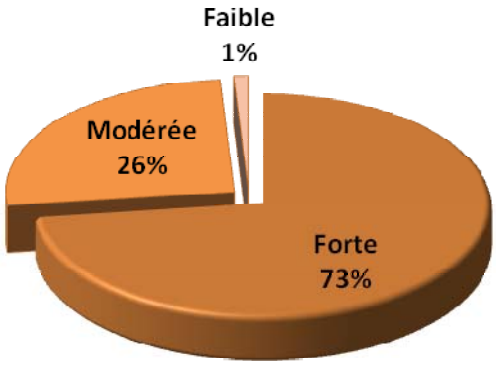
Extrait du **Livre Blanc : Sécurité des Systèmes d'Information**

Eléments chiffrés

Dépendance des entreprises vis-à-vis de leur Système d'Information (Clusif 2008)

Les systèmes d'information sont devenus un des éléments névralgiques dans le fonctionnement et la performance des organismes (Entreprises, administrations, …).

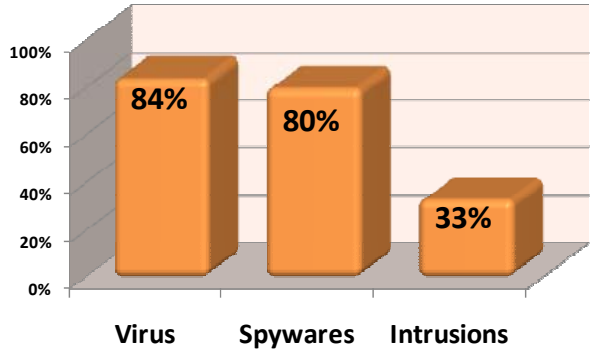
Cependant, une dépendance trop forte et une complexité non maîtrisée, sont synonymes de faiblesse potentielle et d'insécurité, si elles ne sont pas gérées



Répartition des d'attaques subies par les entreprises (FBI : 2005)

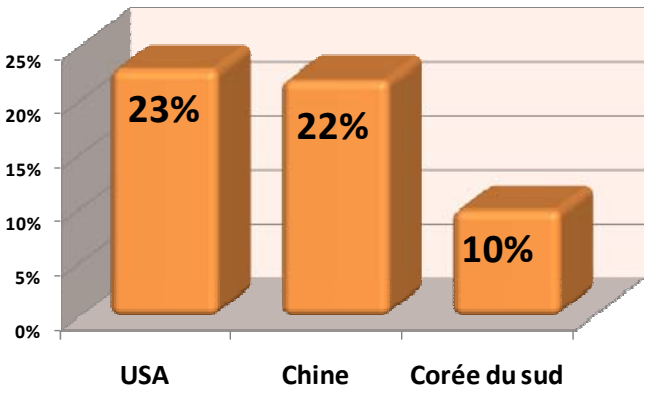
Les exemples de malveillance visant les systèmes d'information sont nombreux :

- Les ordinateurs incontrôlables et inutilisables à cause de virus informatiques.
- Les logiciels espions (spyware) installés discrètement sur nos ordinateurs pour épier nos habitudes, nos comportements, nos données.
- L'intrusion par un pirate dans un réseau engendrant le vol d'informations.



Top 3 : Provenance des SPAM

Le SPAM, ou envoi massif de courriers indésirables, présente des contenus très variés, principalement pour des sollicitations commerciales. Au delà de l'aspect « qualitatif » des produits proposés, cela constitue une véritable problématique d'engorgement des serveurs et messagerie et des boites aux lettres. La Facture est estimée à plus de 10 milliard d'€. Le SPAM est aussi utilisé dans le cheminement de code malicieux et la phase de prise de contact dans l'ingénierie sociale.



Extrait du **Livre Blanc : Sécurité des Systèmes d'Information**

Quelques Faits …

Continuité de Service : Un petit maillon d'une chaine, peut la rendre vulnérable.
En juillet 2008, une carte réseau défectueuse du système de la tour de contrôle a engendré la fermeture temporaire de l'aéroport de Dublin.

Ingénierie sociale : le SCAM, arnaque en faisant miroiter de l'argent
Un gérant d'un cybercafé Camerounais, responsable d'un réseau de SCAM est interpellé en 2006 après les plaintes de plusieurs victimes françaises, pour un préjudice de 500 000 €.

Les codes malicieux (virus, spyware, cheval de Troie) : Véritable pandémie
Le nombre d'un millions de logiciels malveillants a été dépassé en 2008.
Plus de 3200 nouveaux virus ou variantes font leur apparition chaque mois.
(F-Secure 2008).

33% de tous les disfonctionnements des applications Windows, sont causé par des spywares.
(MS Watson/OCA, 2004).

Botnet : les attaquants cherchent désormais à « monétiser » leurs méfaits
En aout 2008, les autorités néerlandaises ont arrêté un botmaster de 19 ans qui était à la tête du botnet Shadow contrôlant plus de 100 000 machines zombies.

Insécurité sur Internet
Un ordinateur non protégé, connecté à internet subit en moyenne 100 attaques par jour.

Politique de sécurité du système d'information au sein des entreprises Françaises
Seulement 55 % des entreprises sont dotées d'une Politique de sécurité de l'information (PSI).

« Cyber guerre » : de la fiction à la réalité
Avril 2007, cyber affrontement entre russes et estoniens suite à l'enlèvement à Tallin d'un mémorial de soldats soviétiques. Rapidement, l'Estonie, a subi une série d'attaques importantes (déni de service, virus). Les cibles: sites gouvernementaux, banques, médias et organisation politiques. Même les appels aux urgences (ambulances, incendies) sont restés indisponibles pendant plus d'une heure.