



Forum du CLUSIF

21 Septembre 2006

Forum du CLUSIF

- Bilan des travaux effectués au CLUSIF sur la saison 2005/2006
- Lieu d'échange entre les membres du CLUSIF
- Point d'avancement des travaux en cours
- Regard sur le futur



Maîtrise et Protection de l'Information

M. Eric BALANÇA (Venice Security)

Objectif du document

- Rapport « **Maîtrise et protection de l'information** » publié en juin 2006
- Un double objectif :
 - o Inciter les dirigeants de PME –PMI, mais aussi l'ensemble des acteurs économiques, à **utiliser les technologies de l'information et de la communication** ;
 - o Apporter des éléments pour que l'entreprise **s'engage dans une politique de réduction des risques inhérents à l'emploi de ces technologies**
- Rôle prépondérant des TIC
 - o Accéder à de nombreuses sources d'informations,
 - o Assurer la diffusion d'informations aux bonnes personnes et au bon moment
 - o Suivre sa réputation et anticiper les évolutions

Les dimensions de l'information

- « Maîtriser et protéger » l'information dans et hors des murs de l'entreprise
- Identification de 3 catégories de flux d'informations
 - o L'information interne à l'entreprise et accessible uniquement à un nombre restreints de personnes « habilités »
 - o L'information en libre accès dans l'entreprise ou celle communiquée à l'extérieur
 - o L'information concernant l'entreprise dont elle n'est ni initiatrice, ni destinatrice
- L'entreprise a intérêt à identifier ses flux d'informations et déployer les moyens adaptés pour les maîtriser et protéger

« Ne pas prévoir, c'est déjà gémir »

Léonard de Vinci

« Mieux vaut penser le changement que changer de pansement »

Francis Blanche

Et pour aller plus loin ...

- Nouveau GT : « Destruction de l'information »
 - **Objectif** : sensibiliser tout acteur/décideur à cet aspect dans le cycle de vie de l'information
 - S'adresse aux entreprises ayant un savoir-faire spécifique ou une position concurrentielle attractive
 - **Programme** :
 1. Rappel sur le cycle de vie, la sensibilité et la durée de vie de l'information
 2. Techniques de récupération des informations (Etat de l'Art)
 3. Typologie/profil des acteurs
 4. Présentation des méthodes de destruction des informations (niveaux de destruction attendus selon formats et types de supports ...)
 5. Procédures et moyens de contrôle de leur application
 6. Normes et standards

Lancement le 29 septembre à 14h30 dans les locaux du CLUSIF



Risk Manager & Responsable
Sécurité du Système d'Information
*Deux métiers s'unissent pour la gestion
des risques liés au Système d'Information*

M. Luc VIGNANCOUR (MARSH)

RM et RSSI

- Document réalisé par un panel composé de membres du CLUSIF et de membres de l'AMRAE
- Réunions mensuelles pour échanger sur les différents sujets et valider les écrits

RM et RSSI

Le Risk Manager traite des risques **de l'entreprise** par l'analyse des impacts sur les divers secteurs qui la composent :

- Production
- Finance
- Ressources humaines
- Engagement à l'égard des tiers

Le système d'information est souvent perçu comme un ensemble d'outils pour l'entreprise plutôt que comme un processus intégré dans l'entreprise.

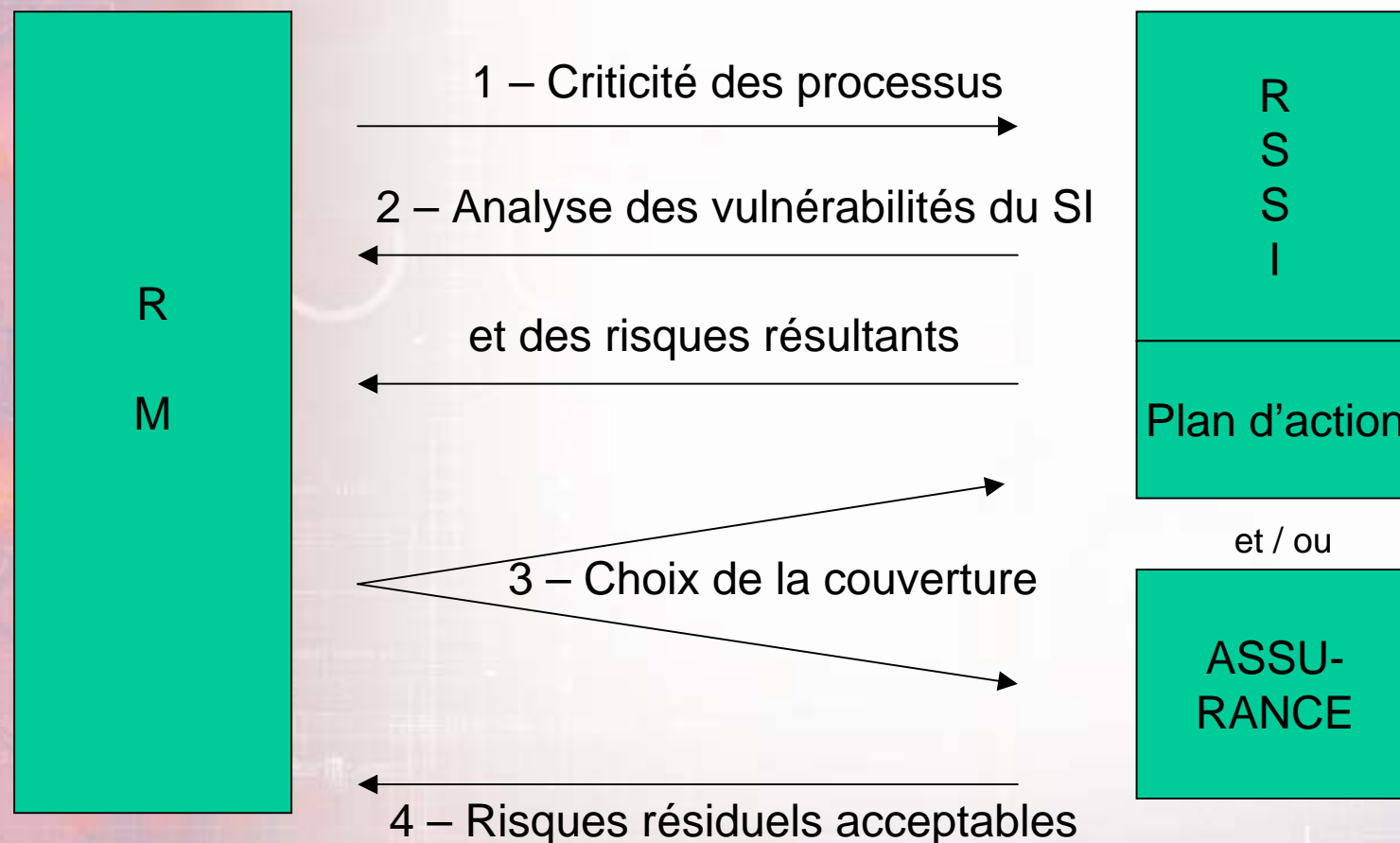
RM et RSSI

Le RSSI traite des risques **des systèmes d'information** par l'analyse des impacts sur son domaine :

- Disponibilité
- Intégrité
- Confidentialité
- Traçabilité

Il manque au RSSI les conséquences de ces impacts sur le fonctionnement de l'entreprise.

Communication RM ↔ RSSI



RM et RSSI

- Ce processus de communication interactif permet
 - au RSSI de retirer un support supplémentaire pour la gestion des risques liés au SI
 - au RM d'en retirer une connaissance plus complète des risques de ce domaine spécifique
- Et donc une meilleure gestion des risques de l'entreprise



Sécurité de la messagerie électronique

M. Robert BERGERON (Cap Gemini)

Sécurité de la messagerie

- Objectifs du document :
 - Fournir au lecteur les bases pour la compréhension des risques associés à la messagerie et leurs parades.
- Destination :
 - DSI, RSSI, personnes en charge d'un projet de messagerie
- Contenu :
 - Architecture et Protocoles
 - Risques et menaces
 - Solutions
 - Aspects juridiques

L'architecture et les protocoles

- Les composants de base de la messagerie
 - MUA : Mail User Agent
 - MTA : Mail Transfer Agent
 - MDA : Mail Delivery Agent
- Les principaux protocoles
 - SMTP pour l'envoi (+ ESMTP)
 - POP3 et IMAP pour l'accès aux Boîtes-aux-lettres

Menaces et risques

- Atteintes aux flux légitimes
 - Perte d'un e-mail - Perte de confidentialité - Perte d'intégrité - Usurpation de l'identité de l'émetteur – Répudiation - ...
- Atteintes à la messagerie et au SI
 - Programmes malveillants (virus, chevaux de Troie, ...) - Spam - Interruption de service - Open-relay - ...
- Atteintes à l'organisation
 - Contenus illicites ou offensants - Utilisation abusive - Accomplissement d'actes frauduleux par la messagerie - Le phishing - ...

Solutions de sécurité

- Sécurisation des flux légitimes
 - Chiffrement et signature électronique
 - Sécurisation des protocoles
 - Traçabilité des échanges
- Sécurisation du système de messagerie
 - Filtrage et analyse de contenu (virus, spam) - Règles de communication (contrôle de contenu) - Conformité aux protocoles SMTP - ...
 - Positionnement des fonctions de sécurité (Interne, Hébergeur, MSSP, ISP)
- Mesures organisationnelles
 - Politique de sécurité, charte, bonnes pratiques (utilisateur et administrateur)



Réglementation

- Principaux thèmes évoqués :
 - La divulgation de données personnelles (salariés ou clients)
 - La contrefaçon (licences piratées par l'entreprise ou ses salariés)
 - Le non respect des dispositions de la Loi sur la Sécurité Quotidienne (LSQ) et la Loi sur l'Économie Numérique (LEN) sur la conservation des données de connexion et de chiffrement.
 - La divulgation de savoir faire par un salarié de l'entreprise



Création d'un label Formations CLUSIF pour les formations sécurité SI

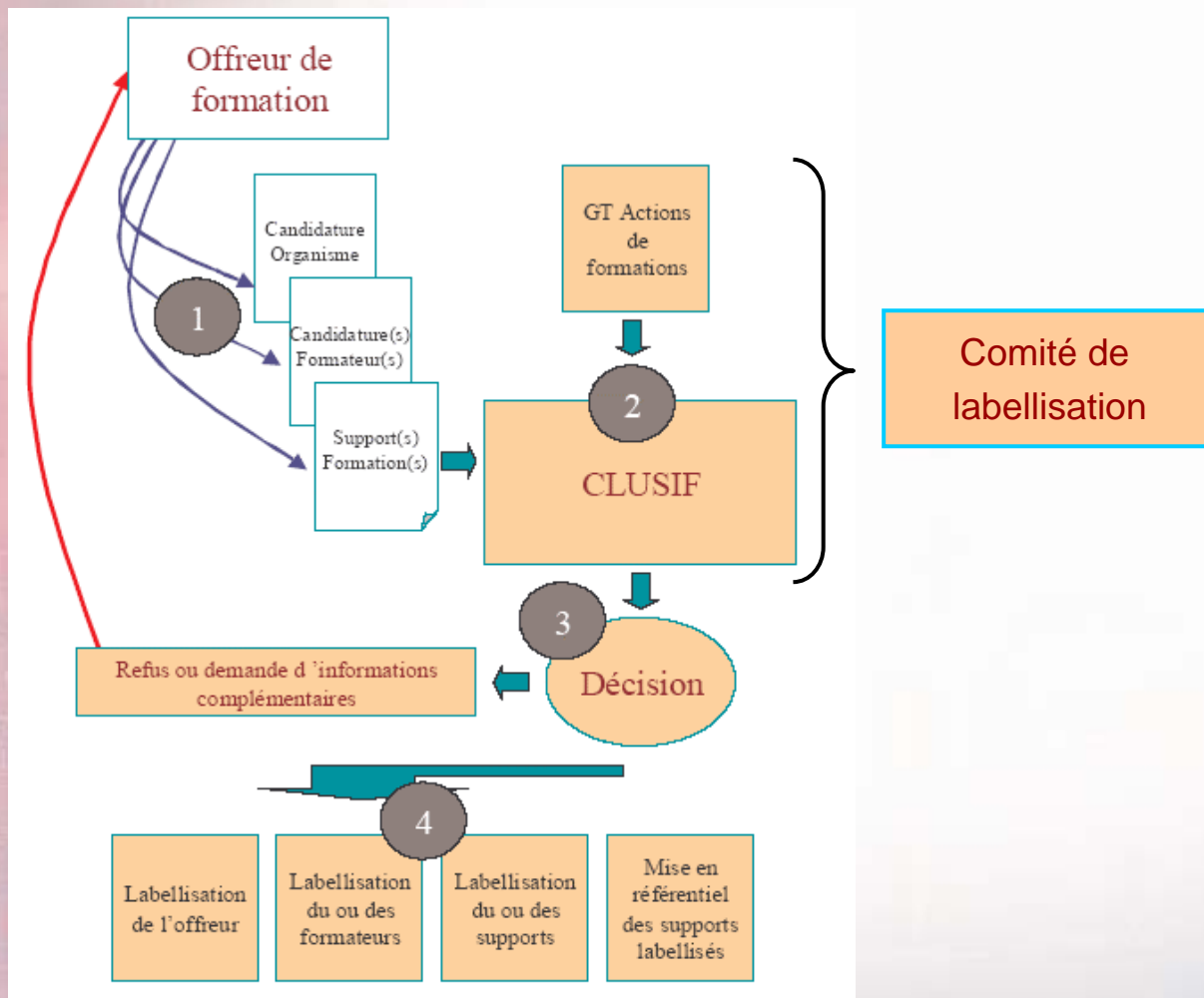
M. Pierre GOJAT (Orange)

Ce qui fait l'objet du label

Le Label que le CLUSIF projette de décerner s'applique à un triptyque:

- formation
- formateur délivrant cette formation
- organisme délivrant cette formation

Comment ça marche ? (1/2)



Comment ça marche ? (2/2)

Le Label que le CLUSIF décerne

- est valable un an
- est renouvelable avec une procédure allégée
- est révocable à tout instant
- est décerné de manière paritaire et discrétionnaire (comité mixte membres et CA du CLUSIF)
- est décerné gratuitement la première année de fonctionnement du label

Principales propriétés du label (1/3)

Aide aux sociétés françaises pour mieux connaître et sélectionner des formations (lire formation+formateur+organisme) qui :

- satisfont à un standard établi par la profession réunissant à la fois offreurs et utilisateurs
- s'engagent en matière d'éthique
- se soumettent à un suivi régulier par la CLUSIF
 - elles sont d'actualité, notamment en matière de caractérisation des menaces
 - elles prennent en compte les évolutions rapides des problématiques de sécurité des SI et de l'information et les évolutions technologiques
 - elles maintiennent l'accès approprié à un niveau de connaissance adapté
 - utilisent une pédagogie moderne et adaptée

Principales propriétés du label (2/3)

Aide apportée aux organismes de formations et aux formateurs

- meilleure notoriété globale
- information sûre vers des sociétés cibles concernées
- accès facilité aux sociétés membres
- recommandations du comité de labellisation
- auto évaluation compétitive

Principales propriétés du label (3/3)

Le CLUSIF agit dans son rôle

- occupation d'un terrain légitime de l'intermédiation offreurs/utilisateurs et institutions diverses
- rôle d'aiguillon pour la diffusion des connaissances et la montée en compétences
- rôle de modérateur des initiatives de formation sécurité



Comment obtenir le label ?

Dossier de candidature

1. Fiche descriptive synthétique
2. Dossier de candidature formation (descriptif et support de cours)
3. Dossier de candidature formateur
CV, signature de la charte ou déclaration par le formateur
4. Dossier de candidature organisme
5. Toute pièce justificative à l'initiative du demandeur
6. Pour les demandes de renouvellement annuelles, dossier éventuellement allégé avec mise à jour au minimum du dossier 2. descriptif de la formation

Un label facilement identifiable





GT ISO2700x

M. Frédéric HUYNH (Ernst & Young)

Contexte

- Existence du Groupe depuis Mars 2002.
- Quinzaine de membres utilisateurs et offreurs.
- Échanges et travaux autour de l'interprétation et l'utilisation des normes ISO17799 et ISO2700x :
 - discussions sur les évolutions normatives en cours,
 - débats sur l'utilisation des normes,
 - points d'actualités,
 - production de documents CLUSIF :
 - ISO17799:2000 : Une présentation générale,
 - Une approche normative du Management de la Sécurité de l'Information : BS7799-2,
 - ISO17799:2005 : Une présentation générale,
 - Métriques pour un SMSI selon ISO27001.

ISO17799:2005 : Une présentation générale

- Présenter de manière objective le contenu de la norme, son intérêt et les différents usages possibles de la norme.
- Points forts :
 - Mise à jour suite à la publication de la nouvelle version de la norme
 - Recul et objectivité
 - Analyse et conseils sur les usages de la norme
 - Présentation des limites et des améliorations

Métriques pour un SMSI selon ISO27001 *(travaux en cours)*

- Proposer une méthodologie d'élaboration de métriques de sécurité dans le cadre d'un SMSI, illustrée par des exemples concrets selon les 133 mesures de sécurité normatives.
 - Intégration du concept de PDCA,
 - Travaux réalisés en tenant compte du projet de norme ISO27004 (Information Security Management Measurements).



Les virus informatiques

M. François PAGET (McAfee)

Les Virus Informatiques

En guise d'introduction

- Il s'agit d'une refonte complète d'un précédent document datant de janvier 1998.
- Le travail a débuté en janvier 2003. Notre groupe n'a jamais dépassé la dizaine de personnes ; nous avons souvent travaillé à 3 ou 4.
- 3 ans ont été nécessaires. La problématique de 2003 différait de celle de 1998. Entre 2003 et maintenant d'autres changements se sont imposés à nous :
 - 15000 virus (01/1998), puis 63000 (01/2003) et aujourd'hui plus de 200000 programmes malveillants.
 - La menace touche l'information et non plus seulement le système d'information.
 - Les auteurs ne sont plus les mêmes, la réponse se doit donc d'être différente.

Les Virus Informatiques

Objectifs et destinataires

- Derrière le terme générique de « virus informatiques » se cache de nombreux programmes malveillants. Le document dresse dans un premier temps une typologie complète des infections informatiques et des anti-virus. Viennent ensuite 3 aspects du phénomène rarement synthétisés dans un seul document :
 - L'organisation de la lutte anti-virale,
 - L'aspect juridique,
 - L'assurance contre les virus.
- Le document s'adresse aux responsables sécurité, aux directeurs des systèmes d'information et à leurs équipes. Il est aussi destiné à tous ceux qui ont des responsabilités dans le domaine de la sécurité de l'information.

Les Virus Informatiques

L'organisation de la lutte anti-virale

- A l'aide d'une vision concentrique des risques, le document décrit les divers moyens de prévention et de protection depuis le poste de travail jusqu'au périmètre externe à l'entreprise :
 - Le poste de travail et les ressources propres à l'utilisateur,
 - Les ressources partagées,
 - Les passerelles,
 - Le monde extérieur.
- L'homme se retrouve acteur et responsable à tous les niveaux.
- Conseils vis-à-vis des mises à jour et du paramétrage.

Les Virus Informatiques

L'aspect juridique

- Qu'il s'agisse de responsabilité civile ou de responsabilité pénale, les différents textes applicables sont expliqués et argumentés :
 - Code pénal,
 - Loi informatique et libertés,
 - Loi sur la protection du droit d'auteur,
 - Loi Godfrain,
 - Loi relative à la sécurité quotidienne,
 - Loi pour la sécurité intérieure,
 - Loi pour la confiance dans l'économie numérique,
 - Loi relative aux communications électroniques et aux services de communication audiovisuelle,
 - Intérêts fondamentaux de la nation,
 - Secrets de la correspondance.
- Regard sur l'international
 - Quelques points clés de la convention du Conseil de l'Europe sur la cybercriminalité.

Les Virus Informatiques

L'assurance contre les virus

Après avoir présenté les principes qui régissent l'assurance des biens de l'assuré, détaillé les critères de souscription, et le déroulement d'un appel en garantie, le document précise quelques tendances relatives à l'assurance des systèmes d'information contre la malveillance informatique et plus particulièrement les virus informatiques.



Espace Méthodes MEHARI V3

M. Jean-Louis ROULE



Espace méthodes : structure

- Animé par Jean-Philippe JOUAS
- Objectif : faire évoluer MEHARI
méthode d'analyse et de management des risques
- Organisé en 3 groupes de travail
 - Principes et Bases de connaissance MEHARI
 - Intégration de MEHARI (ex. SOX, ISO, Bâle 2)
 - Documentation (et marketing) de MEHARI

Mode de travail récursif par versions

Espace méthodes : historique

Activité continue avec un cycle de versions sur 2 à 3 ans

Rappel historique des versions Mehari :

V1, V2, V2.5 : de 1998 à 2003

V3 : novembre 2004 (CD-ROM Français seul)

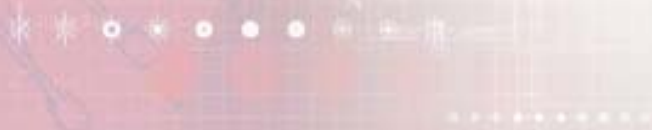
février 2006 : CD-ROM Français+Anglais

Vx (prochaine version) : objectif fin 2006

Espace méthodes : 2005-2006

Travail sur la version Vx :

- **Scoring ISO 17799:2005 suite à un chantier Mehari**
 - ⇒ **base d'audit des vulnérabilités affinée**
- **Position de Mehari vs. ISMS ISO 27001**
- **Documentation : mieux passer des enjeux aux risques**
- **etc.**



Espace méthodes : 2005-2006

Documentation en français : 2004 – début 2005

Traduction en anglais : mai – décembre 2005

CD-ROM bilingue : février 2006

Autres traductions : Allemand – Italien : 2006

Promotion :

Plaquettes : 2005 (Français et Anglais)

Bases de connaissance publiques (Fr+En)

Contacts réactivés avec le Québec

Nouveaux de contacts en Europe :

Autriche, Roumanie

Liaison avec universités (cours Mehari)

Espace méthodes : attentes, espoir

Développer plus de moyens au Clusif :

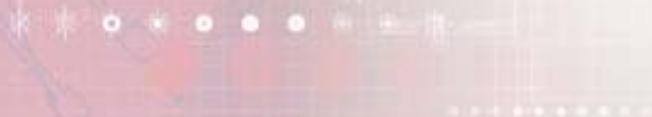
Plus de participants actifs : RSSI, consultants !!

Renforcer Marketing et communication

Maîtriser les Budgets (traductions, AFNOR?)

Créer Formations, présentations, argumentaires.

Améliorer le site du CLUSIF (Français & Anglais)





Enquête Politique de Sécurité et sinistralité informatique en France – Bilan de l'année 2005

M. Laurent BELLEFIN (Solucom)

GT Enquête Politique de Sécurité et sinistralité informatique en France 2005

Objectifs de l'enquête 2005

- Établir un **état des lieux** des politiques de sécurité et de la sinistralité informatique en France
- Déterminer les **tendances générales** en matière de sécurité de l'information

Démarche retenue

- Questionnaire basé sur les thèmes de l'ISO 17799:2005, avec un zoom sur les thèmes d'actualité
- Enquête confiée à un cabinet d'étude marketing spécialisé (GMV Conseil)

Rapport publié le 28 juin 2006, disponible sur le site du CLUSIF

Une enquête de référence basée sur un échantillon large et représentatif

Enquête téléphonique réalisée en février et mars 2006

Réalisée sur 3 cibles différentes

- Les entreprises de plus de 200 employés **400 entreprises**
- Les mairies des communes de plus de 30000 habitants **50 mairies**
- Les hôpitaux publics **186 hôpitaux**

Sur un échantillon statistiquement représentatif

Quelques résultats de l'enquête

- Une formalisation des politiques qui progresse
 - 56% des entreprises disposent d'une PSSI, 54 % d'une charte utilisateur
 - 41% des entreprises ont nommé un RSSI, qui est dédié à cette fonction dans 24% des entreprises
- Mais un investissement qui n'augmente que très progressivement
 - Le manque de budget reste le premier frein aux actions de sécurité pour 37% des entreprises
 - Seulement 38% des entreprises ont augmenté leur budget sécurité en 2005

Quelques résultats de l'enquête

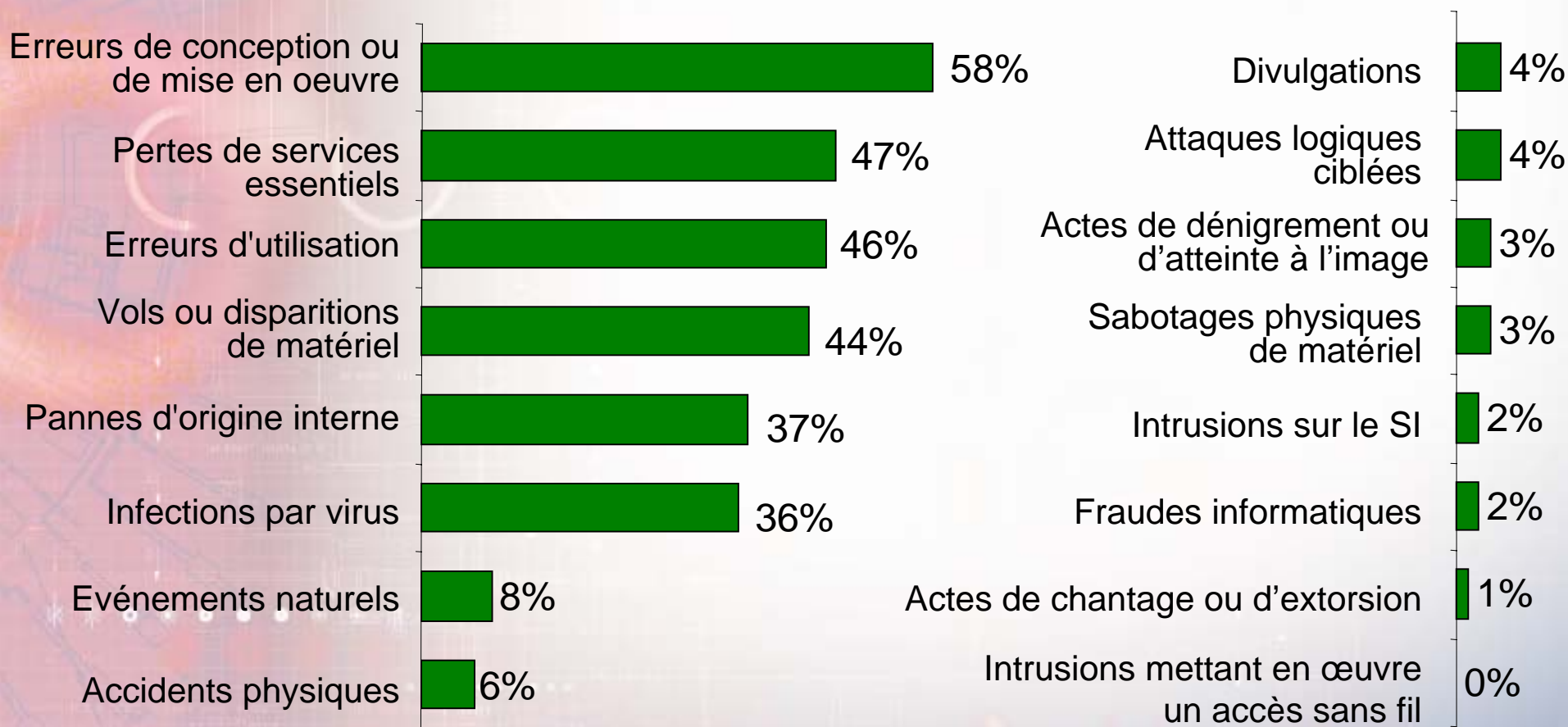
- Usage des nouvelles technologies : des politiques encore souvent restrictives
 - 56% des entreprises interdisent le Wifi, 43% interdisent les PDA
- Des nouvelles technologies de sécurité qui se diffusent lentement...
 - 66% des entreprises n'utilisent pas d'outil de chiffrement
 - 54% des entreprises n'utilisent pas encore de pare-feu personnel
- Technologie de gestion des identités et des accès : encore les balbutiements !

Quelques résultats de l'enquête

- Des processus opérationnels en progression
 - 76% des entreprises réalisent une veille partielle ou systématique
 - 57% ont formalisé le processus de déploiement de correctif
- Mais :
 - Les impacts des incidents ne sont pas mesurés dans 76% des entreprises
 - Seulement 20% des entreprises ont mis en place un tableau de bord sécurité
 - 42% des entreprises n'ont mis en place aucune mesure pour garantir la continuité d'activité

Vols, attaques ciblées, divulgations... une malveillance confirmée

% des entreprises ayant rencontré des incidents de type :



Conclusion : un constat mitigé !

Une prise de conscience qui s'améliore
(75% des entreprises estiment être très dépendantes de leur SI)

Mais des approches qui restent partielles, et des freins qui subsistent

Passer de l'artisanat à un vrai **systeme de management de la sécurité de l'information**, en s'appuyant sur les normes et les standards
→ La seule voie pour convaincre les décideurs



En 2006 / 2007

M. Pascal LOINTIER (ACE)

Et encore d'autres GT ou travaux en cours...

- Conception d'un centre informatique sécurisé
- Criminalistique
- Destruction et Récupération d'informations
- Fiches de sécurité pour la micro-informatique
- Gestion de crise
- Gestion des identités
- Malveillance téléphonique
- Panorama de la cybercriminalité
- Réseau privé virtuel (VPN)
- Spam
- Spyware

Espace RSSI, programme 2006-2007

- Sensibilisation à la sécurité
- Le réseau d'entreprise
- Les tests d'intrusion
- Problématique VoIP et ToIP
- La réglementation
- La gestion de crise
- La gestion des risques
- La gestion des identités
- La politique sécurité
- Le système de classification des informations
- Retour expérience MEO d'un ISMS (norme ISO 27001)
- La sécurité des mises à jour des systèmes et applications
- Le verrouillage des postes de travail

Contacts

<http://www.clusif.asso.fr/>

CLUSIF
30, rue Pierre SEMARD
75009 PARIS

clusif@clusif.asso.fr

01 53 25 08 80