pénale exercée par une Partie conformément à son droit interne.

5 Lorsque plusieurs Parties revendiquent une compétence à l'égard d'une infraction présumée visée dans la présente Convention, les Parties concernées se concertent, lorsque cela est opportun, afin de déterminer la mieux à même d'exercer les poursuites.

Chapitre III – Coopération internationale

Section 1 – Principes généraux

Titre 1 – Principes généraux relatifs à la coopération internationale

Article 23 – Principes généraux relatifs à la coopération internationale

Les Parties coopèrent les unes avec les autres, conformément aux dispositions du présent chapitre, en application des instruments internationaux pertinents sur la coopération

internationale en matière pénale, des arrangements reposant sur des législations uniformes ou réciproques et de leur droit national, dans la mesure la plus large possible, aux fins d'investigations ou de procédures concernant les infractions pénales liées à des systèmes et des données informatiques ou pour recueillir les preuves, sous forme électronique, d'une infraction pénale.

Titre 2 – Principes relatifs à l'extradition

Article 24 – Extradition

1 a Le présent article s'applique à l'extradition entre les Parties pour les infractions pénales définies conformément aux articles 2 à 11 de la présente Convention, à condition qu'elles soient punissables dans la législation des deux Parties concernées par une peine privative de liberté pour une période maximale d'au moins un an, ou par une peine plus sévère.

b Lorsqu'il est exigé une peine minimale différente, sur la base d'un traité d'extradition tel qu'applicable entre deux ou plusieurs parties, y compris la Convention européenne d'extradition (STE n° 24), ou d'un arrangement reposant sur des législations uniformes ou réciproques, la peine minimale prévue par ce traité ou cet arrangement s'applique.

2 Les infractions pénales décrites au paragraphe 1 du présent article sont considérées comme incluses en tant qu'infractions pouvant donner lieu à extradition dans tout traité d'extradition existant entre ou parmi les Parties. Les Parties s'engagent à inclure de telles infractions comme infractions pouvant donner lieu à extradition dans tout traité d'extradition pouvant être conclu entre ou parmi elles.

3 Lorsqu'une Partie conditionne l'extradition à l'existence d'un traité et reçoit une demande d'extradition d'une autre Partie avec laquelle elle n'a pas conclu de traité d'extradition, elle peut considérer la présente Convention comme fondement juridique pour l'extradition au regard de toute infraction pénale mentionnée au paragraphe 1 du présent article.

4 Les Parties qui ne conditionnent pas l'extradition à l'existence d'un traité reconnaissent les infractions pénales mentionnées au paragraphe 1 du présent article comme des infractions pouvant donner lieu entre elles à l'extradition.

5 L'extradition est soumise aux conditions prévues par le droit interne de la Partie requise ou par les traités d'extradition en vigueur, y compris les motifs pour lesquels la Partie requise peut refuser l'extradition.

6 Si l'extradition pour une infraction pénale mentionnée au paragraphe 1 du présent article est refusée uniquement sur la base de la nationalité de la personne recherchée ou parce que la Partie requise s'estime compétente pour cette infraction, la Partie requise soumet l'affaire, à la demande de la Partie requérante, à ses autorités compétentes aux fins de poursuites, et rendra compte, en temps utile, de l'issue de l'affaire à la Partie requérante. Les autorités en question prendront leur décision et mèneront l'enquête et la procédure de la même manière que pour toute autre infraction de nature comparable, conformément à la législation de cette Partie.

7 a Chaque Partie communique au Secrétaire Général du Conseil de l'Europe, au moment de la signature ou du dépôt de son instrument de ratification, d'acceptation, d'approbation ou d'adhésion, le nom et l'adresse de chaque autorité responsable de l'envoi ou de la réception d'une demande d'extradition ou d'arrestation provisoire, en l'absence de traité.

b Le Secrétaire Général du Conseil de l'Europe établit et tient à jour un registre des autorités ainsi désignées par les Parties. Chaque Partie doit veiller en permanence à l'exactitude des données figurant dans le registre.

Titre 3 – Principes généraux relatifs à l'entraide

Article 25 – Principes généraux relatifs à l'entraide

1 Les Parties s'accordent l'entraide la plus large possible aux fins d'investigations ou de procédures concernant les infractions pénales liées à des systèmes et à des données informatiques, ou afin de recueillir les preuves sous forme électronique d'une infraction pénale.

2 Chaque Partie adopte également les mesures législatives et autres qui se révèlent nécessaires pour s'acquitter des obligations énoncées aux articles 27 à 35.

3 Chaque Partie peut, en cas d'urgence, formuler une demande d'entraide ou les communications s'y rapportant par des moyens rapides de communication, tels que la télécopie ou le courrier électronique, pour autant que ces moyens offrent des conditions suffisantes de sécurité et d'authentification (y compris, si nécessaire, le cryptage), avec confirmation officielle ultérieure si l'État requis l'exige. L'État requis accepte la demande et y répond par n'importe lequel de ces moyens rapides de communication.

4 Sauf disposition contraire expressément prévue dans les articles du présent chapitre, l'entraide est soumise aux conditions fixées par le droit interne de la Partie requise ou par les traités d'entraide applicables, y compris les motifs sur la base desquels la Partie requise peut refuser la coopération. La Partie requise ne doit pas exercer son droit de refuser l'entraide concernant les infractions visées aux articles 2 à 11 au seul motif que la demande porte sur une infraction qu'elle considère comme de nature fiscale.

5 Lorsque, conformément aux dispositions du présent chapitre, la Partie requise est autorisée à subordonner l'entraide à l'existence d'une double incrimination, cette condition sera considérée comme satisfaite si le comportement constituant l'infraction, pour laquelle l'entraide est requise, est qualifié d'infraction pénale par son droit interne, que le droit interne classe ou non l'infraction dans la même catégorie d'infractions ou qu'il la désigne ou non par la même terminologie que le droit de la Partie requérante.

Article 26 – Information spontanée

1 Une Partie peut, dans les limites de son droit interne et en l'absence de demande préalable, communiquer à une autre Partie des informations obtenues dans le cadre de ses propres enquêtes lorsqu'elle estime que cela pourrait aider la Partie destinataire à engager ou à mener à bien des enquêtes ou des procédures au sujet d'infractions pénales établies conformément à la présente Convention, ou lorsque ces informations pourraient aboutir à une demande de coopération formulée par cette Partie au titre du présent chapitre.

2 Avant de communiquer de telles informations, la Partie qui les fournit peut demander qu'elles restent confidentielles ou qu'elles ne soient utilisées qu'à certaines conditions. Si la Partie destinataire ne peut faire droit à cette demande, elle doit en informer l'autre Partie, qui devra alors déterminer si les informations en question devraient néanmoins être fournies. Si la Partie destinataire accepte les informations aux conditions prescrites, elle sera liée par ces dernières.

Titre 4 – Procédures relatives aux demandes d'entraide en l'absence d'accords internationaux applicables

Article 27 – Procédures relatives aux demandes d'entraide en l'absence d'accords internationaux applicables

1 En l'absence de traité d'entraide ou d'arrangement reposant sur des législations uniformes ou réciproques en vigueur entre la Partie requérante et la Partie requise, les dispositions des paragraphes 2 à 9 du présent article s'appliquent. Elles ne s'appliquent pas lorsqu'un traité, un arrangement ou une législation de ce type existent, à moins que les Parties concernées ne décident d'appliquer à la place tout ou partie du reste de cet article.

2 a Chaque Partie désigne une ou plusieurs autorités centrales chargées d'envoyer les demandes d'entraide ou d'y répondre, de les exécuter ou de les transmettre aux autorités compétentes pour leur exécution ;

b Les autorités centrales communiquent directement les unes avec les autres ;

c Chaque Partie, au moment de la signature ou du dépôt de ses instruments de ratification, d'acceptation, d'approbation ou d'adhésion, communique au Secrétaire Général du Conseil de l'Europe les noms et adresses des autorités désignées en application du présent paragraphe ;

d Le Secrétaire Général du Conseil de l'Europe établit et tient à jour un registre des autorités centrales désignées par les Parties. Chaque Partie veille en permanence à l'exactitude des données figurant dans le registre.

3 Les demandes d'entraide sous le présent article sont exécutées conformément à la procédure spécifiée par la Partie requérante, sauf lorsqu'elle est incompatible avec la législation de la Partie requise.

4 Outre les conditions ou les motifs de refus prévus à l'article 25, paragraphe 4, l'entraide peut être refusée par la Partie requise :

a si la demande porte sur une infraction que la Partie requise considère comme étant de nature politique ou liée à une infraction de nature politique ; ou

b si la Partie requise estime que le fait d'accéder à la demande risquerait de porter atteinte à sa souveraineté, à sa sécurité, à son ordre public ou à d'autres intérêts essentiels.

5 La Partie requise peut surseoir à l'exécution de la demande si cela risquerait de porter préjudice à des enquêtes ou procédures conduites par ses autorités.

6 Avant de refuser ou de différer sa coopération, la Partie requise examine, après avoir le cas échéant consulté la Partie requérante, s'il peut être fait droit à la demande partiellement, ou sous réserve des conditions qu'elle juge nécessaires.

7 La Partie requise informe rapidement la Partie requérante de la suite qu'elle entend donner à la demande d'entraide. Elle doit motiver son éventuel refus d'y faire droit ou l'éventuel ajournement de la demande. La Partie requise informe également la Partie requérante de tout motif rendant l'exécution de l'entraide impossible ou étant susceptible de la retarder de manière significative.

8 La Partie requérante peut demander que la Partie requise garde confidentiels le fait et l'objet de toute demande formulée au titre du présent chapitre, sauf dans la mesure nécessaire à l'exécution de ladite demande. Si la Partie requise ne peut faire droit à cette demande de confidentialité, elle doit en informer rapidement la Partie requérante, qui devra alors déterminer si la demande doit néanmoins être exécutée.

9 a En cas d'urgence, les autorités judiciaires de la Partie requérante peuvent adresser directement à leurs homologues de la Partie requise les demandes d'entraide ou les communications s'y rapportant. Dans un tel cas, copie est adressée simultanément aux autorités centrales de la Partie requise par le biais de l'autorité centrale de la Partie requérante.

b Toute demande ou communication formulée au titre du présent paragraphe peut l'être par l'intermédiaire de l'Organisation internationale de police criminelle (Interpol).

c Lorsqu'une demande a été formulée en application de l'alinéa a. du présent article et lorsque l'autorité n'est pas compétente pour la traiter, elle la transmet à l'autorité nationale compétente et en informe directement la Partie requérante.

d Les demandes ou communications effectuées en application du présent paragraphe qui ne supposent pas de mesure de coercition peuvent être directement transmises par les autorités compétentes de la Partie requérante aux autorités compétentes de la Partie requise.

e Chaque Partie peut informer le Secrétaire Général du Conseil de l'Europe, au moment de la signature ou du dépôt de son instrument de ratification, d'acceptation, d'approbation ou d'adhésion, que, pour des raisons d'efficacité, les demandes faites sous ce paragraphe devront être adressées à son autorité centrale.

Article 28 – Confidentialité et restriction d'utilisation

1 En l'absence de traité d'entraide ou d'arrangement reposant sur des législations uniformes ou réciproques en vigueur entre la Partie requérante et la Partie requise, les dispositions du présent article s'appliquent. Elles ne s'appliquent pas lorsqu'un traité, un arrangement ou une législation de ce type existent, à moins que les Parties concernées ne décident d'appliquer à la place tout ou partie du présent article.

2 La Partie requise peut subordonner la communication d'informations ou de matériels en réponse à une demande :

a à la condition que ceux-ci restent confidentiels lorsque la demande d'entraide ne pourrait être respectée en l'absence de cette condition ; ou

b à la condition qu'ils ne soient pas utilisés aux fins d'enquêtes ou de procédures autres que celles indiquées dans la demande.

3 Si la Partie requérante ne peut satisfaire à l'une des conditions énoncées au paragraphe 2, elle en informe rapidement la Partie requise, qui détermine alors si l'information doit néanmoins être fournie. Si la Partie requérante accepte cette condition, elle sera liée par celle-ci.

4 Toute Partie qui fournit des informations ou du matériel soumis à l'une des conditions énoncées au paragraphe 2 peut exiger de l'autre Partie qu'elle lui communique des précisions, en relation avec cette condition, quant à l'usage fait de ces informations ou de ce matériel.

Section 2 – Dispositions spécifiques

Titre 1 – Entraide en matière de mesures provisoires

Article 29 – Conservation rapide de données informatiques stockées

1 Une Partie peut demander à une autre Partie d'ordonner ou d'imposer d'une autre façon la conservation rapide de données stockées au moyen d'un système informatique se trouvant sur le territoire de cette autre Partie, et au sujet desquelles la Partie requérante a l'intention de soumettre une demande d'entraide en vue de la perquisition ou de l'accès par un moyen similaire, de la saisie ou de l'obtention par un moyen similaire, ou de la divulgation desdites données.

2 Une demande de conservation faite en application du paragraphe 1 doit préciser :

a l'autorité qui demande la conservation ;

b l'infraction faisant l'objet de l'enquête ou de procédures pénales et un bref exposé des faits qui s'y rattachent ;

c les données informatiques stockées à conserver et la nature de leur lien avec l'infraction ;

d toutes les informations disponibles permettant d'identifier le gardien des données informatiques stockées ou l'emplacement du système informatique ;

e la nécessité de la mesure de conservation ; et

f le fait que la Partie entend soumettre une demande d'entraide en vue de la perquisition ou de l'accès par un moyen similaire, de la saisie ou de l'obtention par un moyen similaire, ou de la divulgation des données informatiques stockées.

3 Après avoir reçu la demande d'une autre Partie, la Partie requise doit prendre toutes les mesures appropriées afin de procéder sans délai à la conservation des données spécifiées, conformément à son droit interne. Pour pouvoir répondre à une telle demande, la double incrimination n'est pas requise comme condition préalable à la conservation.

4 Une Partie qui exige la double incrimination comme condition pour répondre à une demande d'entraide visant la perquisition ou l'accès similaire, la saisie ou l'obtention par un moyen similaire ou la divulgation des données stockées peut, pour des infractions autres que celles établies conformément aux articles 2 à 11 de la présente Convention, se réserver le droit de refuser la demande de conservation au titre du présent article dans le cas où elle a des raisons de penser que, au moment de la divulgation, la condition de double incrimination ne pourra pas être remplie.

5 En outre, une demande de conservation peut être refusée uniquement :

a si la demande porte sur une infraction que la Partie requise considère comme étant de nature politique ou liée à une infraction de nature politique ; ou

b si la Partie requise estime que le fait d'accéder à la demande risquerait de porter atteinte à sa souveraineté, à sa sécurité, à l'ordre public ou à d'autres intérêts essentiels.

6 Lorsque la Partie requise estime que la conservation simple ne suffira pas à garantir la disponibilité future des données, ou compromettra la confidentialité de l'enquête de la Partie requérante, ou nuira d'une autre façon à celle-ci, elle en informe rapidement la Partie requérante, qui décide alors s'il convient néanmoins d'exécuter la demande.

7 Toute conservation effectuée en réponse à une demande visée au paragraphe 1 sera valable pour une période d'au moins soixante jours afin de permettre à la Partie requérante de soumettre une demande en vue de la perquisition ou de l'accès par un moyen similaire, de la saisie ou de l'obtention par un moyen similaire, ou de la divulgation des données. Après la réception d'une telle demande, les données doivent continuer à être conservées en attendant l'adoption d'une décision concernant la demande.

Article 30 – Divulgation rapide de données conservées

1 Lorsque, en exécutant une demande de conservation de données relatives au trafic concernant une communication spécifique formulée en application de l'article 29, la Partie requise découvre qu'un fournisseur de services dans un autre Etat a participé à la transmission de cette communication, la Partie requise divulgue rapidement à la Partie requérante une quantité suffisante de données concernant le trafic, aux fins d'identifier ce fournisseur de services et la voie par laquelle la communication a été transmise.

2 La divulgation de données relatives au trafic en application du paragraphe 1 peut être refusée seulement :

a si la demande porte sur une infraction que la Partie requise considère comme étant de nature politique ou liée à une infraction de nature politique ; ou

b si elle considère que le fait d'accéder à la demande risquerait de porter atteinte à sa souveraineté, à sa sécurité, à son ordre public ou à d'autres intérêts essentiels.

Titre 2 – Entraide concernant les pouvoirs d'investigation

Article 31 – Entraide concernant l'accès aux données stockées

1 Une Partie peut demander à une autre Partie de perquisitionner ou d'accéder de façon similaire, de saisir ou d'obtenir de façon similaire, de divulguer des données stockées au moyen d'un système informatique se trouvant sur le territoire de cette autre Partie, y compris les données conservées conformément à l'article 29.

2 La Partie requise satisfait à la demande en appliquant les instruments internationaux, les arrangements et les législations mentionnés à l'article 23, et en se conformant aux dispositions pertinentes du présent chapitre.

3 La demande doit être satisfaite aussi rapidement que possible dans les cas suivants :

a il y a des raisons de penser que les données pertinentes sont particulièrement sensibles aux risques de perte ou de modification ; ou

b les instruments, arrangements et législations visés au paragraphe 2 prévoient une coopération rapide.

Article 32 – Accès transfrontière à des données stockées, avec consentement ou lorsqu'elles sont accessibles au public

Une Partie peut, sans l'autorisation d'une autre Partie :

a accéder à des données informatiques stockées accessibles au public (source ouverte), quelle que soit la localisation géographique de ces données ; ou

b accéder à, ou recevoir au moyen d'un système informatique situé sur son territoire, des données informatiques stockées situées dans un autre Etat, si la Partie obtient le consentement légal et volontaire de la personne légalement autorisée à lui divulguer ces données au moyen de ce système informatique.

Article 33 – Entraide dans la collecte en temps réel de données relatives au trafic

1 Les Parties s'accordent l'entraide dans la collecte en temps réel de données relatives au trafic, associées à des communications spécifiées sur leur territoire, transmises au moyen d'un système informatique. Sous réserve des dispositions du paragraphe 2, cette entraide est régie par les conditions et les procédures prévues en droit interne.

2 Chaque Partie accorde cette entraide au moins à l'égard des infractions pénales pour lesquelles la collecte en temps réel de données concernant le trafic serait disponible dans une affaire analogue au niveau interne.

Article 34 – Entraide en matière d'interception de données relatives au contenu

Les Parties s'accordent l'entraide, dans la mesure permise par leurs traités et lois internes applicables, pour la collecte ou l'enregistrement en temps réel de données relatives au contenu de communications spécifiques transmises au moyen d'un système informatique.

Titre 3 – Réseau 24/7

Article 35 – Réseau 24/7

1 Chaque Partie désigne un point de contact joignable vingt-quatre heures sur vingt-quatre, sept jours sur sept, afin d'assurer une assistance immédiate pour des investigations concernant les infractions pénales liées à des systèmes et à des données informatiques, ou pour recueillir les

preuves sous forme électronique d'une infraction pénale. Cette assistance englobera la facilitation, ou, si le droit et la pratique internes le permettent, l'application directe des mesures suivantes :

a apport de conseils techniques ;

b conservation des données, conformément aux articles 29 et 30 ;

c recueil de preuves, apport d'informations à caractère juridique, et localisation des suspects.

2 a Le point de contact d'une Partie aura les moyens de correspondre avec le point de contact d'une autre Partie selon une procédure accélérée.

b Si le point de contact désigné par une Partie ne dépend pas de l'autorité ou des autorités de cette Partie responsables de l'entraide internationale ou de l'extradition, le point de contact veillera à pouvoir agir en coordination avec cette ou ces autorités, selon une procédure accélérée.

3 Chaque Partie fera en sorte de disposer d'un personnel formé et équipé en vue de faciliter le fonctionnement du réseau.

Chapitre IV – Clauses finales

Article 36 – Signature et entrée en vigueur

1 La présente Convention est ouverte à la signature des États membres du Conseil de l'Europe et des États non membres qui ont participé à son élaboration.

2 La présente Convention est soumise à ratification, acceptation ou approbation. Les instruments de ratification, d'acceptation ou d'approbation sont déposés près le Secrétaire Général du Conseil de l'Europe.

3 La présente Convention entrera en vigueur le premier jour du mois qui suit l'expiration d'une période de trois mois après la date à laquelle cinq États, incluant au moins trois États membres du Conseil de l'Europe, auront exprimé leur consentement à être liés par la Convention, conformément aux dispositions des paragraphes 1 et 2.

4 Pour tout État signataire qui exprimera ultérieurement son consentement à être lié par la Convention, celle-ci entrera en vigueur le premier jour du mois qui suit l'expiration d'une période de trois mois après la date de l'expression de son consentement à être lié par la Convention, conformément aux dispositions des paragraphes 1 et 2.

Article 37 – Adhésion à la Convention

1 Après l'entrée en vigueur de la présente Convention, le Comité des Ministres du Conseil de l'Europe peut, après avoir consulté les États contractants à la Convention et en avoir obtenu l'assentiment unanime, inviter tout État non membre du Conseil, n'ayant pas participé à son élaboration, à adhérer à la présente Convention. La décision est prise à la majorité prévue à l'article 20.d du Statut du Conseil de l'Europe et à l'unanimité des représentants des États contractants ayant le droit de siéger au Comité des Ministres.

2 Pour tout État adhérent à la Convention, conformément au paragraphe 1 ci-dessus, la Convention entrera en vigueur le premier jour du mois qui suit l'expiration d'une période de trois mois après la date de dépôt de l'instrument d'adhésion près le Secrétaire Général du Conseil de l'Europe.

Article 38 – Application territoriale

1 Tout État peut, au moment de la signature ou au moment du dépôt de son instrument de ratification, d'acceptation, d'approbation ou d'adhésion, désigner le ou les territoires auxquels s'appliquera la présente Convention.

2 Tout État peut, à tout autre moment par la suite, par déclaration adressée au Secrétaire Général du Conseil de l'Europe, étendre l'application de la présente Convention à tout autre territoire désigné dans la déclaration. La Convention entrera en vigueur à l'égard de ce territoire le premier jour du mois qui suit l'expiration d'une période de trois mois après la date de réception de la déclaration par le Secrétaire Général.

3 Toute déclaration faite en application des deux paragraphes précédents peut être retirée, en ce qui concerne tout territoire désigné dans cette déclaration, par notification adressée au Secrétaire Général du Conseil de l'Europe. Le retrait prendra effet le premier jour du mois qui suit l'expiration d'une période de trois mois après la date de réception de ladite notification par le Secrétaire Général.

Article 39 – Effets de la Convention

1 L'objet de la présente Convention est de compléter les traités ou les accords multilatéraux ou bilatéraux applicables existant entre les Parties, y compris les dispositions :

– de la Convention européenne d'extradition, ouverte à la signature le 13 décembre 1957, à Paris (STE n° 24) ;

– de la Convention européenne d'entraide judiciaire en matière pénale, ouverte à la signature le 20 avril 1959, à Strasbourg (STE n° 30) ;

– du Protocole additionnel à la Convention européenne d'entraide judiciaire en matière pénale, ouvert à la signature le 17 mars 1978, à Strasbourg (STE n° 99).

2 Si deux ou plusieurs Parties ont déjà conclu un accord ou un traité relatif aux matières traitées par la présente Convention, ou si elles ont autrement établi leurs relations sur ces sujets, ou si elles le feront à l'avenir, elles ont aussi la faculté d'appliquer ledit accord ou traité ou d'établir leurs relations en conséquence, au lieu de la présente Convention. Toutefois, lorsque les Parties établiront leurs relations relatives aux matières faisant l'objet de la présente Convention d'une manière différente de celle y prévue, elles le feront d'une manière qui ne soit pas incompatible avec les objectifs et les principes de la Convention.

3 Rien dans la présente Convention n'affecte d'autres droits, restrictions, obligations et responsabilités d'une Partie.

Article 40 – Déclarations

Par déclaration écrite adressée au Secrétaire Général du Conseil de l'Europe, tout État peut, au moment de la signature ou du dépôt de son instrument de ratification, d'acceptation, d'approbation ou d'adhésion, déclarer qu'il se prévaut de la faculté d'exiger, le cas échéant, un ou plusieurs éléments supplémentaires tels que prévus aux articles 2, 3, 6, paragraphe 1.b, 7, 9, paragraphe 3, et 27, paragraphe 9.e.

Article 41 – Clause fédérale

1 Un État fédéral peut se réserver le droit d'honorer les obligations contenues dans le chapitre II de la présente Convention dans la mesure où celles-ci sont compatibles avec les principes fondamentaux qui gouvernent les relations entre son gouvernement central et les États constituants ou autres entités territoriales analogues, à condition qu'il soit en mesure de coopérer sur la base du chapitre III.

2 Lorsqu'il fait une réserve prévue au paragraphe 1, un État fédéral ne saurait faire usage des termes d'une telle réserve pour exclure ou diminuer de manière substantielle ses obligations en vertu du chapitre II. En tout état de cause, il se dote de moyens étendus et effectifs permettant la mise en oeuvre des mesures prévues par ledit chapitre.

3 En ce qui concerne les dispositions de cette Convention dont l'application relève de la compétence législative de chacun des États constituants ou autres entités territoriales analogues, qui ne sont pas, en vertu du système constitutionnel de la fédération, tenus de prendre des mesures législatives, le gouvernement fédéral porte, avec son avis favorable, lesdites dispositions à la connaissance des autorités compétentes des États constituants, en les encourageant à adopter les mesures appropriées pour les mettre en œuvre.

Article 42 – Réserves

Par notification écrite adressée au Secrétaire Général du Conseil de l'Europe, tout État peut, au moment de la signature ou du dépôt de son instrument de ratification, d'acceptation, d'approbation ou d'adhésion, déclarer qu'il se prévaut de la ou les réserves prévues à l'article 4, paragraphe 2, à l'article 6, paragraphe 3, à l'article 9, paragraphe 4, à l'article 10, paragraphe 3, à l'article 11, paragraphe 3, à l'article 14, paragraphe 3, à l'article 22, paragraphe 2, à l'article 29, paragraphe 4, et à l'article 41, paragraphe 1. Aucune autre réserve ne peut être faite.

Article 43 – Statut et retrait des réserves

1 Une Partie qui a fait une réserve conformément à l'article 42 peut la retirer en totalité ou en partie par notification adressée au Secrétaire Général du Conseil de l'Europe. Ce retrait prend effet à la date de réception de ladite notification par le Secrétaire Général. Si la notification indique que le retrait d'une réserve doit prendre effet à une date précise, et si cette date est postérieure à celle à laquelle le Secrétaire Général reçoit la notification, le retrait prend effet à cette date ultérieure.

2 Une Partie qui a fait une réserve comme celles mentionnées à l'article 42 retire cette réserve, en totalité ou en partie, dès que les circonstances le permettent.

3 Le Secrétaire Général du Conseil de l'Europe peut périodiquement demander aux Parties ayant fait une ou plusieurs réserves comme celles mentionnées à l'article 42 des informations sur les perspectives de leur retrait.

Article 44 – Amendements

1 Des amendements à la présente Convention peuvent être proposés par chaque Partie, et sont communiqués par le Secrétaire Général du Conseil de l'Europe aux États membres du Conseil de l'Europe, aux États non membres ayant pris part à l'élaboration de la présente Convention, ainsi qu'à tout État y ayant adhéré ou ayant été invité à y adhérer, conformément aux dispositions de l'article 37.

2 Tout amendement proposé par une Partie est communiqué au Comité européen pour les problèmes criminels (CDPC), qui soumet au Comité des Ministres son avis sur ledit amendement.

3 Le Comité des Ministres examine l'amendement proposé et l'avis soumis par le CDPC et, après consultation avec les États non membres parties à la présente Convention, peut adopter l'amendement.

4 Le texte de tout amendement adopté par le Comité des Ministres conformément au paragraphe 3 du présent article est communiqué aux Parties pour acceptation.

5 Tout amendement adopté conformément au paragraphe 3 du présent article entre en vigueur le trentième jour après que toutes les Parties ont informé le Secrétaire Général de leur acceptation.

Article 45 – Règlement des différends

1 Le Comité européen pour les problèmes criminels du Conseil de l'Europe (CDPC) est tenu informé de l'interprétation et de l'application de la présente Convention.

2 En cas de différend entre les Parties sur l'interprétation ou l'application de la présente Convention, les Parties s'efforceront de parvenir à un règlement du différend par la négociation ou par tout autre moyen pacifique de leur choix, y compris la soumission du différend au CDPC, à un tribunal arbitral qui prendra des décisions qui lieront les Parties au différend, ou à la Cour internationale de justice, selon un accord entre les Parties concernées.

Article 46 – Concertation des Parties

1 Les Parties se concertent périodiquement, au besoin, afin de faciliter :

a l'usage et la mise en œuvre effectifs de la présente Convention, y compris l'identification de tout problème en la matière, ainsi que les effets de toute déclaration ou réserve faite conformément à la présente Convention ;

b l'échange d'informations sur les nouveautés juridiques, politiques ou techniques importantes observées dans le domaine de la criminalité informatique et la collecte de preuves sous forme électronique ;

c l'examen de l'éventualité de compléter ou d'amender la Convention.

2 Le Comité européen pour les problèmes criminels (CDPC) est tenu périodiquement au courant du résultat des concertations mentionnées au paragraphe 1.

3 Le CDPC facilite, au besoin, les concertations mentionnées au paragraphe 1 et adopte les mesures nécessaires pour aider les Parties dans leurs efforts visant à compléter ou amender la Convention. Au plus tard à l'issue d'un délai de trois ans à compter de l'entrée en vigueur de la présente Convention, le CDPC procédera, en coopération avec les Parties, à un réexamen de l'ensemble des dispositions de la Convention et proposera, le cas échéant, les amendements appropriés.

4 Sauf lorsque le Conseil de l'Europe les prend en charge, les frais occasionnés par l'application des dispositions du paragraphe 1 sont supportés par les Parties, de la manière qu'elles déterminent.

5 Les Parties sont assistées par le Secrétariat du Conseil de l'Europe dans l'exercice de leurs fonctions découlant du présent article.

Article 47 – Dénonciation

1 Toute Partie peut, à tout moment, dénoncer la présente Convention par notification au Secrétaire Général du Conseil de l'Europe.

2 La dénonciation prendra effet le premier jour du mois qui suit l'expiration d'une période de trois mois après la date de réception de la notification par le Secrétaire Général.

Article 48 – Notification

Le Secrétaire Général du Conseil de l'Europe notifie aux États membres du Conseil de l'Europe, aux États non membres ayant pris part à l'élaboration de la présente Convention, ainsi qu'à tout État y ayant adhéré ou ayant été invité à y adhérer :

a toute signature ;

b le dépôt de tout instrument de ratification, d'acceptation, d'approbation ou d'adhésion ;

c toute date d'entrée en vigueur de la présente Convention, conformément à ses articles 36 et 37 ;

d toute déclaration faite en application de l'article 40 ou toute réserve faite en application de l'article 42 :

e tout autre acte, notification ou communication ayant trait à la présente Convention.

En foi de quoi, les soussignés, dûment autorisés à cet effet, ont signé la présente Convention.

Fait à Budapest, le 23 novembre 2001, en français et en anglais, les deux textes faisant également foi, en un seul exemplaire qui sera déposé dans les archives du Conseil de l'Europe. Le Secrétaire Général du Conseil de l'Europe en communiquera copie certifiée conforme à chacun des États membres du Conseil de l'Europe, aux États non membres qui ont participé à l'élaboration de la Convention et à tout État invité à y adhérer.