CLUSIF

L'ESPRIT DE L'ÉCHANGE

Politiques de sécurité des systèmes d'information et sinistralité en France

Bilan 2003

- Huit regards sur l'actualité
- Trois focus

CLUB DE LA SÉCURITÉ DES SYSTÈMES D'INFORMATION FRANÇAIS

Remerciements

Le Clusif remercie les personnes qui ont participé à cette étude :

Ace Europe	Pascal Lointier
CIO	Philippe Rosé
Clusif	Marie-Agnès Couwez
Expertel Consulting	Stéphane Surget Roué
IRCGN	Eric Freyssinet
La Poste	Frédéric Chavoutier
Ministère de l'Economie, des Finances et de l'Industrie Service du HFD	Claude Maudelonde
Mission de liaison Gendarmerie à la DGPN	Joël Ferry
Molines Consultants	Gérard Molines

Enquête statistique réalisée pour le Clusif par le cabinet GMV Conseil.

Rédaction : Marie-Agnès Couwez

Éditorial

Une entreprise organisée aujourd'hui sans informatique a peu de chance de survivre dans les dix ans à venir. Le système d'information et ses connections avec d'autres réseaux participe fortement à la valeur d'une entité, à l'atteinte de ses objectifs, à l'augmentation de sa productivité.

Une politique globale de sécurité bien comprise protège le système en lui-même mais plus largement l'information. Ces deux aspects, numérique et non numérique, que peut recouvrir une même donnée sont indissociables et le facteur commun est l'humain, éternel «maillon faible».

C'est dans ce contexte que le Clusif présente, sous un angle nouveau, l'état des lieux des politiques de sécurité en France et de la sinistralité. Les *Regards sur l'actualité*, accompagnés de recommandations, comme le focus sur les entreprises de 200 à 500 salariés, permettent à un utilisateur de se positionner sur des thématiques ou un secteur d'activité. Les offreurs de produits ou de services de sécurité peuvent aussi identifier les axes où doivent porter les efforts.

La protection de l'information, des données et du système d'information, concerne toutes les entreprises sans exception. La prise de conscience de l'importance du patrimoine informationnel est très insuffisante en France. Les actions pédagogiques menées en ce sens par les services de l'Etat auprès des entreprises en témoignent.
Il serait illusoire et surtout dangereux de penser que les pratiques européennes et mondiales de fraude, de chantage ou d'espionnage économique et industriel s'arrêtent à nos frontières.

Sous un autre angle, les conclusions de la mission parlementaire menée par Jean-Paul Charié font état de l'arrêt des investissements des PME dans les nouvelles technologies, avec pour conséquence leur perte de compétitivité au plan européen. Cela n'a rien d'une fatalité mais appelle des actions. Il s'agit de lutter contre la peur du changement, d'expliquer les enjeux, de faire valoir les opportunités.

Il revient à chaque professionnel de la sécurité de démontrer l'intérêt des moyens numériques pour la compétitivité des entreprises et la nécessité de protéger son patrimoine. Comme pour toute technologie ou invention, les risques liés ne doivent pas freiner les développements. Le discours facile de la peur ne doit pas prendre le pas sur le devoir d'information et d'accompagnement.

Les actions à mener et pour lesquelles le Clusif continuera d'apporter sa contribution peuvent se résumer par :

FORMER ET RELAYER LA BONNE INFORMATION

Table des Matières

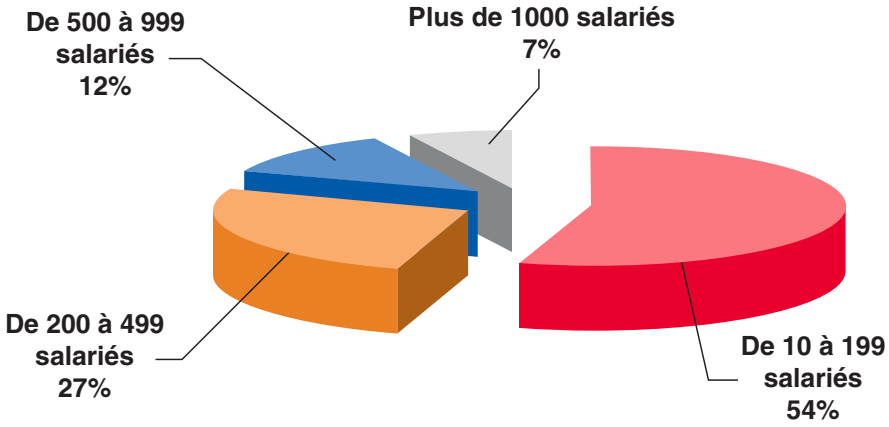
MÉTHODOLOGIE

Les réponses à l'enquête statistique émanent de 608 entreprises et de 111 collectivités publiques.
Le recueil des données s'est effectué essentiellement par des entretiens téléphoniques, à partir d'un questionnaire adressé par fax.

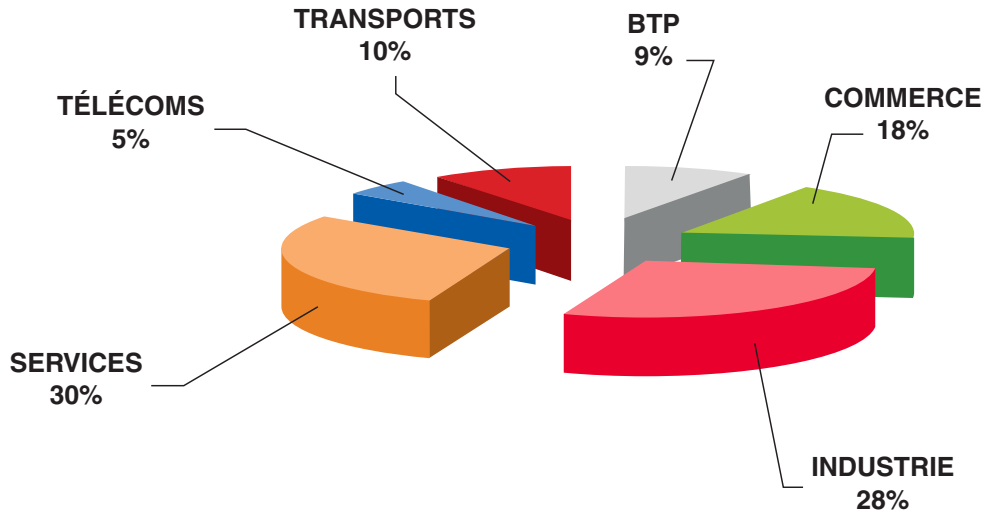
Entreprises

Le choix de l'échantillon prend deux critères en compte : l'effectif et le secteur d'activité.

Répartition par effectif :



Répartition par secteur d'activité :



Les données des entreprises sont redressées à partir des fichiers de l'INSEE (Institut National de la Statistique et des Etudes Economiques) en fonction du poids réel des secteurs et des effectifs dans l'économie française.

	De 10 à 199 salariés	De 200 à 499 salariés	De 500 à 999 salariés	Plus de 1.000 salariés	Total	Total en %	Données INSEE
BTP	42	10	2	0	54	9 %	12 %
COMMERCE	72	29	8	3	112	18 %	25 %
INDUSTRIE	83	43	26	22	174	28 %	25 %
SERVICES	78	60	30	11	179	29 %	27 %
TÉLÉCOMS	16	5	6	3	30	5 %	2 %
TRANSPORTS	40	15	3	1	59	10 %	9 %
Total	331	162	75	40	608		
Total en %	54 %	27 %	12 %	7 %			

Données INSEE	96 %	2 %	1%	1 %

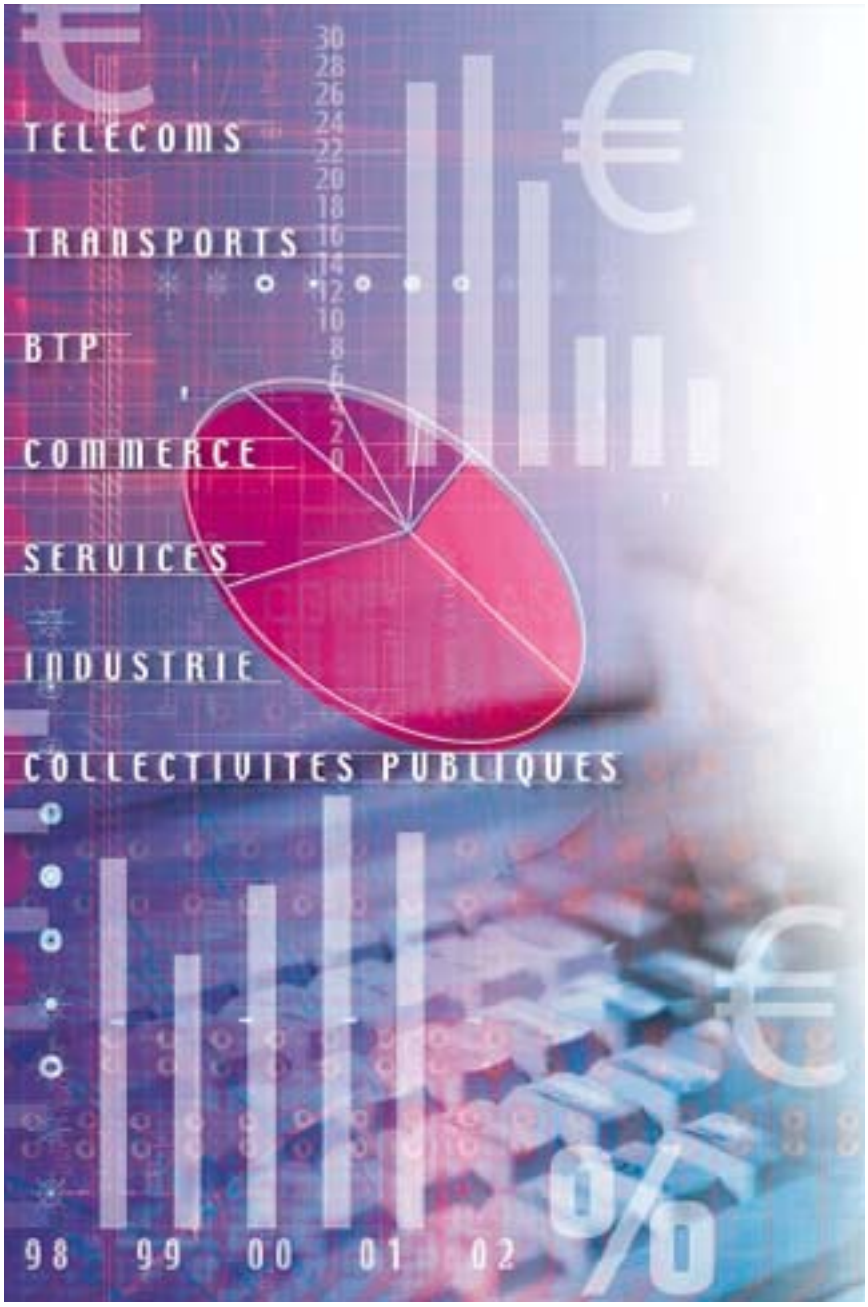
Collectivités publiques

Afin que l'échantillon soit plus représentatif, cette étude ne prend en compte que deux catégories : les collectivités locales et territoriales et les établissements hospitaliers.

L'échantillon a été redressé sur la base des effectifs de la fonction publique.

	Total	Total en %	Effectifs de la Fonction Publique
COLLECTIVITÉS LOCALES, TERRITORIALES	55	50 %	61 %
ÉTABLISSEMENTS HOSPITALIERS	55	50 %	39 %
	111	100 %	100 %

REGARDS SUR L'ACTUALITÉ



Les huit thèmes sélectionnés pour cette première partie représentent soit des tendances en matière de technologie, de comportement, d'organisation, soit des sujets sur ou sous évalués par les entreprises ou les médias en 2003 et au début de l'année 2004.
Nous mettons en perspective quelques réponses recueillies lors de l'enquête avec notre vision sur le sujet traité.

Déploiement du WiFi : quelle sécurité ?

L'installation d'un réseau sans fil concerne, en moyenne nationale, 8 % des entreprises. Ce réseau est chiffré dans seulement 40 % des cas. Ce nombre résume à lui seul la faible prise en compte de la sécurité dans ces déploiements et l'absence de calcul d'impact d'un incident ou d'un sinistre sur ce type de réseau.

La répartition par effectif ou par secteur n'est pas homogène ainsi que l'indiquent les tableaux suivants :

Mise en place d'un réseau WiFi :

Effectifs :			
10 à 199	200 à 499	500 à 999	Plus de 1000
8 %	25 %	20 %	33 %

Secteurs :					
BTP	Commerce	Industrie	Services	Télécoms	Transports
2 %	6 %	7 %	14 %	16 %	8 %

Le point de vue du Clusif

Plusieurs caractéristiques et phénomènes militent en faveur du développement des réseaux sans fil : la facilité d'installation, la mobilité à l'intérieur des bâtiments de l'entreprise, le nomadisme de certains salariés, le faible coût apparent de la mise en œuvre, la notion de service rendu pour des clients…
Cependant, dans l'état actuel de la technologie proposée, la confidentialité de la transmission des données et son intégrité ne sont pas garanties.
Qu'en est-il alors de la confidentialité des messageries ou même des fichiers en cas de connexion au réseau de l'entreprise [1] ? Le risque de détournement de données est bien réel. L'accès par une personne non autorisée et/ou malveillante aux fichiers des Ressources Humaines, par exemple, peut entraîner la responsabilité juridique de l'entité puisque obligation lui est faite par la Loi d'assurer la sécurité des données à caractère personnel.
Le détournement peut aussi concerner des données confidentielles comme des renseignements financiers, commerciaux ou stratégiques.
La norme en vigueur 802.11 (a, b, g) comporte des faiblesses, progressivement corrigées, quant à l'authentification et à la robustesse du chiffrement utilisé.
La normalisation en cours 802.11i, avec le label associé WPA (Wi-Fi Protected Access) améliorera l'authentification et assurera la gestion dynamique des clefs (TKIP -Temporal Key Integrity Protocol-).

[1] Cf Panorama 2003 de la cybercriminalité pour les malveillances avérées via un réseau WiFi

Recommandations :

Pour parer aux lacunes actuelles de cette technologie, des mesures doivent être prises sur les plans technique, organisationnel et humain :

- ☞ la politique de déploiement doit être l'aboutissement d'un travail de concertation entre la direction générale et la direction informatique (ou les personnes en charge de l'informatique),
- ☞ le réseau WiFi doit être sécurisé par la mise en œuvre d'un réseau privé virtuel (VPN),
- ☞ les personnes en charge de l'informatique s'assurent qu'il n'existe pas de déploiement sauvage,
- ☞ les conséquences d'un déploiement sauvage peuvent amener :
  - * le non respect du cadre légal fixé par l'ART (Autorité de Régulation des Télécoms),
  - * l'intrusion sur un autre réseau sans fil avec le risque d'une plainte juridique de cette autre entité,
  - * la «mise à disposition» du PC qui peut ainsi servir de relais pour une attaque sur Internet et engager la responsabilité pénale de l'entreprise.
- ☞ ces conséquences doivent faire l'objet d'une communication particulière auprès de l'ensemble des salariés,
- ☞ pour aider les entreprises à maîtriser les risques, le Clusif a publié une fiche de synthèse «*Réseaux sans fil : menaces, enjeux et parades*» disponible sur : https://www.clusif.asso.fr/fr/production/ouvrages/pdf/RSF.pdf

Nomadisme et protection de l'information

L'accès distant pour les salariés mobiles est en progression de 7 points par rapport à l'an passé et atteint 25 % en moyenne nationale. L'effectif prime largement sur l'activité pour le développement de ce type d'accès.

Accès distant par effectif :	10 à 199	200 à 499	500 à 999	Plus de 1000
	24 %	51 %	71 %	77 %

Le point de vue du Clusif

Les terminaux mobiles, le nomadisme dans le monde du travail et les technologies liées sont en constante progression : développement du parc des ordinateurs portables, des PDA (agendas électroniques), des téléphones multi-fonctions, ayant tous comme point commun de se connecter à internet de n'importe quel lieu et, éventuellement, au réseau de l'entreprise, à son intranet.
Globalement, en matière de sécurisation, les technologies nomades arrivent en queue.

Deux problèmes majeurs se posent : la protection contre le vol physique du matériel et la sécurisation des accès distants. Contre le vol, la parade se situe essentiellement dans la sensibilisation forte, voire même la formation des utilisateurs. Trois populations sont particulièrement exposées : les cadres dirigeants, les commerciaux et les consultants. Le vol physique de l'ordinateur ou du PDA signifie la perte et/ou la divulgation de données vitales de l'entreprise, tels des documents commerciaux, des tarifs, des listes de clients ou de fournisseurs, une stratégie en cours d'élaboration… L'impact est réellement significatif pour les données personnelles telles que des références bancaires ou un numéro de Sécurité Sociale, comprenant le code d'accès internet, qui peuvent être stockées sur un PDA.

Un autre aspect est celui de la gestion de la sécurité sur ces postes. Il peut sembler étonnant que les entreprises acquièrent, parfois sans réel besoin, des ordinateurs portables plus chers que des postes fixes et plus difficiles à administrer en matière de sécurité, donc nécessitant des investissements humains et financiers supplémentaires. Nous reviendrons sur cet aspect dans le paragraphe traité ci-dessous consacré au Retour sur Investissement et son «adjoint» le RoSI, le retour sur investissement de sécurité.

Les difficultés de sécurisation sont principalement de quatre ordres :
- l'usage à titre personnel du portable de l'entreprise avec d'une part, le risque d'infection par virus et, d'autre part, le téléchargement de programmes qui peuvent se révéler incompatibles avec les applications professionnelles,
- la mise à jour de la sécurité du portable, qu'il s'agisse de l'antivirus ou de l'application des correctifs *(patchs),*
- la confidentialité des données (chiffrement),
- la disponibilité des données (sauvegarde).

Recommandations :

☞ l'affectation d'un ordinateur portable à un salarié doit s'accompagner d'une «feuille de vigilance» évoquant les risques exposés ci-dessus et les obligations de sécurité qui en découlent,

☞ la connexion hors réseau d'entreprise ne doit pas être autorisée s'il n'existe pas de réseau privé virtuel (VPN),

☞ la sauvegarde des données doit être réalisée au moyen d'un CD Rom réinscriptible ou d'une clé USB,

☞ le paramétrage des postes doit empêcher les installations sauvages de logiciels,

☞ si l'entreprise n'a pas les moyens de mettre en place des outils d'administration à distance, une procédure de mise à jour et de contrôle des postes doit être instaurée ; elle sera activée avant toute reconnexion au réseau de l'entreprise,

☞ les moyens d'authentification électronique (carte à puce, biométrie, mot de passe de session unique *(token)*…) sont à privilégier. Ils assurent une robustesse des accès au disque dur,

☞ chiffrer le support, éventuellement partiellement, pour les données sensibles.

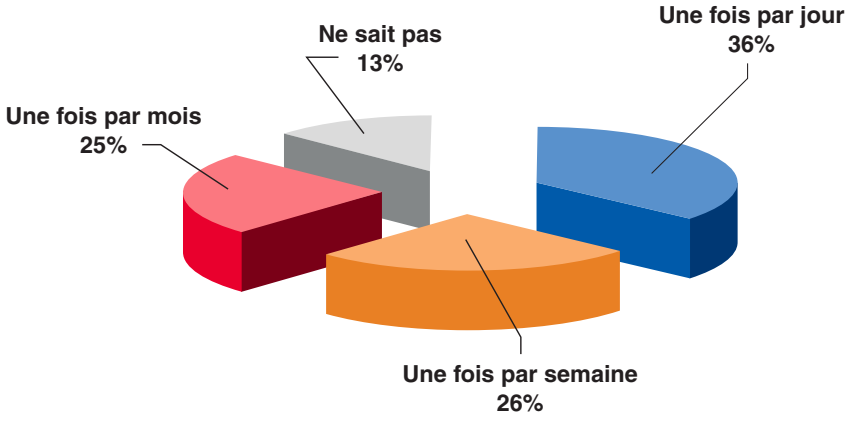
Quel impact des virus ? Sinistres déclarés et contre-mesures

Le questionnaire adressé aux entreprises a mis l'accent sur la différenciation entre un incident de sécurité et un sinistre, ce dernier ayant une connotation plus forte en matière d'impact. De ce fait, la sinistralité déclarée en 2003 régresse largement, puisque 80 % des entreprises interrogées ne déclarent aucun sinistre.

Les infections par virus ne font pas exception à cette diminution et atteignent 17,6 %. Dans ces conditions, il n'est guère étonnant que l'impact des attaques virales soit très peu évalué financièrement et considéré comme élevé pour seulement 11 % des entreprises.

Aujourd'hui encore, 10 % de sociétés déclarent ne pas avoir d'antivirus. Lorsque celui-ci est installé, la fréquence de mise à jour de ces logiciels reste souvent insuffisante.

Fréquence des mises à jour de l'antivirus :



Le point de vue du Clusif

S'il est bien un sujet relatif à la Sécurité des Systèmes qui fasse couler de l'encre, c'est celui des virus. Nous ne chercherons pas ici à définir les différentes raisons de ce véritable raz de marée «informationnel» alors que d'autres attaques, d'autres négligences d'utilisateurs, d'autres manquements à la sécurité peuvent bien plus impacter une entreprise. Les chiffres recueillis pour cette étude, tout comme l'Observatoire d'impact lancé par le Clusif sur Mydoom.A début février 2004, montrent que les virus sont bien plus considérés comme des nuisances. Nous rappelons ci-dessous les conclusions de l'Observatoire :

«Ainsi, si cette infection apparaît comme importante en volume, les conséquences financières semblent proches de zéro. Les antivirus du poste de travail ont parfois dû subir une mise à jour d'urgence, tandis que les antivirus situés sur les passerelles de messagerie semblent avoir convenablement joué leur rôle. Le virus a certainement été la cause majeure de l'engorgement des messageries et de la perte de disponibilité par surcharge du trafic réseau.
Il faut enfin remarquer, phénomène nouveau et en pleine croissance, le surcroît de trafic engendré par les antivirus eux-mêmes qui, mal configurés, retournent vers de nombreux correspondants des messages d'alerte par ailleurs inexacts [2]».

La «réussite» d'une infection virale repose sur trois composantes :
* la faiblesse de la protection mise en œuvre,
* l'absence d'information des utilisateurs,
* pour des raisons mal identifiées, la rapidité et la «sophistication» du virus.

Si l'antivirus est absolument incontournable, il n'est plus à lui seul une solution globale de sécurité contre les programmes malveillants. De plus, la mise à jour quotidienne de la base de signature est désormais un impératif, sauf pour les antivirus génériques. Il est complété d'un pare-feu correctement paramétré et de l'application des *patchs* sur le système d'exploitation et les applications. Car il ne faut pas oublier qu'une faille corrigée ferme la voie d'accès à nombre de virus ou vers.

[2] Etude intégrale disponible sur : https://www.clusif.asso.fr/fr/production/infovir/infovir0911.asp

Alors que l'économie repose de plus en plus sur les systèmes d'information, qu'elle devient Economie Numérique, que la confiance doit s'instaurer entre tous les acteurs, une forme de «marketing de la peur» (tel que cela a été le cas à propos du virus Sasser) est préjudiciable. Ne serait-il pas urgent et utile que la communication s'oriente sur le mode pédagogique ?

Recommandations :

- ☞ installer un antivirus, même chez un particulier,
- ☞ mettre à jour quotidiennement cet antivirus, soit en installant la mise à jour à l'aide du fichier disponible sur le site de l'éditeur soit en activant la mise à jour automatique,
- ☞ informer et former les utilisateurs, au minimum sur les points suivants : l'importance de laisser l'antivirus actif, l'acquisition de bons réflexes dans l'usage de la messagerie (ne pas cliquer sur une pièce jointe sans s'interroger au préalable sur l'expéditeur, sur le type de pièce jointe, sur la nature du message reçu, y compris lorsque l'expéditeur est connu),
- ☞ ne pas considérer l'antivirus comme seul moyen de protection : le pare-feu et l'installation des correctifs sont indispensables,
- ☞ assurer une veille sur les *patchs* critiques et les installer,
- ☞ désactiver les services inutilisés sur les serveurs et sur les stations de travail.

RoI ou RoSI, peu de visibilité

Bien que l'étude ne pose pas directement la question de savoir si les entreprises calculent ou non le RoI (acronyme anglais pour Retour sur Investissement) ou plus particulièrement le RoSI (Retour sur Investissement de Sécurité), nous constatons depuis plusieurs années que le calcul de l'impact financier des sinistres ou incidents avérés n'est pas réalisé dans la majorité des cas. En 2003, seulement 46 % des entreprises de plus de 1000 salariés y procèdent et cette pratique tombe à 20 % environ pour les effectifs de 200 à 1000.
Dans ces conditions, comment justifier la mise en œuvre de nouveaux moyens et le budget associé ?

Le point de vue du Clusif

Si, aujourd'hui, le sujet est souvent abordé dans la presse spécialisée, la constatation est toujours la même : le calcul du RoI ou du RoSI est loin d'être une pratique courante.
Plusieurs facteurs peuvent être avancés : manque d'indicateurs, manque d'analyse des impacts en cas de sinistre, lorsqu'il ne s'agit pas d'un manque de prise de conscience des risques liés aux systèmes d'information. Ajoutons un manque de méthodologies rigoureuses, de standard et d'outils de benchmarking sectoriel.

L'impératif de sécurité informatique n'est pas encore évident pour certaines directions générales et leur réponse sur une augmentation éventuelle de budget peut se limiter à la question suivante : «quel gain l'entreprise va réaliser grâce à cette sécurisation ? »
D'où la nécessité, en premier lieu, de faire prendre conscience à chaque dirigeant de ses responsabilités, tant économiques que réglementaires et juridiques.

Nous ne citerons que trois exemples qui concernent toutes les entreprises :
- la tenue de la comptabilité sur informatique ainsi que l'archivage fiscal soumis à des lois,
- le respect de la réglementation sur les données à caractère personnel contrôlée par la CNIL,
- l'engagement du dirigeant au regard du Code Pénal pour tout traitement automatisé de données.

Toute entreprise doit donc se poser la question de savoir si les moyens techniques et organisationnels qu'elle a mis en œuvre sont suffisants pour répondre à l'exigence de conservation et de confidentialité des données.

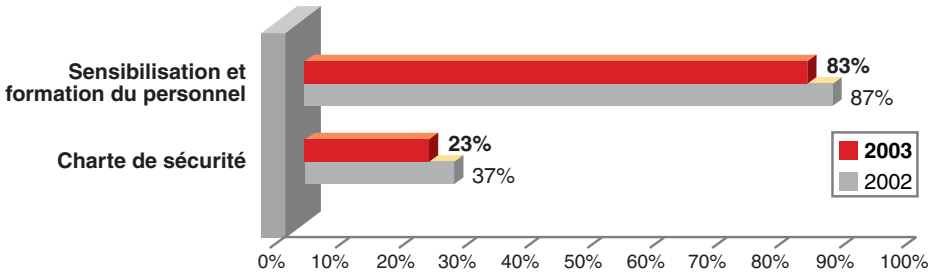
Nous avons abordé précédemment la thématique du nomadisme, en soulignant le coût plus élevé, à l'achat, des ordinateurs portables et leur difficulté d'administration, qui elle aussi a un coût. Malgré cela, les perspectives de ventes à moyen terme dépassent celles des postes fixes. Dans une étude du Gartner d'octobre 2003 donnant des scénarios permettant de calculer le retour sur investissement sur ces matériels (en fonction du temps passé par le salarié sur son portable dans ses déplacements professionnels) il apparaît que les gains de productivité sont rapidement acquis. Certaines solutions de sécurité orientées sur la performance peuvent parfaitement faire l'objet d'un calcul de RoSI qui aboutit également à une meilleure rentabilité.

Recommandations :

☞ Un groupe de travail au Clusif a mené une réflexion sur le sujet : *«Retour sur investissement en sécurité des systèmes d'information : quelques clés pour argumenter»*. Cet ouvrage est à paraître prochainement.

Sensibilisation : quels moyens pour quels objectifs ?

La sensibilisation et la formation apparaissent stables tandis que la mise en place de chartes de sécurité s'affiche en retrait en 2003.



Le point de vue du Clusif

Le chiffre élevé de sensibilisation et formation, réparti uniformément dans toutes les tailles d'entreprises, étonne quelque peu par rapport à la réalité de retours d'expérience dont nous avons connaissance ou d'enquêtes d'organismes et de médias.
Les directions générales, tout comme l'ensemble des salariés, sont loin d'être suffisamment sensibilisées à la valeur des informations détenues par l'entreprise, à la guerre économique,

aux multiples moyens d'attaques, utilisant ou non les canaux numériques. Ce qui explique que les budgets et les moyens consacrés à la sécurité ne soient pas toujours affectés en conséquence.

La mobilisation doit être générale. Encore faut-il que chaque salarié ait bien compris les risques, évolutifs, liés à l'usage de la messagerie, à une connexion à distance ou encore les conséquences possibles de téléchargement de fichiers.
A titre d'exemple, combien de salariés n'ont pas encore intégré le principe d'usurpation d'identité et continuent de croire, lorsqu'ils reçoivent un mail virusé d'une personne qui leur est connue, que c'est réellement cette personne qui leur a adressé le mail ?

Recommandations :

- ☞ responsabiliser l'utilisateur en tant que propriétaire de données et ainsi l'impliquer dans la démarche globale de sécurité de l'information,
- ☞ former dans la continuité, en fonction de nouvelles technologies ou habitudes adoptées par l'entreprise et qui vont engendrer de nouvelles vulnérabilités,
- ☞ formaliser les consignes de sécurité dans un seul document, remis à chaque session de sensibilisation,
- ☞ rappeler les messages pour éviter la dégradation des bonnes pratiques,
- ☞ s'appuyer sur l'actualité pour relancer la sensibilisation.

Gestion des correctifs (patchs) : un déploiement indispensable

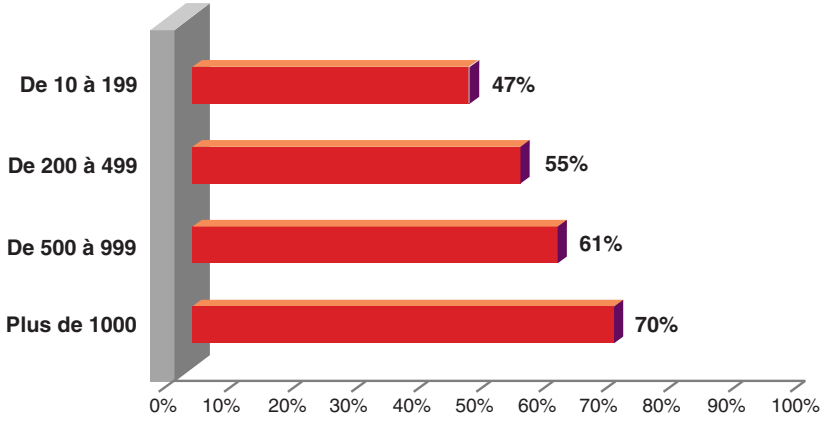
Seulement 51 % des répondants ont installé les correctifs *(patchs)* majeurs ou recommandés, selon la répartition suivante :

Effectifs :	10 à 199	200 à 499	500 à 999	Plus de 1000
	50 %	59 %	62 %	77 %

Secteurs :	BTP	Commerce	Industrie	Services	Télécoms	Transports
	44 %	46 %	45 %	56 %	68 %	35 %

La politique de mise à jour des systèmes d'exploitation et des applications est formalisée dans 47 % des cas, dont 68 % qui externalisent cette procédure.

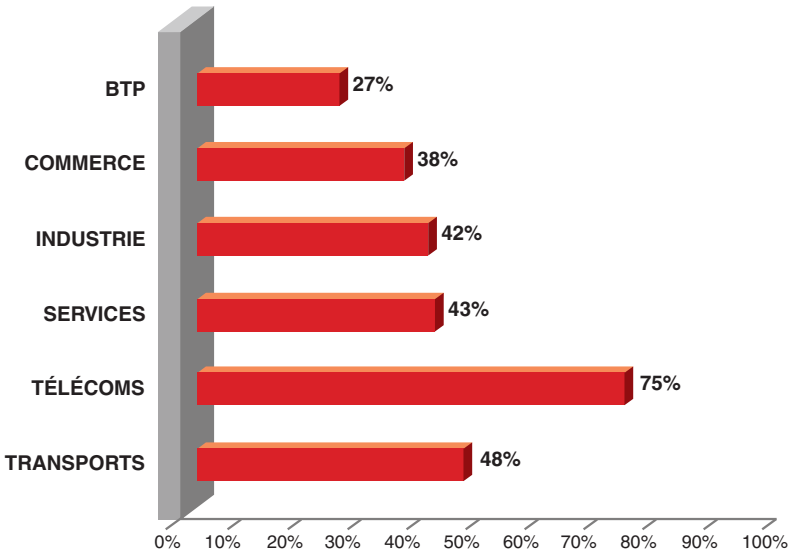
Formalisation de la politique de mise à jour des systèmes d'exploitation et des applications :



Plus de la moitié des entreprises estime que le temps consacré à ces tâches de mises à jour est plus lourd qu'en 2002.

Concernant la veille sur les questions de sécurité, elle est pratiquée par 41 % des entreprises en moyenne, avec une forte disparité selon les secteurs.

La pratique de la veille sécurité :



Si dans les grandes entreprises (plus de 500 salariés) la pratique de cette veille est généralisée à 90 %, elle n'est pas suivie d'effet au même niveau par la mise en place des correctifs.

Le point de vue du Clusif

Au niveau national, la faible application des *patchs* cumulée à des mises à jour d'antivirus insuffisantes explique que le nombre de postes touchés par les attaques virales soit si important.
Comme le rappelait le CNRS dans sa lettre du mois d'avril 2004, le correctif permettant d'éviter les attaques par le ver Blaster était disponible le 16 juillet 2003 alors que l'exploitation à grande échelle de cette faille - permettant de prendre le contrôle à distance de machines vulnérables - a commencé vers le 11 août, et de conclure : «On voit donc bien qu'en très peu de temps, le pire peut arriver. On voit aussi qu'avec des moyens et/ou une bonne organisation, le pire peut aussi être évité».

Il existe toutefois un problème possible de compatibilité avec les applications existantes. Dans ce cas, il est essentiel pour les entreprises de consulter le plus rapidement possible l'information disponible sur les sites des CERT, des associations professionnelles, des éditeurs, afin de rassembler tous les éléments qui vont décider de l'action de sécurité à engager.

Recommandations :

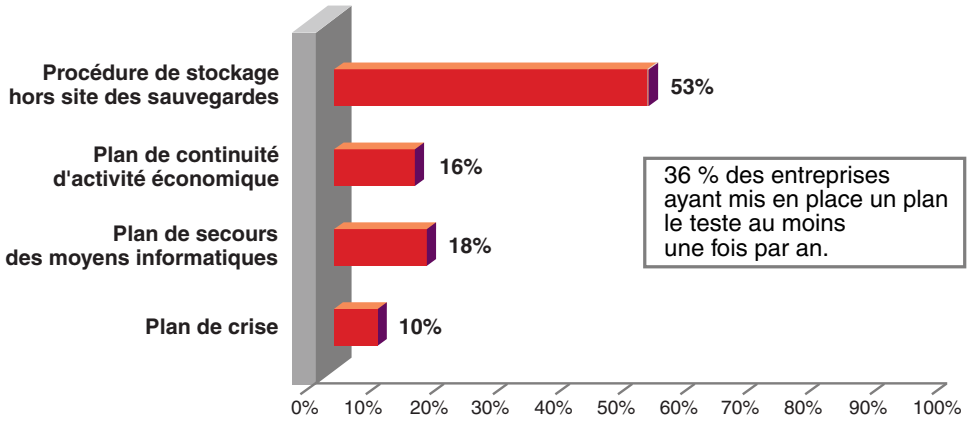
☞ apprécier la criticité de la faille par rapport à l'activité informatique et donc économique,
☞ effectuer des tests de non régression ; l'installation du patch ne doit pas polluer les flux d'information ou provoquer un dysfonctionnement,
☞ ces deux premiers points amènent à une sélection des *patchs* à déployer.

Recommandations :

☞ instaurer une procédure push qui permet une distribution rapide du correctif lors de menaces avérées,
☞ ne pas se limiter aux seuls serveurs et stations de travail mais sécuriser aussi les périphériques tels que les routeurs et les imprimantes réseaux,
☞ désigner un responsable de la gestion des *patchs*,
☞ s'abonner à un service de veille à valeur ajoutée (option pour se délester de la tâche en interne).

Continuité de l'activité et prise de risque des entreprises

Si les procédures de sauvegarde de l'information semblaient presque acquises dans nos précédentes études, il n'en est pas de même lorsque la question posée concerne les procédures de stockage de ces informations sauvegardées. Dans le meilleur des résultats, les Télécoms, c'est tout de même un quart des entreprises qui ne stockent pas leurs sauvegardes hors site.
Quant aux plans qui permettent de préserver l'activité en cas d'incident majeur, force est de constater qu'ils sont peu développés.



Comme dans l'ensemble de cette étude, il existe toujours des écarts importants en fonction de la taille de l'entreprise.

	De 10 à 199	De 200 à 499	De 500 à 999	Plus de 1.000
Procédure de stockage hors site des sauvegardes	52 %	59 %	77 %	66 %
Plan de secours des moyens informatiques	17 %	34 %	49 %	61 %
Plan de continuité d'activité économique	16 %	29 %	27 %	54 %
Plan de crise	9 %	28 %	43 %	53 %

Le point de vue du Clusif

La citation que le Clusif met en exergue sur sa plaquette *«Les hommes ne voient la nécessité que dans la crise»* semble particulièrement bien s'appliquer à ce domaine.

C'est souvent après un sinistre ou une panne importante que l'entreprise va réagir.

Dans une situation d'urgence, sans sauvegarde hors site, sans plan préparé, comment l'activité va-t-elle redémarrer ?
C'est le choix du risque, maîtrisé ou non, assuré ou non. La raison souvent invoquée pour ce choix est le coût élevé de la mise en œuvre d'un plan de continuité. A contrario, l'estimation des pertes en cas de sinistre n'est quasiment jamais réalisée.
Par exemple, la centralisation sur un seul serveur de programmes répond à un souci de réduction des coûts ; mais en cas de défaillance du serveur et en l'absence de secours, c'est le fonctionnement ou la survie même de l'entreprise qui est en jeu.

Quelle société peut se déclarer à l'abri d'une inondation, comme dans le sud-est de la France en 2003, d'un incendie, d'une défaillance grave du système d'information, soit par accident soit par malveillance ? Pourtant, de la sauvegarde hors site, dont la restauration est régulièrement testée, au plan de crise, en passant par le plan de continuité, les procédures sont encore loin d'être généralisées.

Au vu de ces résultats, une question d'importance se pose : comment ces entreprises respectent-elles leurs obligations légales en matière d'archivage ? Dans ce domaine, les deux contraintes majeures sont la durée de conservation et l'intégrité totale des données, sans conversion ou modification. Pour le premier point, nous rappellerons simplement quelques durées légales de conservation : cinq ans pour les bulletins de paie, dix ans pour des commandes, factures ou autres éléments de facturation, trente ans pour des contrats commerciaux.
Sur le deuxième point, l'entreprise doit prendre en compte, à chaque évolution de son système d'information et de ses applications, le fait qu'elle peut être amenée, dans dix ans ou plus, à fournir la preuve numérique en parfait état de conservation du support et sans aucune altération.

Recommandations si le plan de continuité existe :

- ☞ ne pas se limiter au secours informatique mais envisager la continuité des services. Ainsi, il est nécessaire de prendre en compte les besoins des utilisateurs et d'identifier les ressources critiques pour l'activité économique et non sur le seul plan informatique,
- ☞ en fonction des entrées/sorties du personnel, mettre à jour les procédures qui identifient les acteurs clés, les moyens de les contacter,
- ☞ en fonction de l'ajout ou du retrait d'applications ou de fichiers, modifier en conséquence les étapes du processus de récupération des données, identifier les fichiers vitaux qui se modifient au fil du temps,
- ☞ prendre en compte la croissance de l'entreprise, interne ou par acquisition ; les besoins peuvent s'amplifier brusquement, tant en terme de matériel de secours, de surface de repli, de capacité d'accueil, de puissance de traitement…
- ☞ répliquer sur le système de secours toute modification du système d'origine,
- ☞ être vigilant sur le respect des obligations légales d'archivage,
- ☞ plan non testé = plan qui risque de ne pas être d'un grand secours.

Recommandations si aucun plan n'existe :

- ☞ définir un plan de continuité !

- ☞ procéder à une sauvegarde journalière des données sur CD Rom, clé USB, support magnétique, en fonction de la volumétrie des données,
- ☞ conserver la sauvegarde dans un autre bâtiment que le bureau ; éventuellement, un second jeu peut rester sur le site pour les besoins courants d'exploitation,
- ☞ contrôler que ces données sauvegardées sont exploitables,
- ☞ identifier si l'entreprise est dans une zone à risques (inondation, feux de forêt, proximité d'industries à risques…),
- ☞ mesurer la durée d'interruption d'activité que l'entreprise peut supporter (aucun accès aux données essentielles) et estimer cette perte d'activité par jour,
- ☞ imaginer l'impossibilité d'accéder aux bureaux, par exemple par la mise en place d'un périmètre de sécurité civile.

Eléments accidentels : panne informatique, événement naturel…

Le tableau suivant ne concerne que les 20 % d'entreprises qui ont déclaré avoir subi des sinistres en 2003. L'impact des pannes internes n'est qualifié d'élevé que par 9 % des interrogés; celui des pertes de services essentiels atteint 18 % et les événements naturels 12 %.

Taux de sinistres par effectif :

	De 10 à 199	De 200 à 499	De 500 à 999	Plus de 1.000
Panne interne	10 %	18 %	18 %	25 %
Perte de services essentiels	7 %	10 %	11 %	20 %
Événement naturel	2 %	3 %	2 %	8 %

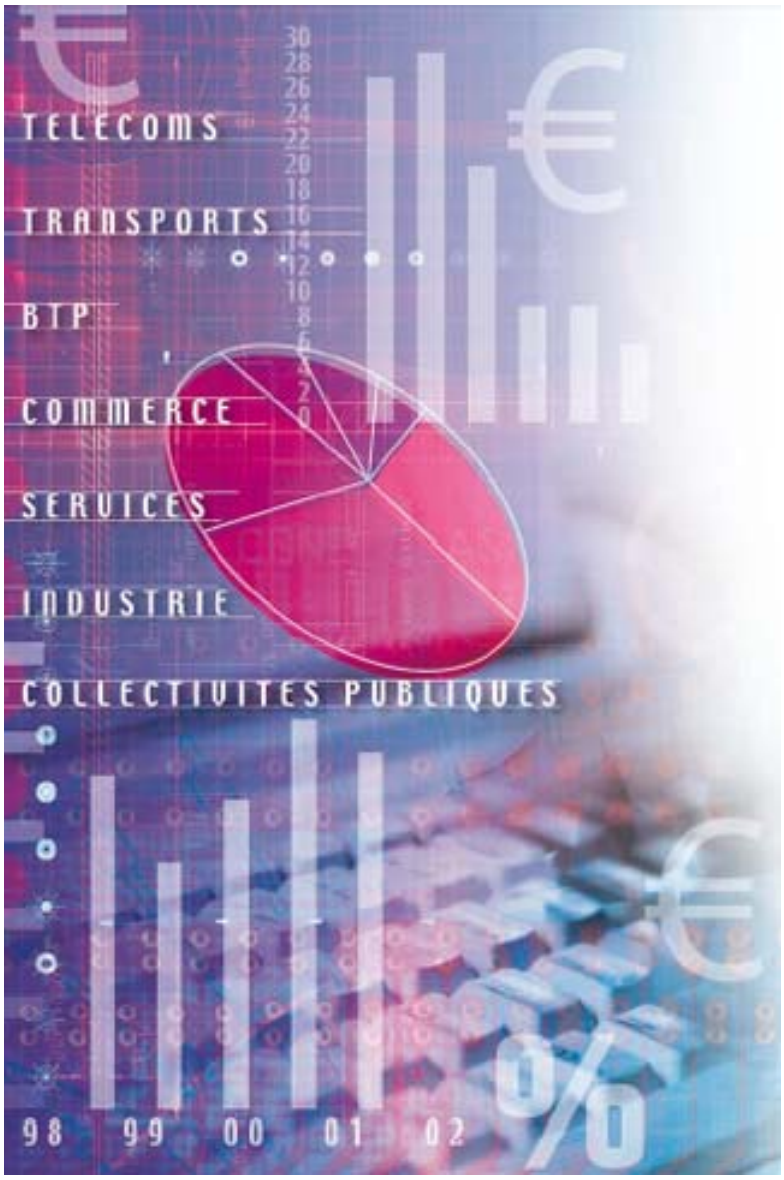
Le point de vue du Clusif

Vague de chaleur, de froid, tempête ou inondation, les dernières années ont été fertiles en événements naturels. Si la prévision dans ce domaine est parfois difficile, la gestion de la situation et les implications sur le système d'information doivent être étudiées dans la sérénité, avant la crise. L'environnement géographique, les implantations industrielles proches donnent les premiers éléments de réflexion.
D'autre part, tous ces phénomènes sont susceptibles d'agir sur la fourniture et l'alimentation en électricité.
Ce n'est que par une vision globale des risques encourus et des dommages possibles que l'entreprise pourra redémarrer son activité dans les meilleurs délais. Encore faut-il entamer la réflexion.
Les centres de données doivent être particulièrement bien équipés pour faire face à une défaillance directe causée, par exemple, par la température ou l'eau, ainsi qu'aux conséquences indirectes sur les ressources électriques.

Recommandations :

- ☞ installer un onduleur qui protège des micro-coupures, des parasites et sur-tensions,
- ☞ se renseigner auprès des mairies et des Directions Départementales de l'Equipement sur la cartographie des eaux, les sites Seveso,
- ☞ contrôler les éléments techniques du contrat en cas d'hébergement de données (Data Center) : comment sera gérée la priorité d'attribution et la disponibilité des équipements mutualisés ?
- ☞ vérifier les niveaux de certification d'installation (test du système d'extinction automatique) et le respect de normes métier (fournisseur d'accès internet par exemple),
- ☞ pour des solutions coûteuses ou délicates à mettre en œuvre (serveur ou générateur électrique de secours) et que l'entreprise ne peut avoir en interne, étudier la disponibilité contractuelle auprès d'un ou plusieurs fournisseurs,
- ☞ pour rappel, un audit de sécurité des systèmes d'information permet d'identifier les menaces pour une entreprise ou un site particulier puis d'ordonner et d'homogénéiser le plan de sécurité (sauvegarde, secours, gestion des droits, anti-intrusion, assurance…).

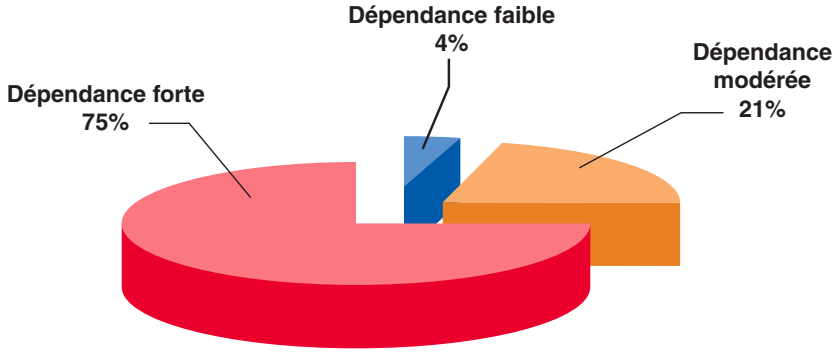
TROIS FOCUS



- Entreprises de 200 à 500 salariés
- Collectivités locales et territoriales
- Établissements hospitaliers

Le sentiment de forte dépendance au système d'information qui prédomine dans cette catégorie est cohérent avec le degré d'ouverture.

Dépendance au système d'information :

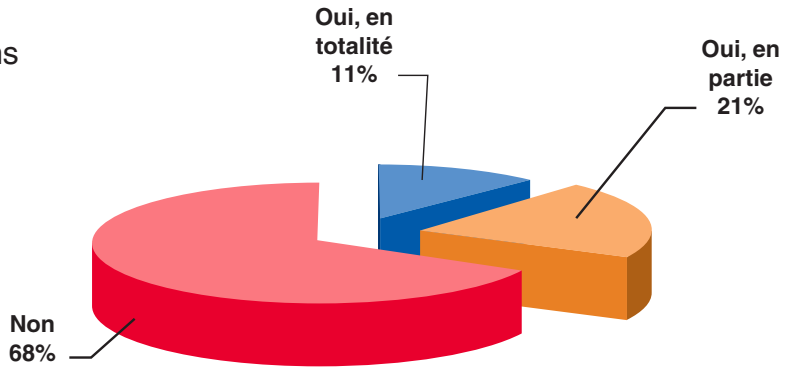


Ouverture des systèmes d'information :

Site Internet	81%
Accès Internet généralisé	62%
Messagerie électronique généralisée	76%
Intranet	75%
Accès distant pour les salariés mobiles	51%
Extranet	34%
Achat sur Internet	11%
Mise en place d'un réseau Wi Fi	25%
Vente sur Internet	9%

La politique de sécurité est formalisée dans 83% de ces entreprises, la moyenne nationale étant de 41 %. Elle s'accompagne de moyens humains, organisationnels et techniques que nous allons détailler.
Les ressources humaines affectées à la sécurité le sont soit à temps plein (54 %) soit à temps partiel (26 %). Ce sont toutefois 20 % d'entreprises qui n'ont aucune personne en charge d'assurer la sécurité de leurs données : une insouciance qui peut coûter cher et qui n'est pas l'exclusivité de cette catégorie d'effectif.

Le recours à l'infogérance pour le système informatique et télécoms se répartit comme suit :



Des prestataires externes interviennent dans 46 % de ces sociétés, ce qui se rapproche de la moyenne nationale de 51%.

Management de la sécurité

Les directions devraient être le moteur de la réflexion en matière de sécurité des données, ce qui n'est pas toujours le cas. En effet, qui mieux que le dirigeant a une vision globale de l'entreprise, de ses enjeux stratégiques, de ce qui fait sa richesse ? C'est de son ressort d'impulser les choix et les bonnes pratiques à mettre en œuvre.

Mesures mises en œuvre :

Sensibilisation et formation du personnel	83%
Révision des mesures de sécurité après un incident	52%
Charte de sécurité	52%
Audit de sécurité, au moins une fois par an	44%

Sécurité physique

Les moyens de contrôle de la sécurité physique sont d'un assez bon niveau, y compris pour les dispositifs antivol puisque, selon les déclarations, cette menace est très faible dans l'échantillon concerné.

Moyens développés :

Dispositif de protection électronique	93%
Dispositif anti-incendie dans les locaux informatiques	84%
Accès restreint aux locaux techniques	61%
Dispositif antivol du matériel	42%

Sécurité logique

Bien que le terme " non trivial " pour les mots de passe ait bien été défini auprès des interlocuteurs, le résultat semble pour le moins optimiste. Nous rappelons qu'il s'agit d'un assemblage d'au moins huit caractères, comportant un ensemble de chiffres, lettres et caractères spéciaux, et présentant un caractère mnémotechnique par sa prononciation ou son mode de création.

Moyens mis en œuvre :

Logiciel antivirus	95%
Mot de passe non trivial	89%
Pare-feu (firewall)	83%
Surveillance du réseau contre les intrusions, système d'alerte	48%
Réalisation de tests (intrusion, vulnérabilité…)	11%
Chiffrement de données	13%
Authentification renforcée par un dispositif électronique	20%

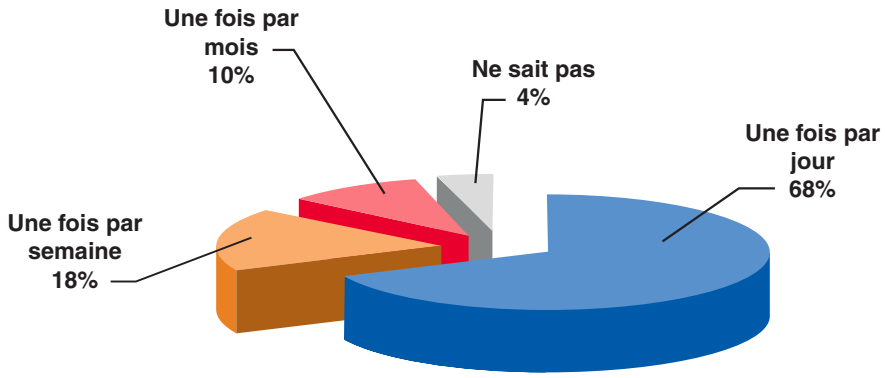
Compte tenu du niveau élevé d'accès distant pour les salariés mobiles et de mise en place de réseau WiFi, les protections en terme de chiffrement de données et d'authentification ne sont pas à niveau.

Les mises à jour : logiciels antivirus et correctifs *(patchs)*

Comme nous l'avons vu dans *Regards sur l'actualité*, il est incohérent, dans la majorité des cas, de dissocier ces deux types de mises à jour, les vers prenant pour base les failles de sécurité du système.

Si 95 % de ces entreprises ont bien installé un logiciel antivirus, les processus de mise à jour ne sont pas encore suffisamment pris en compte pour un tiers d'entre elles, faute de temps, de perception des enjeux ou de compréhension du fonctionnement des produits.

Périodicité des mises à jour de l'antivirus :



Quant à la mise à jour des systèmes d'exploitation et applications, elles sont 41 % à ne pas avoir installé les correctifs majeurs ou recommandés.
Si l'on rapproche ce chiffre de l'ouverture par messagerie électronique (76 %), cela signifie, en prenant l'hypothèse la plus basse, que 17 % de ces entreprises ont des failles non corrigées avec pour certaines, en complément, un antivirus non à jour.

Il semblerait que ce ne soit pas faute d'information, puisque 81% déclarent pratiquer une veille sur les questions de sécurité des systèmes. S'agit-il d'un manque de temps, d'un manque de prise de conscience ou d'un risque assumé ? Il ne faut toutefois pas négliger les cas où la mise à jour est susceptible de modifier la configuration du système et le bon déroulement des applications. Alors, la phase de test s'impose avant le déploiement généralisé.
L'estimation du temps consacré à ces tâches (2003/2002) est en augmentation pour 71%.

Continuité de l'activité

Tandis que 83 % annoncent la mise en œuvre d'une politique de sécurité, la continuité d'activité ne rime toujours pas avec la pérennité de l'entreprise.
Il n'est même plus question de l'ouverture, ou non, des systèmes d'information. Une entreprise peut parfaitement ne pas utiliser de messagerie, ne pas avoir de site internet ; pour autant, peut-elle affirmer qu'elle n'a pas besoin de son informatique ? Suite à un " simple " crash de son disque dur, comment va-t-elle récupérer ses données pour établir le bulletin de paie de ses salariés ou gérer les commandes de ses clients ?

Moyens pour assurer la continuité de l'activité :

Procédure de stockage hors site des sauvegardes	59%
Plan de secours des moyens informatiques	34%
Plan de continuité d'activité économique	29%
Plan de crise	28%

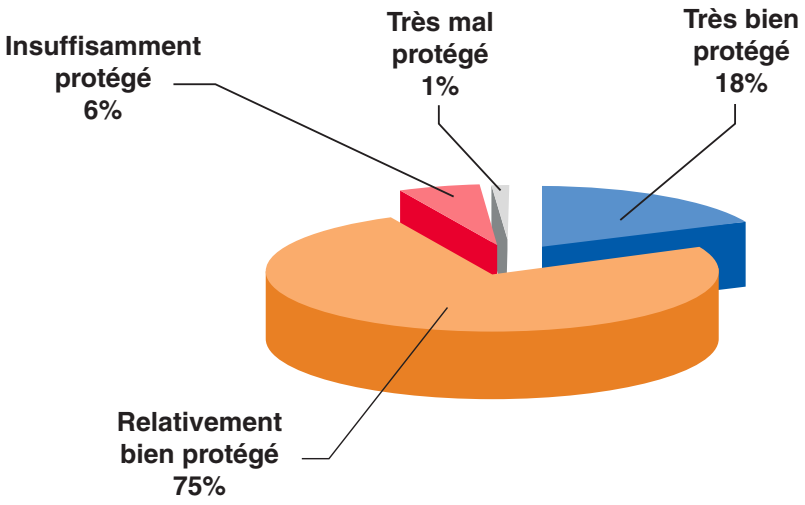
Evaluation de la sinistralité : sinistre ou incident ?

Plus de la moitié des entreprises (59 %) déclare n'avoir subi aucun sinistre. L'accent mis cette année sur la différenciation entre un incident et un sinistre explique cette relativisation des événements. Même en cas d'attaque virale, de nombreuses entreprises considèrent que cela fait partie du quotidien et perd ainsi de sa gravité. D'ailleurs, dans 76 % des cas, l'impact financier n'est pas évalué.

Pour les 41 % qui ont subi des sinistres, les facteurs déclenchant se répartissent comme suit :

Infection par virus	35%
Panne interne	18%
Vol (matériel, logiciel)	15%
Perte de services essentiels	10%
Erreur d'utilisation	8%
Evénement naturel	3%

Le degré de protection estimé par ces PME est très positif, à 93 %.



Ce bel optimisme doit être tempéré par l'ensemble des chiffres précédents. N'y aurait-il pas parmi elles un réseau sans fil non sécurisé, un antivirus désactivé sur un poste, une sauvegarde uniquement dans les locaux de l'entreprise et qui n'a pas été contrôlée depuis un certain temps ?

Mais il est vrai, pour faire bonne mesure, qu'une entreprise sur deux compte renforcer ses dispositifs de sécurité dans les 2 ans à venir.

Et pour demain, quels risques redoutés ?

Ah, ce cher virus ! Ce paragraphe pourrait aussi s'intituler «De l'influence de l'information». Pourquoi redouter un phénomène si peu déclaré en sinistre, tant sur cet échantillon que sur l'échantillon total de l'enquête ? D'autant que l'impact est rarement fort et de ce fait n'est pas quantifié financièrement.

Perception des risques à venir :

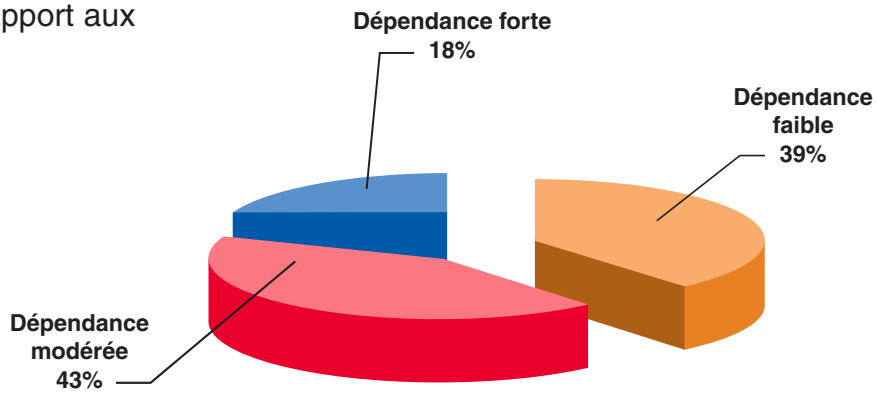
Virus et infection informatique	52%
Accident d'origine interne	36%
Intrusion externe à l'entreprise sans altération	15%
Accident d'origine externe	17%
Vol ou disparition de matériel ou de logiciel	8%
Erreur d'utilisation	9%
Atteinte à l'image	2%
Erreur de conception	2%
Attaque ciblée	1%

Le propos est de relativiser, de quantifier ce type de risque. Les virus existent, ils se professionnalisent et peuvent servir de relais de *spam* comme le Clusif l'explique dans le Panorama de la Cybercriminalité 2003. Toutefois, les parades pour ce type de risque existent aussi et ne demandent qu'à être appliquées.

POLITIQUES DE SÉCURITÉ DANS LES COLLECTIVITÉS LOCALES ET TERRITORIALES

Les collectivités locales et territoriales en France représentent plus de 36 000 communes, 96 départements, 22 régions et de nombreuses communautés urbaines.
Elles sont entrées, à l'instar des autres administrations, dans une phase de mutation importante avec le projet ADELE, plan d'action de l'administration électronique 2004-2007 (http://www.adae.gouv.fr/adele/). La modernisation des services publics et l'augmentation des services électroniques rendus aux citoyens, aux entreprises, aux associations, aux collectivités territoriales, ne peuvent qu'augmenter à terme la dépendance aux systèmes d'information.

Dépendance déclarée par rapport aux systèmes d'information :



Ces changements en cours de réalisation vont profondément influer sur l'ouverture des systèmes, particulièrement en terme d'intranet, d'extranet et de services sur internet. Les collectivités locales et territoriales, de part leur rôle d'interface entre les citoyens et l'administration, ont trois axes de travail :
- la dématérialisation de leurs échanges avec les administrations, avec par exemple une plus grande ouverture des systèmes d'information territoriaux (SIT),
- l'accessibilité de services pour les agents de l'état,
- le développement de services à destination des usagers, particuliers ou entreprises. C'est ainsi qu'à partir de janvier 2005, la dématérialisation des appels d'offres sera rendue obligatoire.

Ouverture des systèmes d'information :

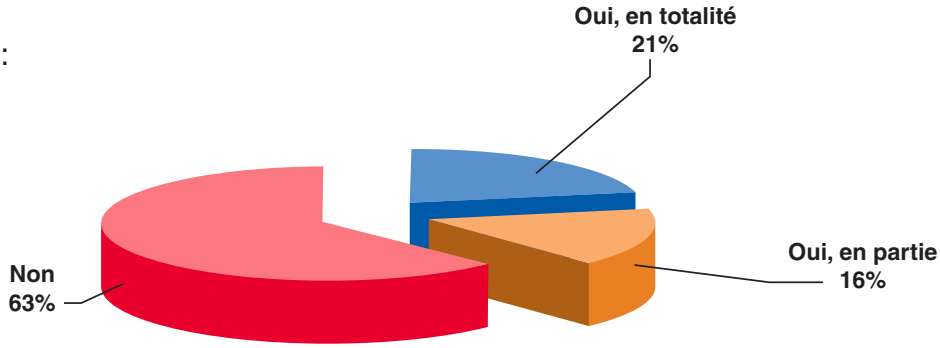
Site Internet	48%
Intranet	13%
Extranet	9%
Accès distant pour les salariés mobiles	7%
Service sur Internet	5%
Mise en place d'un réseau Wi Fi	5%
Achat sur Internet	2%

En matière d'intranet, certaines villes (en général de plus de 100.000 habitants) ont déjà lancé des initiatives qui leur permettent un meilleur échange des documents, le partage de l'information et l'amélioration du travail collaboratif.

Politiques de sécurité et moyens mis en œuvre

Pour éviter toute interprétation hâtive des chiffres de cette étude, il convient de garder en mémoire l'extrême diversité des collectivités locales et territoriales et de fait leurs ressources humaines et financières non homogènes.
Concernant les effectifs en charge de la sécurité des systèmes, 5 % des collectivités ont au moins une personne à temps plein et 16 % une personne à temps partiel. Ce serait donc 79 % qui ne disposeraient pas de ressources spécifiques. Ce chiffre n'est pas aberrant puisque l'ouverture actuelle des systèmes repose surtout sur des sites internet ; la gestion de ceux-ci est majoritairement sous traitée et la fonction sécurité externalisée. Ce dernier point explique le recours important à l'infogérance.

Recours à l'infogérance :



Les collectivités ont également recours, à 53 %, à des prestataires externes de SSI, soit pour de l'audit conseil soit pour des services opérationnels.
Elles sont 18 % à avoir défini une politique de sécurité.

Le plan ADELE fait ressortir les besoins nationaux en matière de ressources humaines compétentes et d'équipements.
Ainsi, la formation d'experts en sécurité est une priorité. De plus, et cela concerne autant les acteurs privés que publics, la sensibilisation et l'implication de chacun sur les comportements et les bonnes pratiques en sécurité doivent être constantes.
Depuis deux ans, la prise de conscience sur ces problématiques a réellement augmenté. Les publications spécialisées, comme la Gazette des Collectivités Territoriales, se font régulièrement l'écho de sujets tels que la mise en œuvre d'une charte de sécurité ou les réponses juridiques adaptées à des contextes de travail en évolution.

Management de la sécurité :

Sensibilisation et formation du personnel	49%
Révision des mesures de sécurité après un incident	31%
Charte de sécurité	31%
Audit de sécurité, au moins une fois par an	23%

Les procédures de stockage hors site des sauvegardes sont appliquées dans 54 % des cas.
Le développement de l'administration électronique, avec des enjeux importants en matière de confidentialité, d'intégrité et de disponibilité des données, va appeler le renforcement de ces dispositifs et de l'archivage électronique des documents numériques.

Les dispositifs de sécurité physique ne sont pas excessivement développés :

Dispositif de protection électronique	77%
Dispositif anti-incendie dans les locaux informatiques	60%
Accès restreint aux locaux techniques	19%
Dispositif antivol du matériel	25%

Concernant la sécurité logique il est à prévoir une augmentation des moyens déployés dans les prochaines années. Ce sera un des effets de la modernisation des services publics et de l'essor de l'administration électronique dans des conditions de confiance.

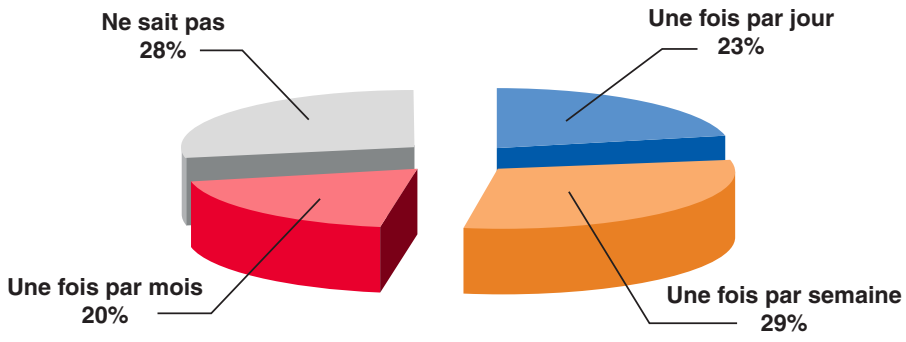
Dispositifs de sécurité logique :

Logiciel antivirus	87%
Mot de passe non trivial	69%
Pare-feu (firewall)	35%
Surveillance du réseau contre les intrusions	19%
Réalisation de tests	11%
Authentification renforcée par un dispositif électronique	7%
Chiffrement de données	6%

Les trois exemples suivants de réalisations et de projets tests en cours illustrent la diversité des opérations concernées par le plan d'action gouvernemental :
- la dématérialisation des achats engage déjà certaines villes dans des procédures garantissant la confidentialité et l'authenticité des échanges,
- les cartes à puce sécurisées dites «cartes de vie quotidienne» expérimentées par une douzaine de communes ont pour objectif l'accès en ligne aux téléservices administratifs,
- la transmission de documents par téléprocédure avec signature électronique, comme des comptes-rendus de conseil municipal à la sous-préfecture, augmente l'authenticité du processus.

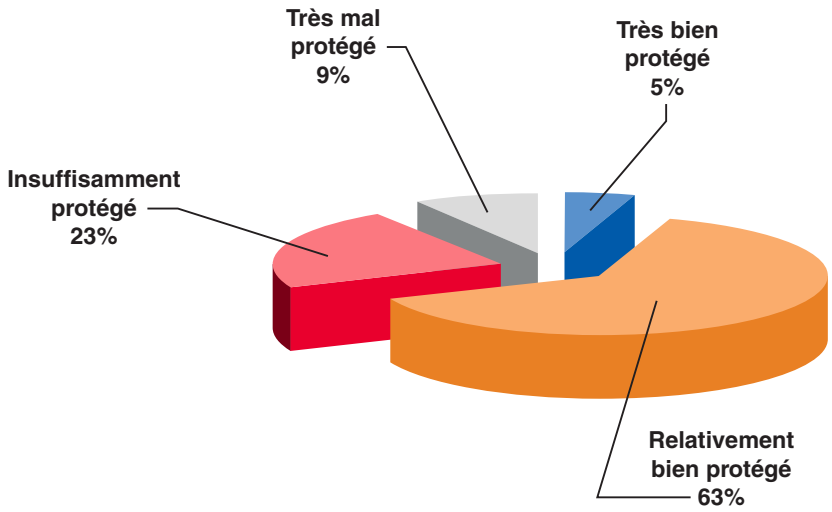
Dans tous les cas, la réduction des coûts de fonctionnement et l'optimisation de l'organisation sont en ligne de mire.
D'autre part, l'accès mutualisé aux données rendra indispensable les processus d'identification, de gestion des accès et d'harmonisation de la gestion des droits.

Parmi les 87 % qui procèdent à la mise à jour de leur logiciel antivirus, la périodicité journalière n'est pas la plus importante.



Par contre, 80 % déclarent avoir installé tous les correctifs majeurs ou recommandés sur leur système d'exploitation et applications. Elles sont 36 % à avoir formalisé ce type de mise à jour.
La veille sur les questions de sécurité des systèmes d'information est pratiquée par 25 % de ces collectivités.

Le sentiment de protection est assez bien évalué compte tenu du degré d'ouverture actuel des systèmes.

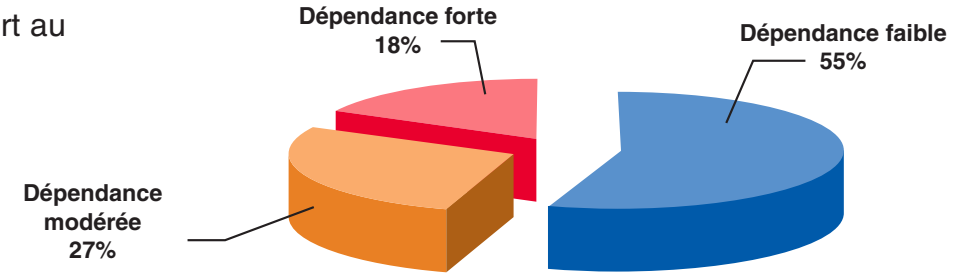


Elles sont 47 % à compter renforcer les dispositifs de sécurité dans les 2 ans à venir.

POLITIQUES DE SÉCURITÉ DANS LES ÉTABLISSEMENTS HOSPITALIERS

A l'heure actuelle, les systèmes d'information hospitaliers sont encore très orientés sur le traitement des données administratives, ce qui explique que la dépendance déclarée soit assez faible. A contrario, un système d'information axé sur l'informatique médicale doit fonctionner 24 heures sur 24, intégrant les notions, encore plus fondamentales dans ce cas, de disponibilité, d'intégrité et de confidentialité des données.

Dépendance par rapport au système d'information :



C'est une véritable mutation que vont devoir opérer les établissements hospitaliers en mettant en œuvre des systèmes d'information centrés sur les données du patient. C'est l'esprit de la loi du 4 mars 2002 qui a établi le principe d'accès par le patient à son dossier médical. Cette disposition va entraîner une dématérialisation des fichiers et de l'ensemble des données. La télémédecine est certainement l'évolution majeure de demain et différents moyens d'accès à ces données, pour tous les acteurs, sont donc appelés à se développer.

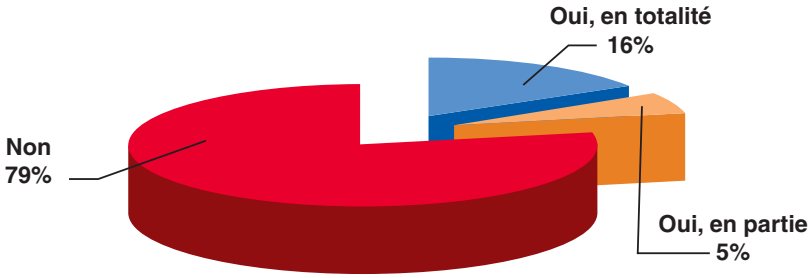
Ouverture des systèmes :

Site Internet	55%
Intranet	56%
Extranet	29%
Accès distant pour les salariés mobiles	22%
Service sur Internet	15%
Mise en place d'un réseau Wi Fi	15%
Achat sur Internet	7%

<u>Politique de sécurité et moyens mis en oeuvre</u>

Les établissements hospitaliers, bien que déclarant en majorité une dépendance faible, ont mis en place à 59 % des ressources affectées à la sécurité des systèmes d'information, soit à temps plein (44 %), soit à temps partiel (15 %).
Le recours à l'infogérance n'est pas très fréquent.

Systèmes d'information et/ou télécoms placés sous contrat d'infogérance :



51 % ont recours à des prestataires externes, soit pour des missions d'audit soit pour des services opérationnels.

Selon le rapport du Professeur Fieschi remis au Ministre de la santé en janvier 2003, *«les systèmes d'information hospitaliers sont faiblement sécurisés, cloisonnés, basés sur des applications verticales peu communicantes»*. Si certains hôpitaux ont déjà intégré une culture sécurité très forte basée sur le caractère vital du système d'information, les politiques de sécurité sont définies dans seulement 42 % des cas.

La sensibilisation du personnel est parfois très incitative et vigilante, avec par exemple l'affichage en bonne place des recommandations de la CNIL concernant la confidentialité des données à caractère personnel. C'est souvent dans ces mêmes unités que les chartes sont rédigées.

Management de la sécurité :

Sensibilisation et formation du personnel	72%
Révision des mesures de sécurité après un incident	43%
Charte de sécurité	34%
Audit de sécurité, au moins une fois par an	32%

Les évolutions législatives et réglementaires en cours (loi du 4 mars 2002 et les décrets d'application à paraître, transposition de la directive européenne…) vont profondément influer sur les systèmes d'information hospitaliers (SIH). Le groupe de travail Santé du Clusif a commencé à publier sur cette thématique et le document *«Etude de la réglementation et des recommandations relatives à la sécurité des systèmes d'information de santé»* est disponible en libre accès sur le site www.clusif.asso.fr.

Tous les établissements vont devoir gérer de façon accrue les trois piliers de la sécurité, l'indice DIC (pour Disponibilité, Intégrité, Confidentialité). Les mesures pour assurer la continuité de l'activité et la gestion du risque opérationnel sont donc en première ligne.

Continuité de l'activité :

Procédure de stockage hors site des sauvegardes	45 %
Plan de secours des moyens informatiques	24 %

Outre les aspects techniques et juridiques qui vont impacter les SIH, la mise en place d'un système de tiers de confiance se situe au cœur de la nouvelle législation afin d'héberger les données individuelles de santé, sans contestation de l'une des parties prenantes.

L'implantation des dispositifs de protection physique est inégale et doit encore se renforcer.

Dispositifs de sécurité physique :

Dispositif de protection électronique	94%
Dispositif anti-incendie dans les locaux informatiques	73%
Accès restreint aux locaux techniques	65%
Dispositif antivol du matériel	37%

L'ensemble des dispositifs de sécurité logique est appelé à se renforcer compte tenu des besoins accrus en identification, authentification et chiffrement nécessités par les évolutions législatives et les contraintes sécuritaires qui en découlent.
Dans la lettre d'information de mai 2004 du GIP-CPS (Cartes de Professionnel de Santé) la Direction de l'Hospitalisation et de l'Offre de Soins (DHOS) indique avoir demandé au Groupement de Modernisation des Systèmes d'Information Hospitaliers (GMSIH) la rédaction d'un ensemble de documents afin d'aider les établissements de santé dans la définition de leur politique de sécurité et dans la mise en œuvre de services de sécurité associés.

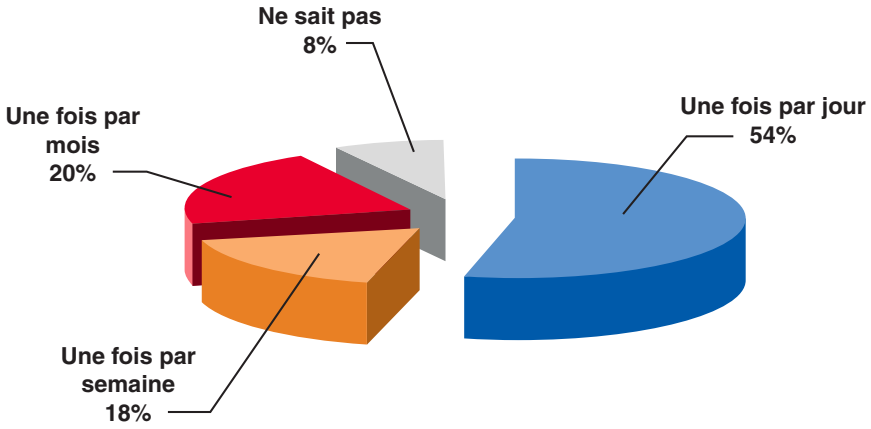
Dispositifs de sécurité logique :

Logiciel antivirus	95%
Mot de passe non trivial	73%
Pare-feu (firewall)	65%
Surveillance du réseau contre les intrusions	42%
Réalisation de tests	24%
Authentification renforcée par un dispositif électronique	15%
Chiffrement de données	16%

La voix sur IP, alliée éventuellement au WiFi, va certainement se développer dans les milieux hospitaliers, là où les téléphones mobiles perturbent les appareils médicaux. Mais selon la formule d'un chroniqueur américain *«il faudra mettre un volant et des freins à ce véhicule qui ne possède pour l'instant qu'un moteur et des roues».*
Concernant le partage des données, la gestion des autorisations d'accès doit s'insérer dans une traçabilité durable.

94 % des établissements procèdent à une mise à jour de leurs logiciels antivirus mais avec une fréquence trop peu élevée.

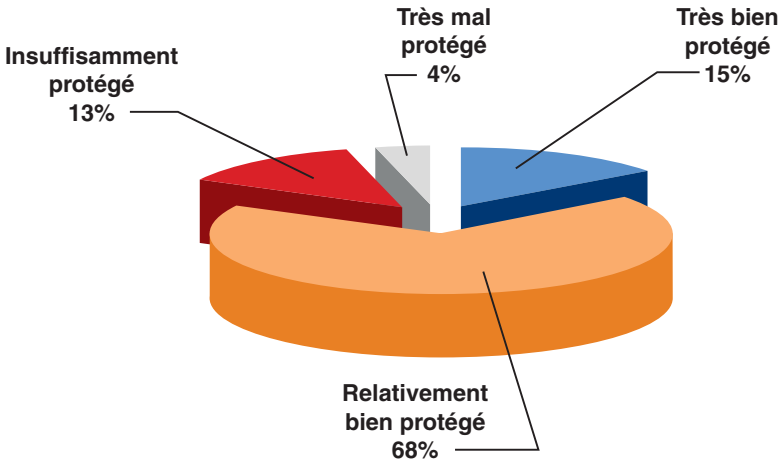
Fréquence des mises à jour des logiciels antivirus :



Tous les établissements interrogés déclarent avoir installé les correctifs majeurs ou recommandés. Cette procédure est même formalisée dans 42 % des cas.

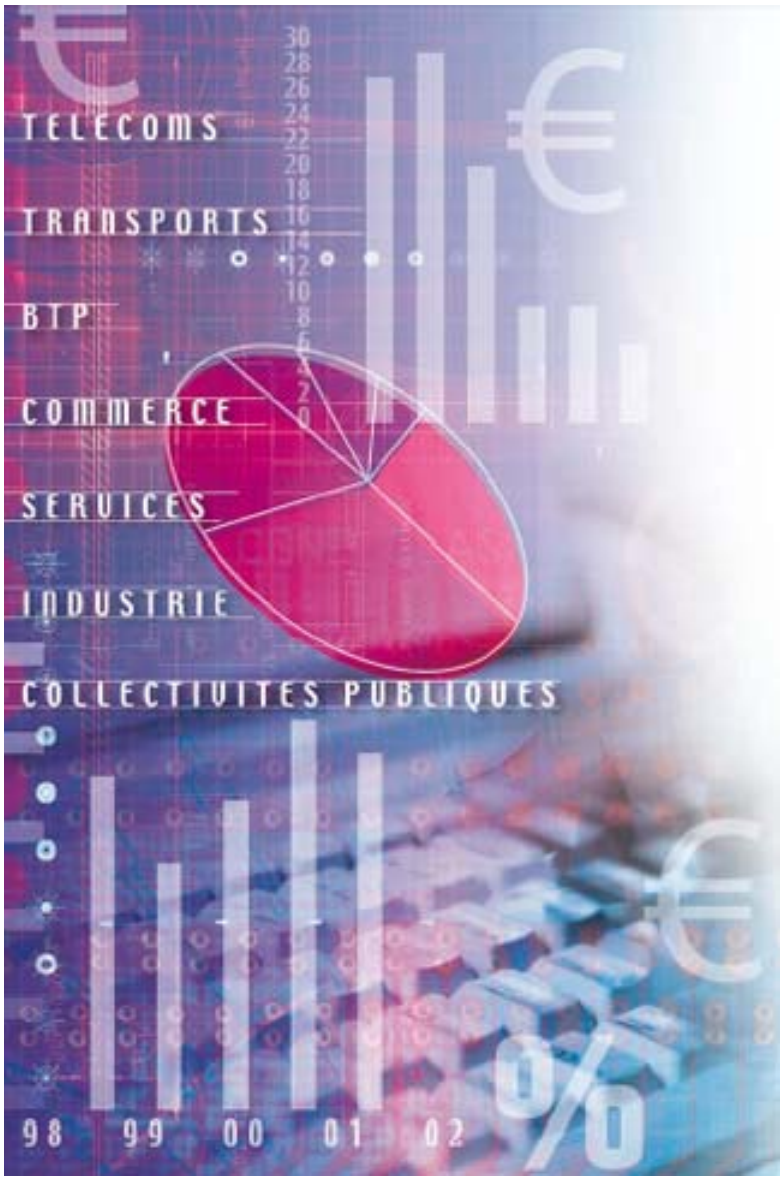
La veille sur les questions relatives à la sécurité des systèmes d'information est pratiquée par 45 %.

Interrogés sur la perception du degré de sécurité par rapport aux mesures mises en œuvre, les établissements hospitaliers se déclarent :



Ces chiffres sont cohérents tant par rapport à l'ouverture qu'aux mesures déployées. Le renforcement des dispositifs de sécurité dans les 2 ans à venir est cité par 39 % de ces établissements.

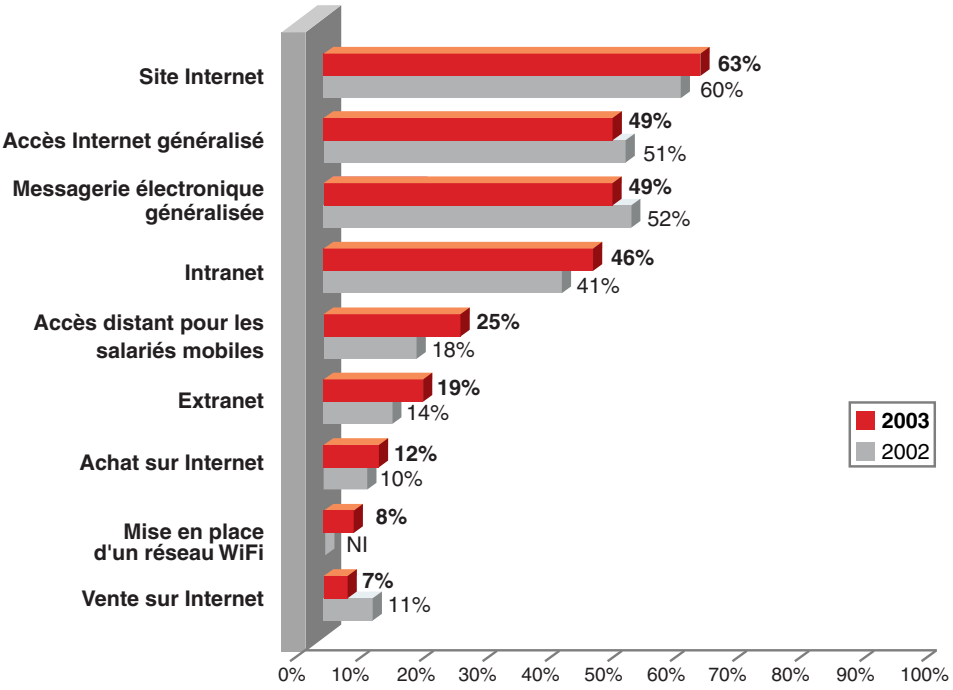
ANNEXE



Autres données nationales des entreprises

Plusieurs éléments dans les mesures mises en œuvre sont stables d'une année sur l'autre et en conséquence n'ont pas fait l'objet dans la présente étude d'un détail particulier [3]. Il nous a semblé plus pertinent de mettre en exergue quelques compléments sectoriels.

L'ouverture des systèmes d'information en 2003 ne fait pas exception à cette stabilité, hormis la progression de l'accès distant pour les salariés mobiles.

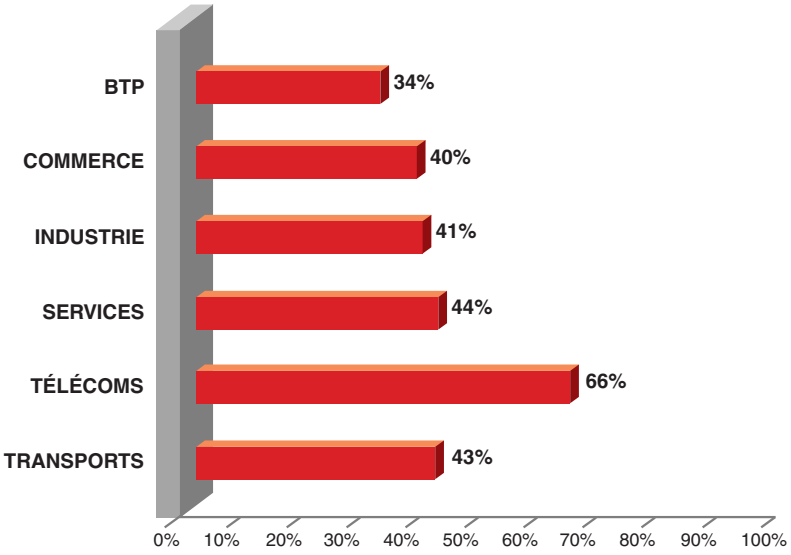


Le secteur d'activité influence cette ouverture :

	BTP	COMMERCE	INDUSTRIE	SERVICES	TÉLÉCOMS	TRANSPORTS
Site internet	53 %	66 %	64 %	65 %	84 %	58 %
Accès internet généralisé	40 %	51 %	43 %	53 %	73 %	59 %
Messagerie électronique généralisée	44 %	45 %	47 %	54 %	83 %	53 %
Intranet	30 %	55 %	41 %	47 %	76 %	41 %
Accès distant pour les salariés mobiles	12 %	29 %	20 %	30 %	35 %	30 %
Extranet	10 %	25 %	16 %	20 %	46 %	16 %
Achat sur internet	3 %	15 %	11 %	13 %	43 %	13 %
Mise en place d'un réseau WiFi	2 %	6 %	7 %	14 %	16 %	8 %
Vente sur internet	0,1 %	12 %	2 %	6 %	48 %	10 %

[3] Toutes les études sur la sinistralité et les politiques de sécurité sont disponibles sur le site www.clusif.asso.fr

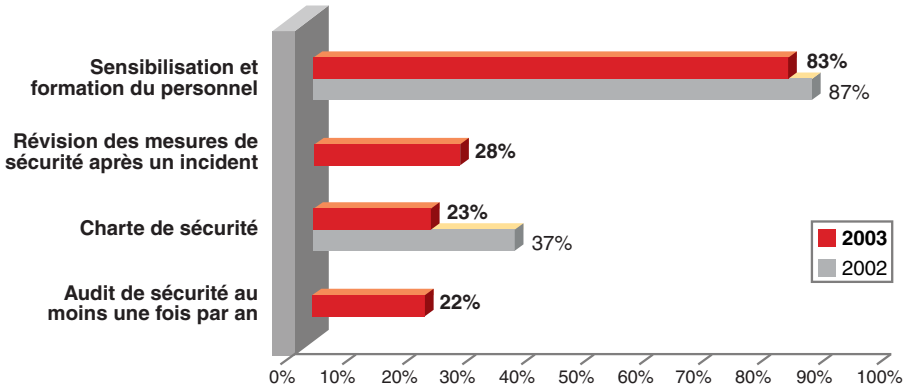
La politique de sécurité est définie dans 41 % des cas, selon la répartition sectorielle suivante :



49 % des entreprises ont au moins une personne en charge de la sécurité informatique.
Un peu plus d'un tiers a placé son système informatique et télécoms sous contrat d'infogérance, dont 25 % en totalité et 13 % partiellement. Dans ce cas, elles sont 86 % à exercer un suivi régulier sur cette infogérance (sécurité technique des matériels, sécurité des informations transmises ou stockées, continuité d'activité...).
La moitié (51 %) fait appel à des prestataires externes, à répartition égale entre audit conseil et services opérationnels.

Management de la sécurité

Le taux de sensibilisation, réparti également entre toutes les tranches d'effectifs, est dans une certaine opposition avec la réalité du terrain. Quelle entreprise oeuvrant dans le domaine de la sécurité n'a pas constaté de nombreux cas où les règles de base ne sont pas appliquées par les salariés ? (mots de passe en évidence, téléchargements non autorisés…)



Mesures de sécurité physique par secteur :

Constatant les faiblesses des protections incendie, nous rappelons ici quelques éléments extraits du document du Clusif *«La sécurité incendie des équipements techniques* [4]».

«Les lois, décrets et règlements des autorités, de l'inspection du travail et des associations professionnelles en matière de construction s'appliquent évidemment aussi aux salles serveurs. Il n'existe pas encore de prescriptions particulières les concernant.

Les impératifs techniques à satisfaire par l'installateur pour le raccordement et l'exploitation des serveurs, ainsi que les recommandations pour la construction et l'architecture des centres de calcul figurent dans les spécifications d'installation du constructeur du système informatique.

Il convient en outre de respecter les conditions et recommandations des sociétés d'assurance en matière d'installations informatiques.

- *Les spécifications et réglementations sont décrites dans les règles techniques ou cahiers de spécifications de l'APSAD et dans certains textes réglementaires relatifs à la sécurité incendie…(tels que)… certaines normes de l'AFNOR, le Code du Travail (notamment le R.233.38 sur l'obligation de sécurité incendie du chef d'entreprise)…»*

	BTP	COMMERCE	INDUSTRIE	SERVICES	TÉLÉCOMS	TRANSPORTS
Dispositif de protection électronique	**72 %**	**93 %**	**87 %**	**77 %**	**84 %**	**90 %**
Dispositif anti-incendie dans les locaux informatiques	**45 %**	**59 %**	**52 %**	**58 %**	**84 %**	**45 %**
Accès restreint aux locaux techniques	**24 %**	**40 %**	**39 %**	**40 %**	**74 %**	**28 %**
Dispositif antivol du matériel	**22 %**	**32 %**	**26 %**	**37 %**	**51 %**	**25 %**

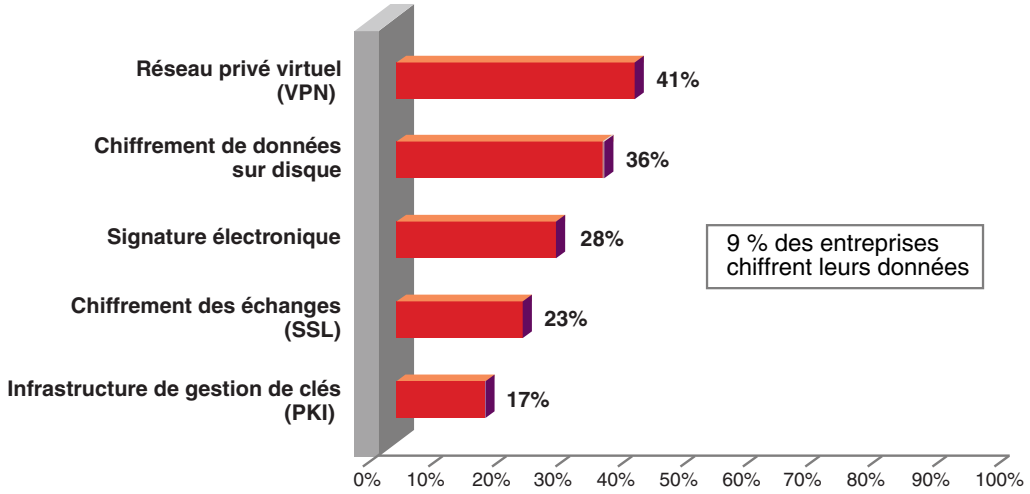
Mesures de sécurité logique par effectif :

Comme nous l'avons vu dans *Regards sur l'actualité*, les logiciels antivirus sont installés mais pas toujours optimisés dans leur usage. Pour les mots de passe, le terme «non trivial» a bien été expliqué ; toutefois, les réponses nous semblent assez éloignées de la réalité.

[4] Document disponible sur https://www.clusif.asso.fr/fr/production/ouvrages/pdf/SecuriteIncendie2002.pd

	De 10 à 199	De 200 à 499	De 500 à 999	Plus de 1.000
Logiciel antivirus	90 %	95 %	89 %	94 %
Mot de passe non trivial	84 %	89 %	92 %	93 %
Pare-feu (firewall)	44 %	83 %	88 %	93 %
Surveillance du réseau contre les intrusions, système d'alerte	34 %	48 %	54 %	73 %
Réalisation de tests (intrusion, vulnérabilité…)	12 %	11 %	16 %	14 %
Chiffrement de données	9 %	13 %	15 %	19 %
Authentification renforcée par un dispositif électronique	8 %	20 %	20 %	38 %

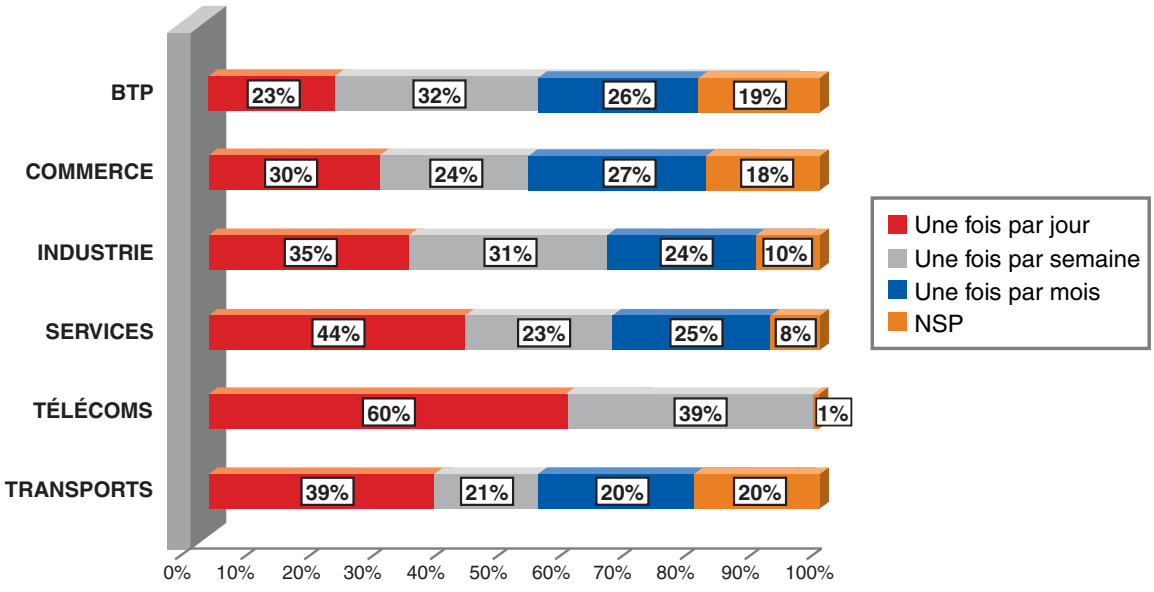
Le chiffrement de données, peu pratiqué, se décline dans différentes solutions :



Les mises à jour : logiciels antivirus et correctifs *(patchs)*

5 % d'entreprises n'ont pas encore de logiciel antivirus. Dans les autres cas, seulement 36 % en effectuent la mise à jour quotidienne.

Tous les secteurs sont concernés par cette carence :



Concernant la mise à jour des systèmes avec les correctifs majeurs ou recommandés, 51 % des entreprises les ont appliqués.

Mise à jour des systèmes par les *patchs* :

	De 10 à 199	De 200 à 499	De 500 à 999	Plus de 1000
Oui	50 %	59 %	62 %	77 %
Non	50 %	41 %	38 %	23 %

Cette procédure est formalisée dans 47 % des cas et elle est alors externalisée à 68 %.
Ces chiffres sont en cohérence avec le niveau de veille effectué par seulement 41 % de sociétés sur les questions de sécurité des systèmes. En l'occurrence, c'est donc sur le prestataire que repose la protection.
Les entreprises estiment, à 52 %, avoir consacré davantage de temps qu'en 2002 pour ces tâches.

Continuité de l'activité

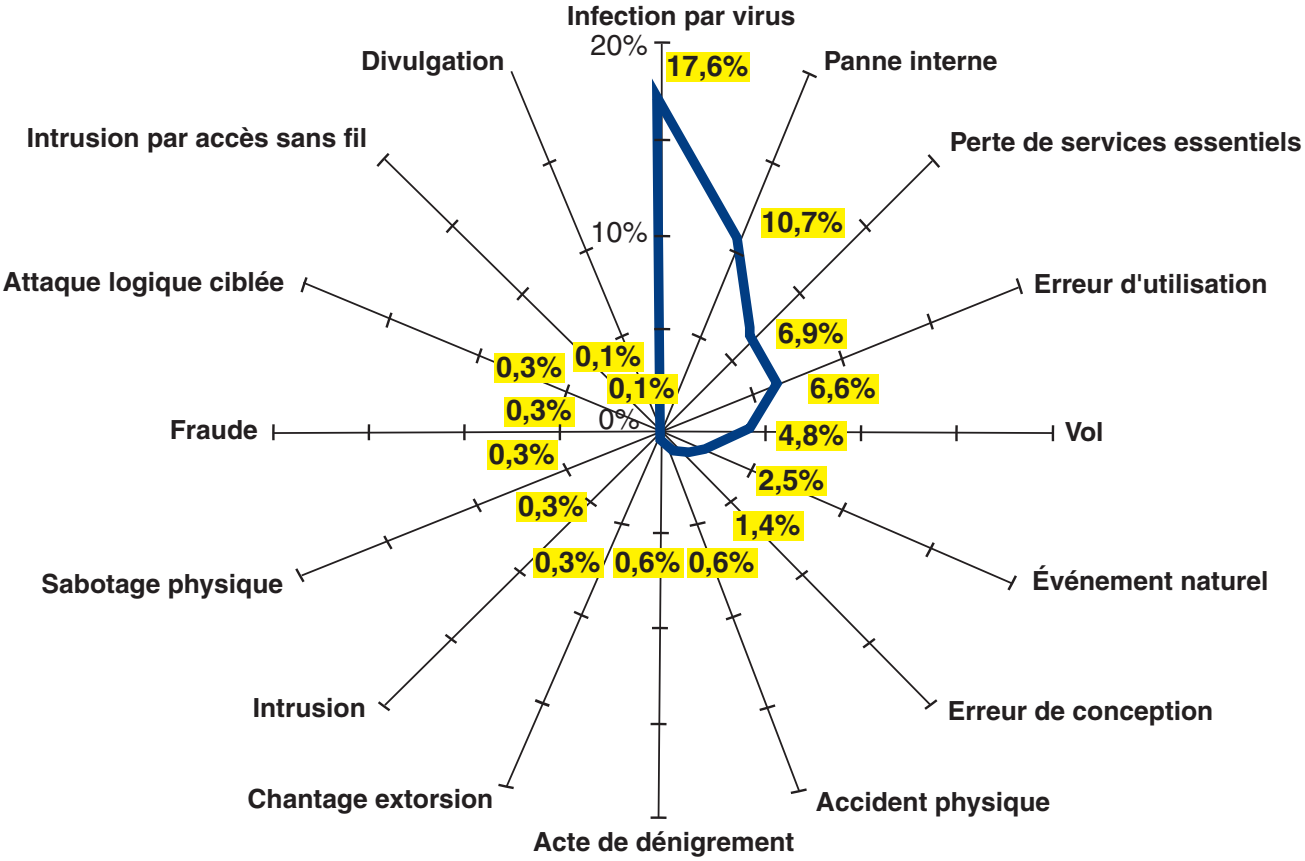
Les moyens mis en œuvre ne sont pas à la hauteur de l'importance stratégique des systèmes d'information pour la pérennité de l'entreprise.

Répartition par secteur :

	BTP	COMMERCE	INDUSTRIE	SERVICES	TÉLÉCOMS	TRANSPORTS
Procédure de stockage hors site des sauvegardes	52 %	51 %	48 %	63 %	75 %	35 %
Plan de secours des moyens informatiques	15 %	10 %	19 %	21 %	73 %	18 %
Plan de continuité d'activité économique	14 %	11 %	16 %	18 %	48 %	25 %
Plan de crise	10 %	6 %	11 %	11 %	49 %	10 %

Evaluation de la sinistralité

Lors du recueil des données, il a bien été insisté sur la notion de sinistre, différente d'un incident en terme de gravité de l'impact. Cette différenciation a eu pour résultat que 80 % des entreprises ont déclaré n'avoir subi aucun sinistre en 2003.



Impact financier des sinistres

Le coût financier consécutif aux sinistres est résorbé par les moyens suivants :

Trésorerie courante	Assurance	Action juridique
90 %	9 %	1 %

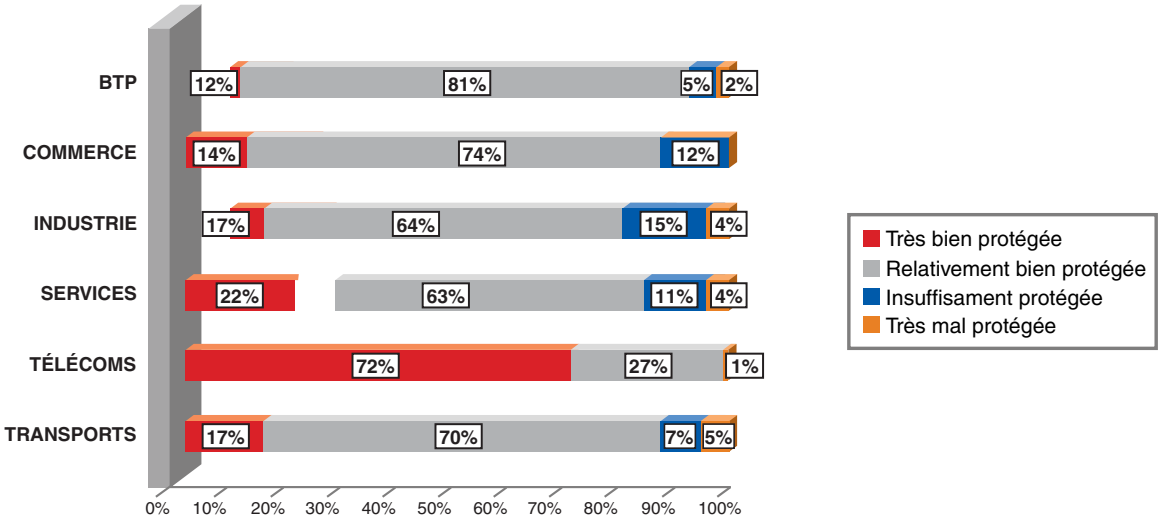
Pour les quelques entreprises qui évaluent le préjudice subi par des sinistres, la répartition de l'impact financier donne le tableau suivant :

Coût de réparation ou remplacement du matériel informatique endommagé ou manquant	**27 %**
Perte d'exploitation	**25 %**
Coût de reconstitution de données, logiciel ou procédure endommagés ou perdus	**19 %**
Perte de patrimoine	**14 %**
Coût de renforcement des protections	**13 %**
Responsabilité encourue par l'entreprise	**2 %**

Sentiment de protection

Les entreprises s'estiment majoritairement relativement bien ou très bien protégées (86 %).

Sentiment de protection par secteur :



36 % des entreprises envisagent de renforcer dans les deux ans leurs dispositifs de sécurité. Et spontanément, avec plusieurs réponses possibles, leurs choix s'orientent sur les quatre axes suivants :
- la protection contre les virus, 60 %,
- la protection contre les intrusions, 23 %,
- les dispositifs de sauvegardes, 11 %,
- la protection contre le vol, 8 %.

Ces derniers chiffres prouvent bien, s'il en était encore besoin, que seule la formation et la transmission de la bonne information feront évoluer les mentalités et les bonnes pratiques en matière de sécurité de l'information en France.

L'ESPRIT DE L'ÉCHANGE

Club de la Sécurité des Systèmes d'Information Français
30, rue Pierre Sémard - 75009 Paris
TÉL.: 01 53 25 08 80
Fax.: 01 53 25 08 88
Mail : clusif@clusif.asso.fr
Web : http://www.clusif.asso.fr

Publication juin 2004