



Les systèmes d'information en
France :
Politiques de sécurité et
sinistralité

Bilan 2003

Présentation à la Presse

↪ Extraits de « Regards sur l'actualité »

↪ Trois focus

- entreprises de 200 à 500 salariés
- collectivités locales
- établissements hospitaliers

↪ Tableau de sinistralité nationale



Une etude originale par :

- Des thematiques d'actualite avec le point de vue du Clusif et des recommandations
- Trois focus pour augmenter l'attractivite de l'etude
- De nouveaux items
- La modification de questions entrainant un fort impact sur les reponses



Déploiement du WiFi : quelle sécurité ?

- A partir de 200 salariés, ce sont de 20 % à 33 % d'entreprises concernées.
- Un réseau chiffré dans seulement 40 % des cas.
- 💣 Attention aux conséquences : sécuritaires, réglementaires, juridiques...

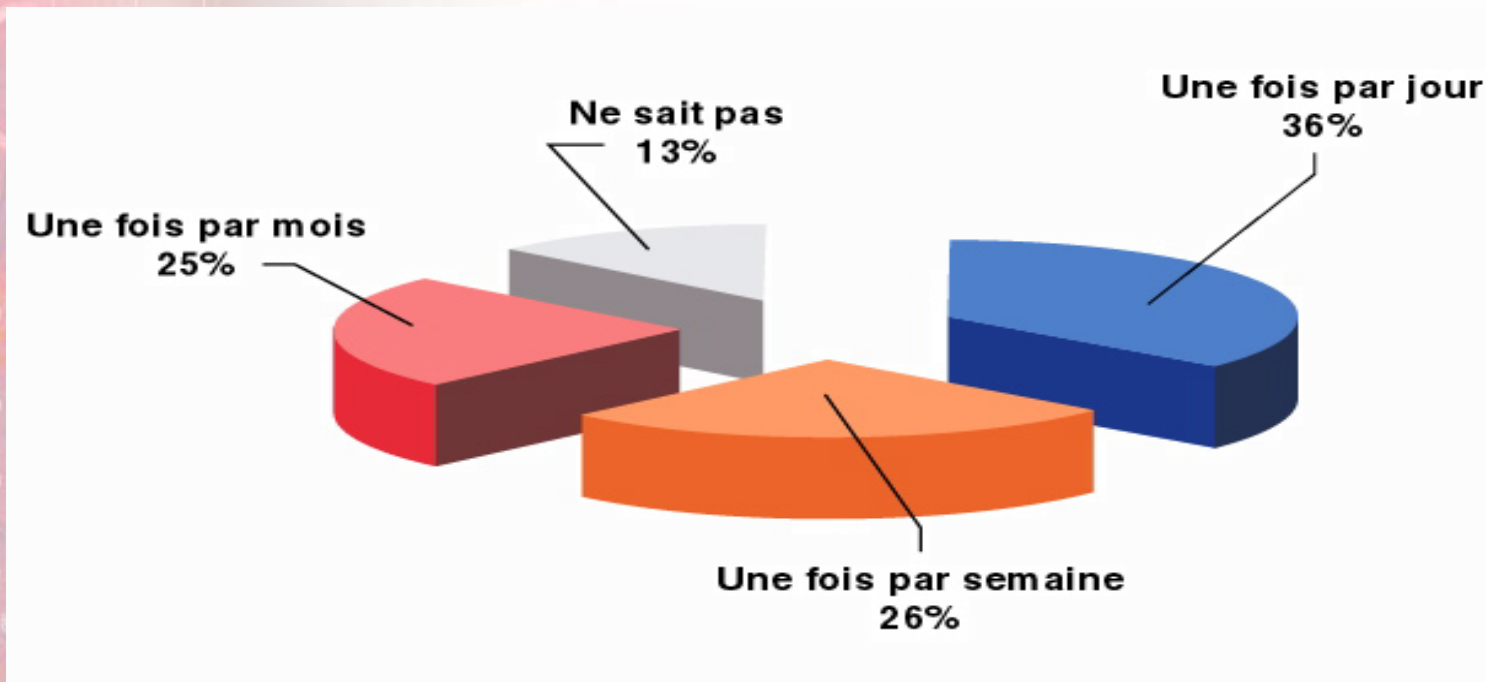


Nomadisme : quelle protection de l'information ?

- 25 % d'entreprises ont un réseau accessible à distance pour leurs salariés (moyenne nationale)
- A partir de 500 salariés, c'est plus de 70% des entreprises qui sont exposées aux risques de l'accès distant
- 💣 Vol physique des terminaux mobiles
- 💣 Sécurisation des accès, des postes, des données...

Quel impact des virus ?

- Sinistralité en baisse, à 17,6 % : les entreprises parlent d'incidents
- Quasiment pas d'étude d'impact financier
- Fréquence des mises à jour :



10 % d'entreprises déclarent ne pas avoir d'antivirus

RoI ou RoSI, peu de visibilité

- Quasi absence de calcul d'impact financier des incidents ou des sinistres : à peine la moitié des entreprises de plus de 1000 salariés y procèdent
- Manque de prise de conscience des dirigeants
- 💣 Absence de sécurité = Risques économiques, réglementaires, juridiques, pour le dirigeant

Gestion des correctifs : attaques virales en vue...

Seulement 51 % des répondants ont installé les correctifs majeurs ou recommandés

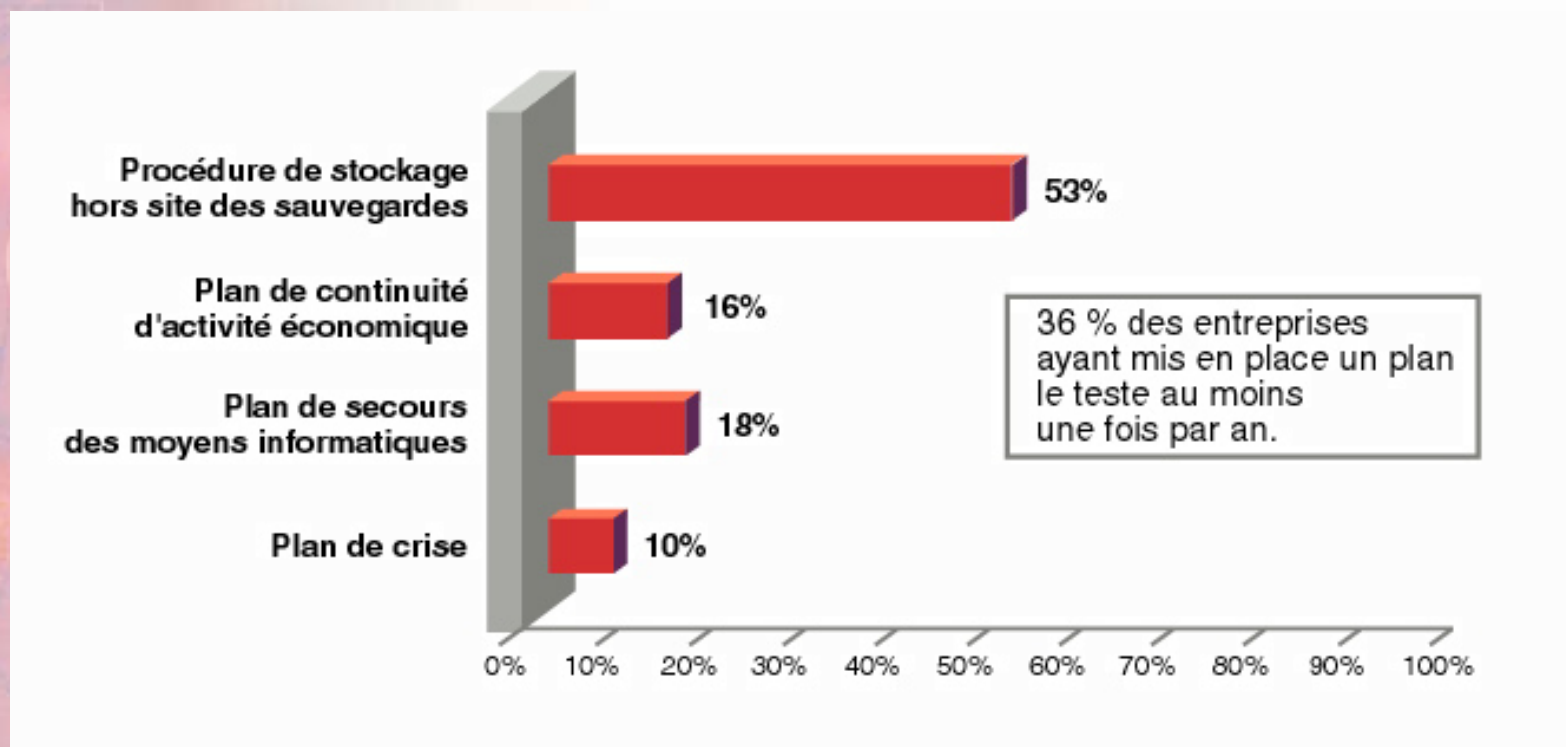
Par effectifs :

10 à 99	200 à 499	500 à 999	Plus de 1000
50 %	59 %	62 %	77 %

Par secteurs :

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

Continuité d'activité : la prise de risque des entreprises



Trois focus

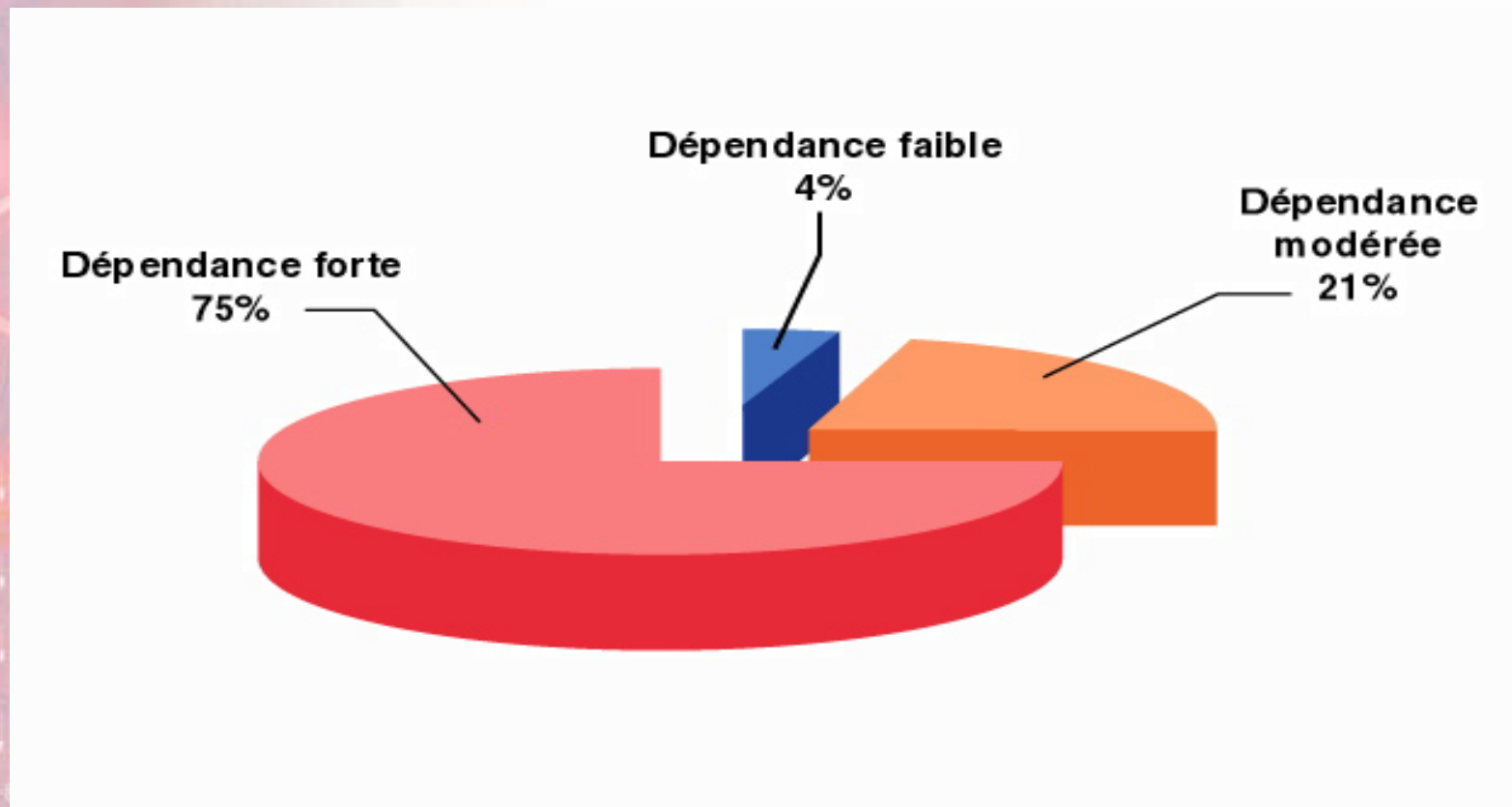
- ↪ Entreprises de 200 à 500 salariés
- ↪ Collectivités locales et territoriales
- ↪ Etablissements hospitaliers



Politiques de sécurité et sinistralité dans les entreprises de 200 à 500 salariés



Une forte dépendance au Système d'Information...



...cohérente par rapport à l'ouverture

Moyens mis en oeuvre

- 83 % ont formalisé la politique de sécurité
- 20 % n'ont personne en charge de la SSI
- 32 % ont recours à l'infogérance, dont 11 % en totalité



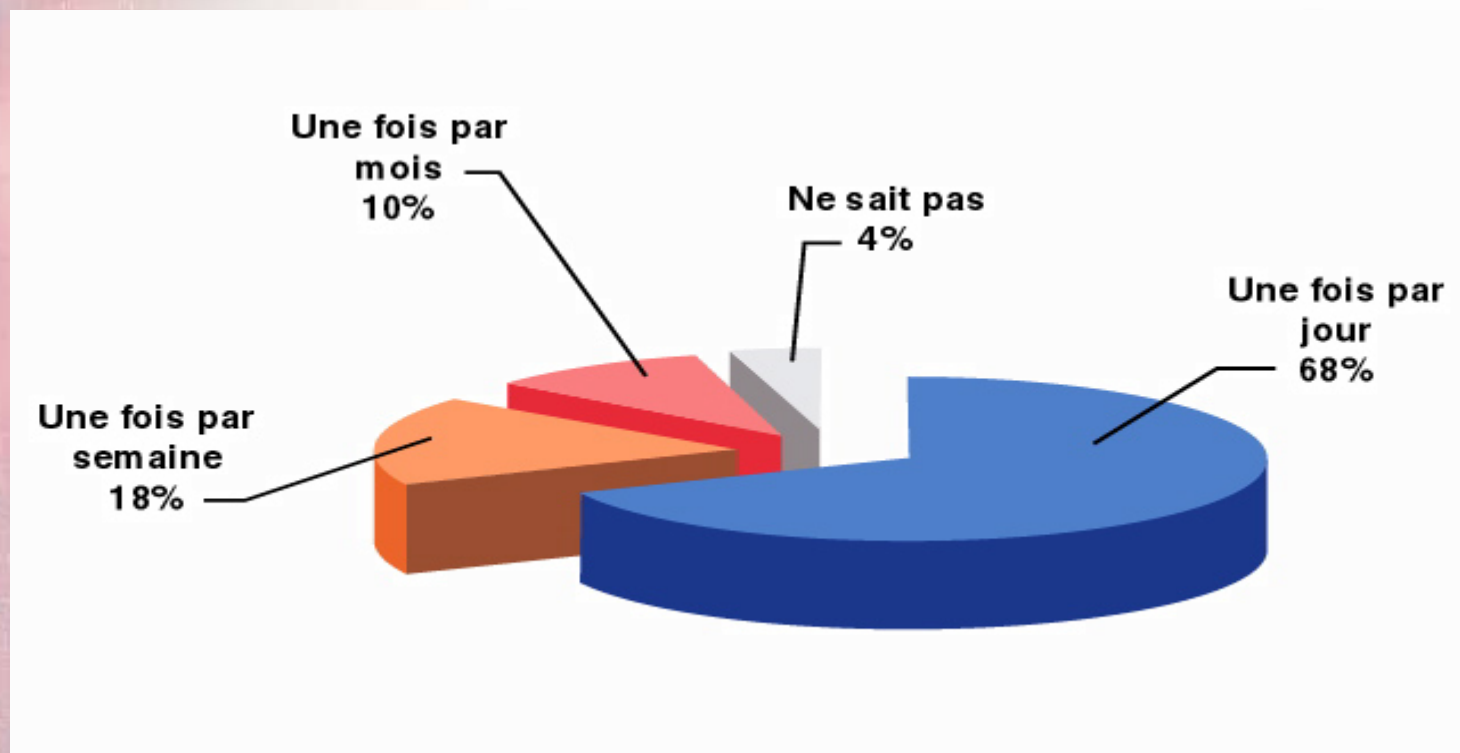
Moyens mis en oeuvre (2)

Sécurité logique

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% (accès distant 51 %)
Authentification renforcée par un dispositif électronique	20%

Moyens mis en oeuvre (3)

Un assez bon niveau des mises à jour d'antivirus...



MAIS 41 % n'ont pas installé les correctifs majeurs ou recommandés

Moyens mis en œuvre (4)

Continuité de l'activité : « *Les hommes ne voient la nécessité que dans la crise* »

La **pérennité** de l'entreprise n'est **toujours pas assurée**.

Les politiques de sécurité ne prennent pas en compte, dans leur majorité, cette dimension stratégique.

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 (1)

- 59 % déclarent n'avoir subi aucun sinistre.
- Relativisation des événements : incidents
- Pas d'évaluation de l'impact financier dans 76 % des cas

Evaluation de la sinistralité (2)

41 % déclarent des sinistres selon les facteurs déclenchant suivants :

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

* Rappel : 41 % n'ont pas installé les correctifs majeurs ou recommandés

En guise de conclusion de ce focus

93 % s'estiment très bien ou relativement bien protégé.

Cet optimisme est à tempérer, compte tenu des failles dans les mesures mises en œuvre.

Toutefois, une entreprise sur deux envisage de renforcer ses dispositifs dans les deux ans.

Politiques de sécurité dans les collectivités locales et territoriales



Un large éventail de situations

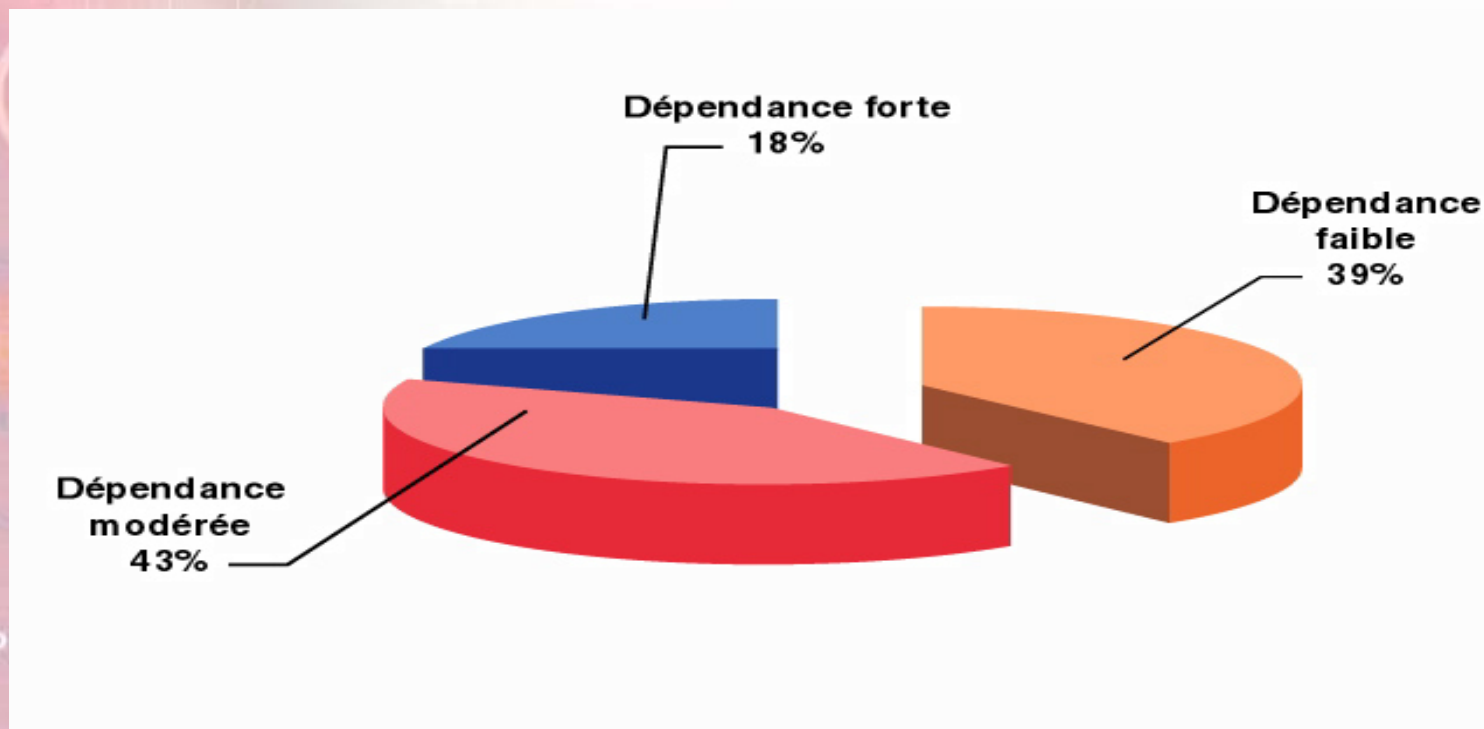
Contrairement au secteur privé (classement par effectif et secteur), peu de points de comparaisons dans les moyens financiers et humains pouvant être dégagés pour la SSI entre :

- les communes, de tailles très diverses et au nombre de 36 000 en France,
- les départements (96)
- les régions (22)
- les communautés urbaines.

Une mutation en route

Le projet ADELE, plan d'action de l'administration électronique 2004-2007, va influencer sur l'ouverture des systèmes.

Aujourd'hui, une dépendance modérée...



...en accord avec une ouverture très modérée

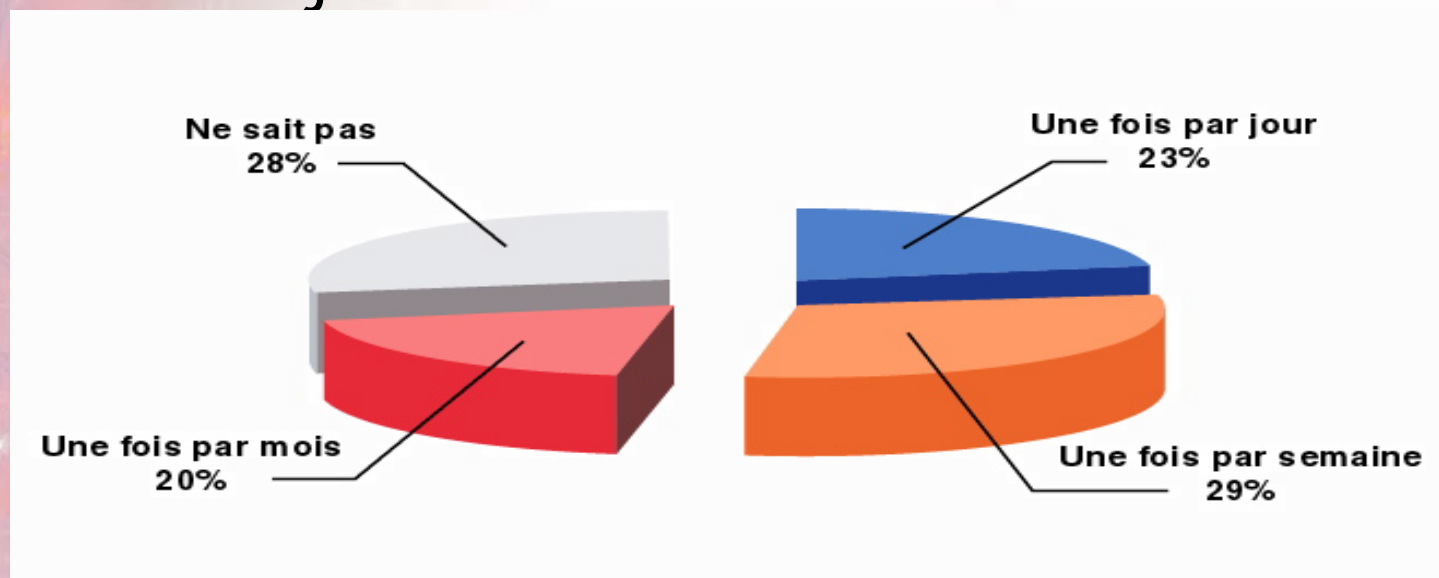
Moyens mis en oeuvre (1)

Des moyens qui, globalement, demandent un renforcement par rapport aux objectifs.

- 21 % ont au moins une personne en charge de la SSI
- 37 % ont recours à l'infogérance, dont 21 % en totalité
- ⇒ Prise en charge de la sécurité cohérente en raison de l'ouverture basée essentiellement sur des sites internet (48 %)

Moyens mis en oeuvre (2)

- Stockage hors site des sauvegardes : 54 %
- ⇒ Renforcement attendu
- Installation des correctifs majeurs ou recommandés 80 %
- Mises à jour des antivirus :



Conclusion de ce focus

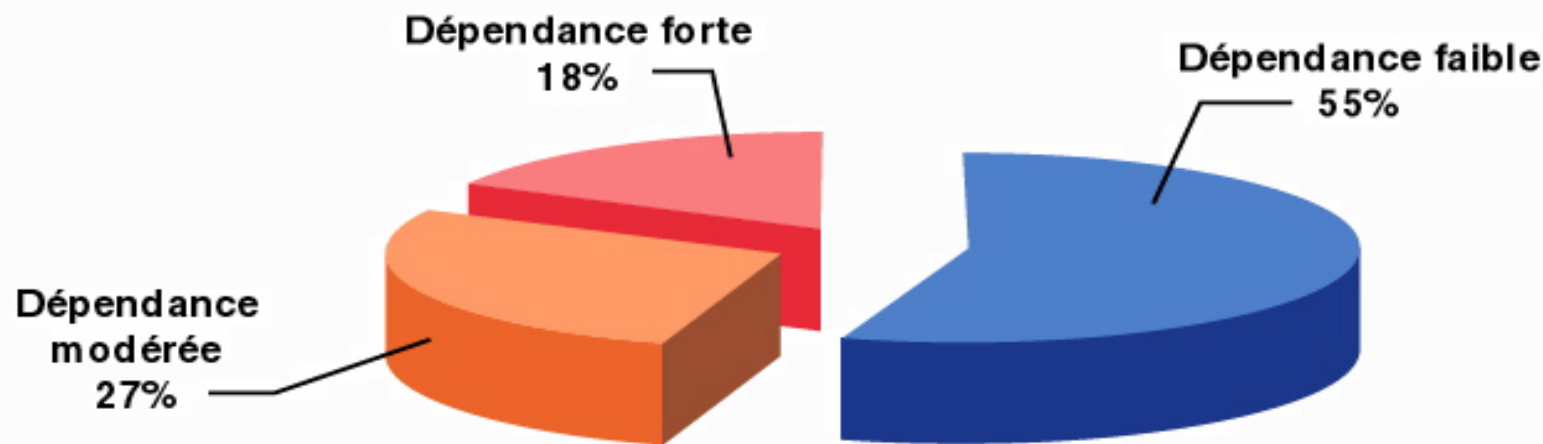
- Des systèmes d'information appelés à une large ouverture : réalisations actuelles et projets tests en témoignent
- Des besoins en hommes et en équipements annoncés
- La formation d'experts en sécurité : une priorité



Politiques de sécurité dans les établissements hospitaliers

Des systèmes orientés sur le traitement des données administratives

D'où une dépendance faible



Une (r)évolution en cours

La dématérialisation des fichiers, des données, afin que le patient accède à son dossier, va influencer sur l'ouverture des systèmes, aujourd'hui moyennement développée.

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

Moyens mis en œuvre (1)

- 59 % ont au moins une personne en charge de la SSI, dont 44 % à temps plein
- 21 % ont recours à l'infogérance, dont 16 % en totalité
- Seulement 42 % ont défini une politique de sécurité

Moyens mis en œuvre (2)

→ Des situations très hétérogènes selon les entités, à commencer par la sensibilisation.

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 %

Moyens mis en œuvre (3)

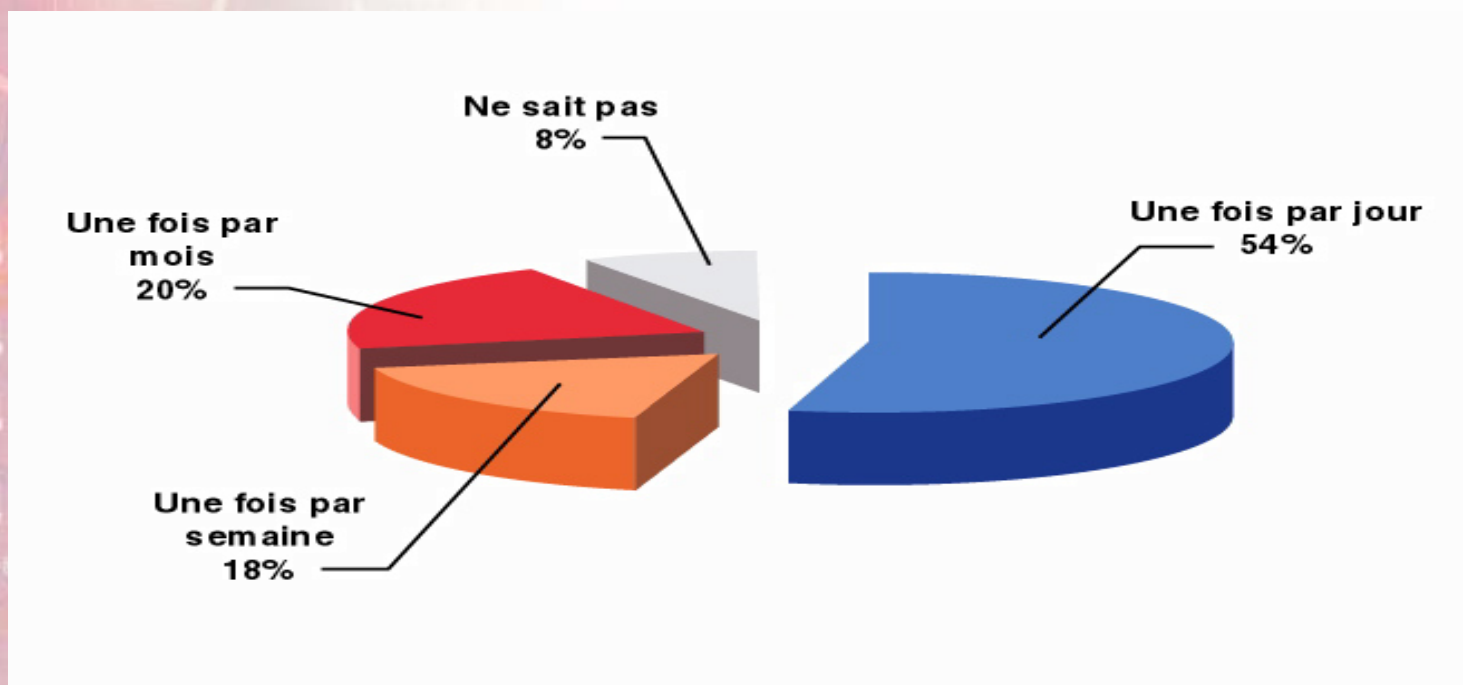
→ Identification, authentification et chiffrement : la nouvelle législation appelle des moyens accrus

Le niveau actuel des mesures en matière de continuité d'activité n'est pas en phase :

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

Moyens mis en œuvre (4)

- Tous les établissements interrogés ont installé les correctifs majeurs ou recommandés.
- Fréquence des mises à jour d'antivirus :

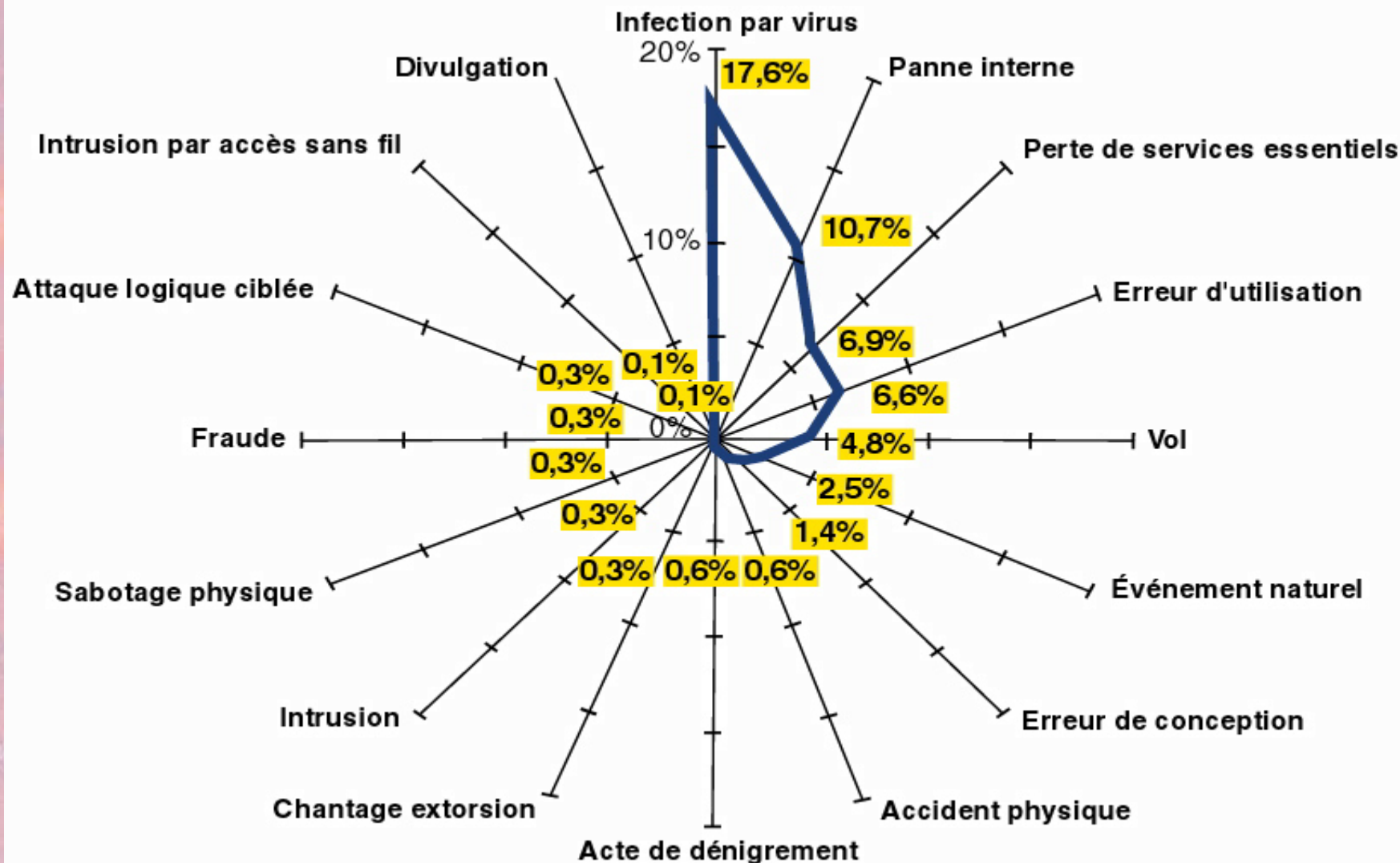


En conclusion de ce focus

Les nouveaux réseaux de santé qui se mettent en place suite à la loi du 4 mars 2002 se distinguent plus par la sensibilité du secteur que par des aspects qui leurs seraient propres en matière de sécurité des S.I.:

- Partage des informations
- Nouveaux modes de communication entre établissements de santé, publics et privés
- Sécurité des données à caractère personnel des patients
- Sécurité des échanges
- Traçabilité : tant pour les autorisations d'accès que pour les produits (le sang par exemple)

Tableau de la sinistralité nationale



Conclusion...finale!

La Sécurité des Systèmes d'Information est au cœur du développement de l'économie.

C'est par le numérique que la France et ses partenaires européens gagneront les nouvelles batailles.

Sécurité des systèmes, sécurité de l'information, une même finalité :

défendre le patrimoine et les savoir-faire