Analisi dei rischio
e
Analisi dei impatti
sul
Business

Jean Paul Coppens

Thema-event
Congreshotel
Ter Elst, Edegem

13/10

ICT, het kloppende hart van uw bedrijf

KMO-IT centrum
Informatie Technologie voor KMO's

Risico Analyse
en
Business impact

Jean Paul Coppens

Microsoft ORACLE SAP AGORIA imec
KMO Trends Industrie BIZZ SMART BUSINESS kmo IWT TMAB echo

Thema-event
Congreshotel
Ter Elst, Edegem

13/10

ICT, het kloppende hart van uw bedrijf

KMO-IT centrum
Informatie Technologie voor KMO's

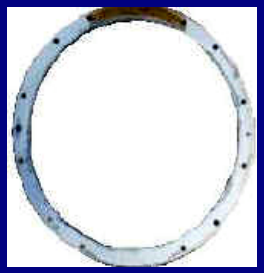
Risicoanalyse, meer vóórdenken, minder nadenken

« The thickness of the rampart is less important than the willingness to defend it »

(*) Thucydide, (5de eeuw B.C)

Microsoft ORACLE SAP AGORIA imec
KMO Trends Industrie BIZZ SMART BUSINESS STRATEGIES kmo iwt TMAB echo

Voorbeeld: Challenger - risico analysis



- The O ring case
- The risk analysis came up with a significant exposure and a high probability of occurrence.
- Conclusion was to send it back to R&D for re-engineering.

Component	Functie	Faalwijze	Effect	E	Oorzaak	O	Controle	D	RPN	Actie	Verantw.
O-ring	gasdicht afsluiten	lekken	Lekkage Brand	10	Trilling bij lage buitentemperatuur	5	prototype	4	200	terug ontwerp afdl	ontwerpafdeling

Voorbeeld: Challenger - Business

- Richard Feynman, the Nobel-prize-winning physicist on the investigating committee, quoted:.
- « Pressures on managers to get approval of the project from Congress and to attain a successful flight led them to down play the significance of negative engineering reports. »

Extracts of Warren report(1996)

Voorbeeld: Challenger – Impact on Business

1986

Space shuttle

Challenger

Business Impact

Het is niet zover van hier gebeurd mijn top 10 van ....juist te laat of bijna

- Agriphar Luik 2004

Risico analysis: definitie (s) - methodologie

- **What if ?**

R = T x I x B

- **Kinney**

R = G x B x W

- **UCB**

R = E x P x F

T=Toestand – situatie
B=Blootstelling
I=impact

W=Waarschijnlijkheid
B=Blootstelling mogelijk
G=Gevolg

E= eigenschappen Product
P= waarschijnlijkheid blootstelling
F =frequentie blootstelling

- Risk analysis: definitie (s) - methodologie

- FMEA: Analyse van de faalwijzen en de gevolgen

Rpn= S x P x D

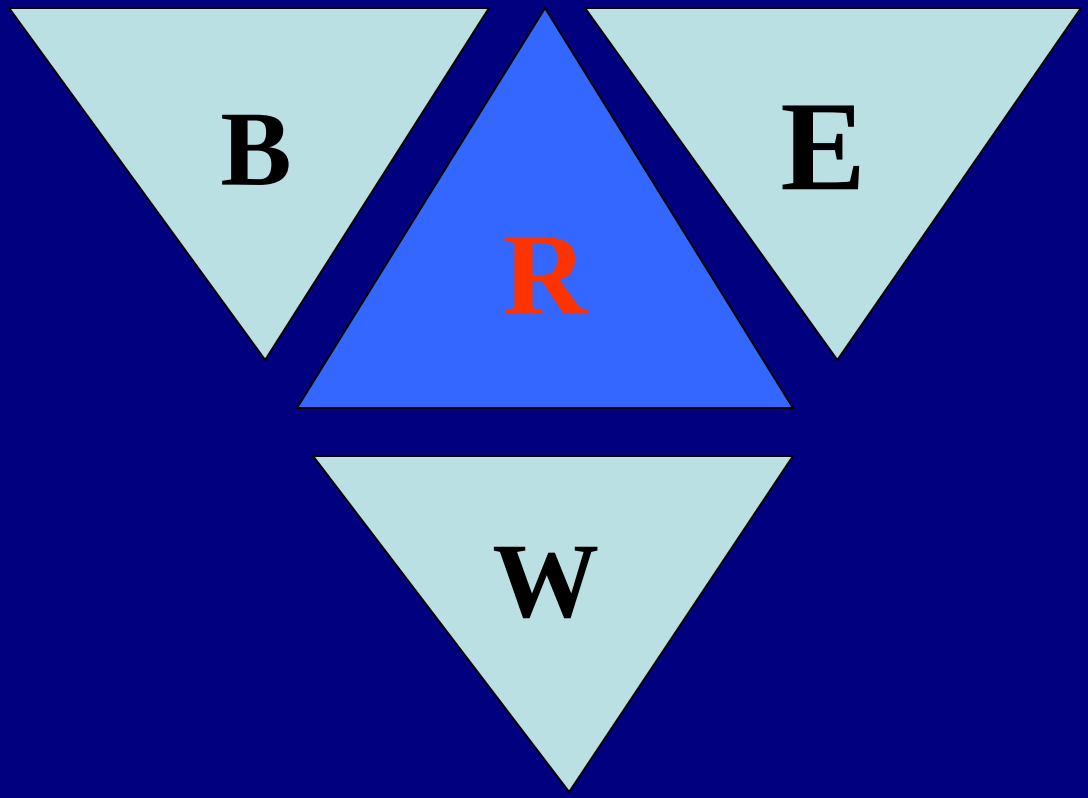
  - S = Ernst van gevolgen
  - P = Faalwijzen-waarschijnlijkheid bepalen
  - D = « Detectability » bepalen

FMEA methode

- Functies en componenten identificeren
- Mogelijke faalwijzen bepalen
- Mogelijke gevolgen beschrijven

- Ernst van gevolgen bepalen **(S**)
- Mogelijke oorzaken en faalwijzen beschrijven
- Faalwijzen-waarschijnlijkheid bepalen **(P)**
- Controle middelen beschrijven
- « Detectability » bepalen **(D**)

- Risk Priority Number berekenen **(RPN = S x P x D)**
- Leg acties vast voor de meest risicovolle faalwijzen (plan, verantwoordelijkheden, deadlines)



Risico factor = Blootstelling * Ernstigheid * Waarschijnlijkheid

Test : The « Zirconium plank S.A » verhuis

- Ons Bedrijf moet verhuizen
  - Men moet naar een niewe zoning .
  - Finaniceel goedkoper.
  - Met goede communicaties, en kort tegen Frankrijk gelegen.
  - Een plus: Kort gelegen tegen de woning van onze baas.
- Men heeft een aantrekelijk plaats gevonden, een *verloren land* in een dorp dat « GUY-Len Gu'yen », of iets gelijkaardigs, noemt.
- Laat ons een vlug R.A. doen, vandaag en B.V. in 1999, van onze keus:
  - Wat is uw risico factor ?
  - I= 1 -> 10
  - B= 1->10
  - W= 1-> 10

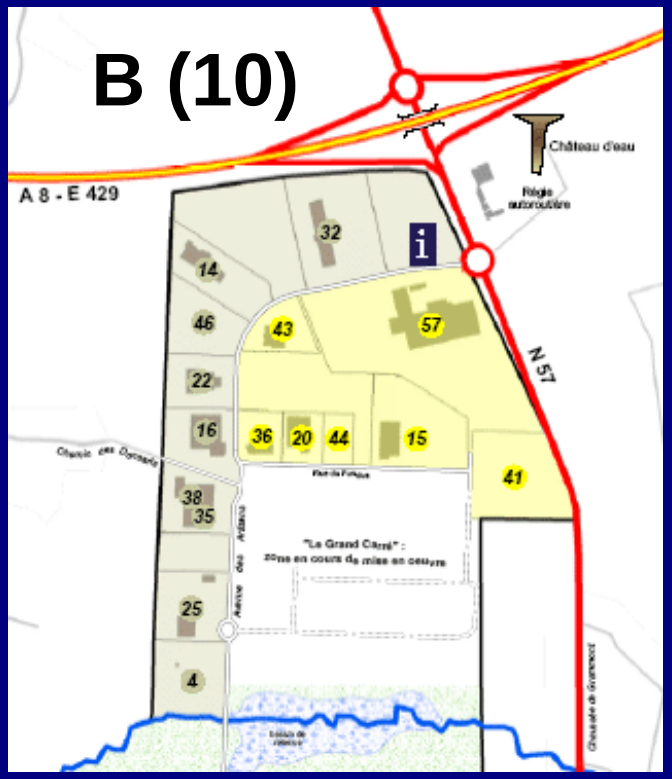
Thema-event
Congreshotel
Ter Elst, Edegem

13/10

ICT, het kloppende hart van uw bedrijf

KMO-IT centrum
Informatie Technologie voor KMO's

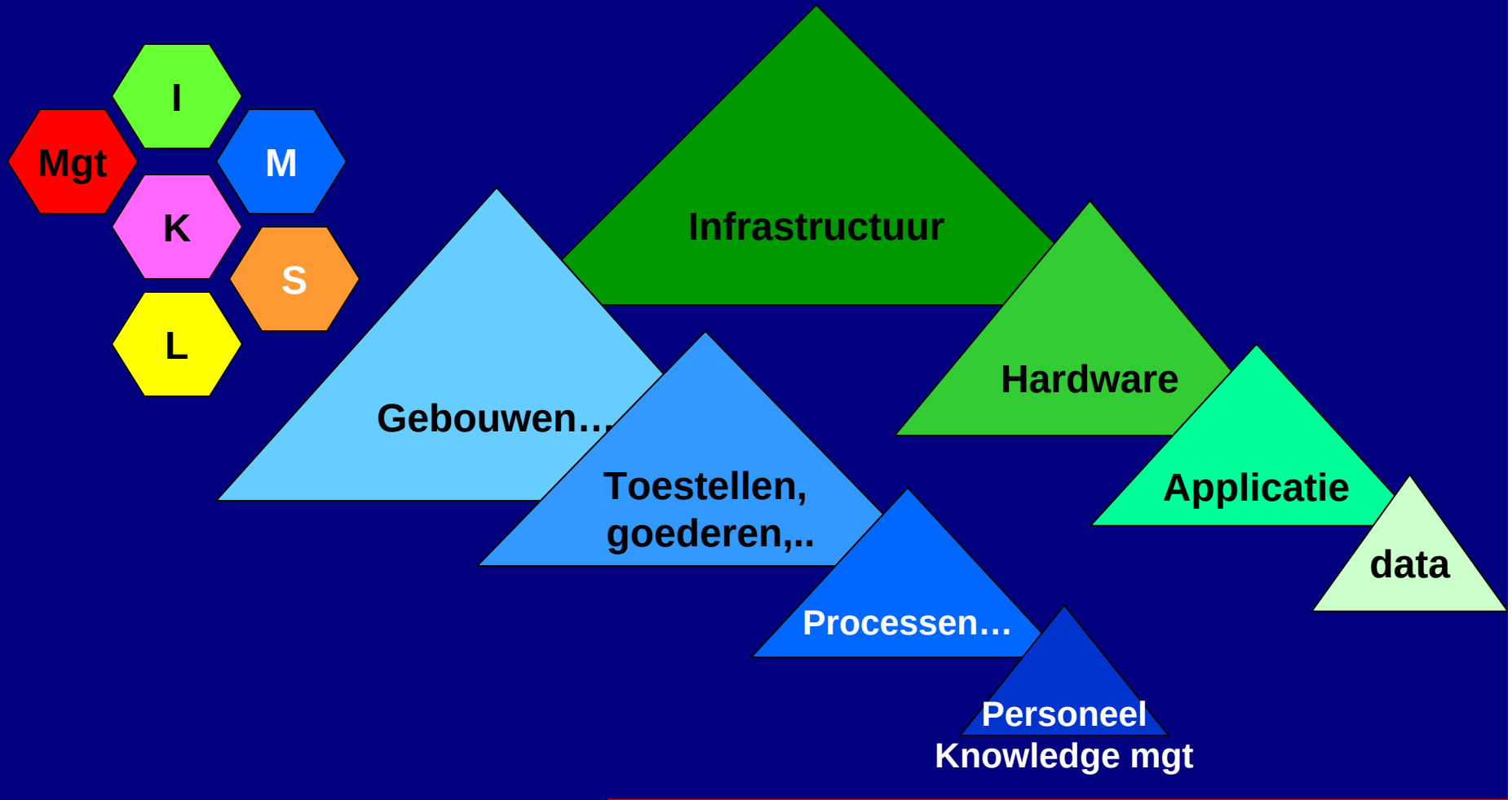
I(10)



Terug naar business continuity

Waar vindt men risico's voor business ?

Terug naar business continuity



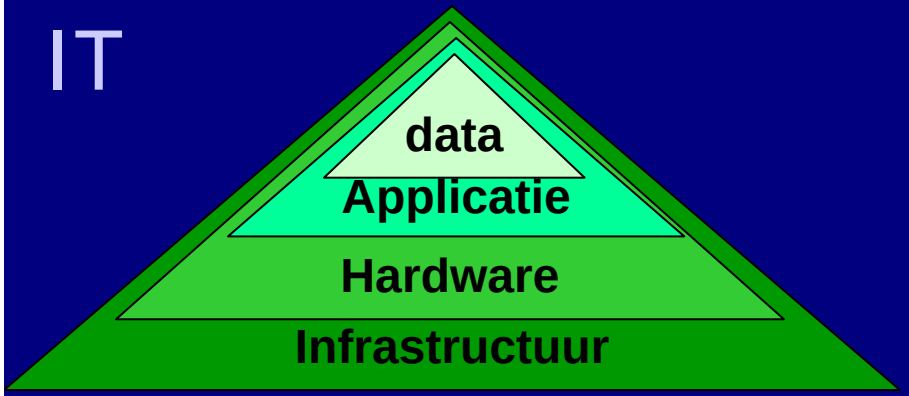
Thema-event
Congreshotel
Ter Elst, Edegem

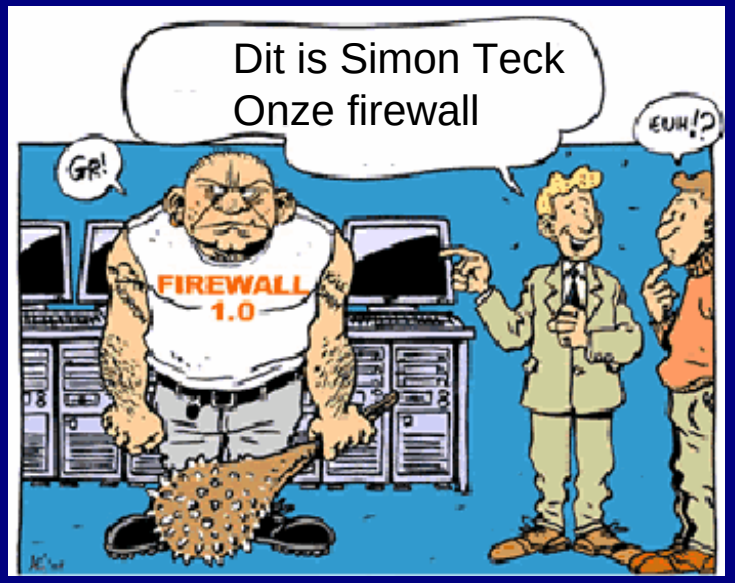
13/10

ICT, het kloppende hart van uw bedrijf

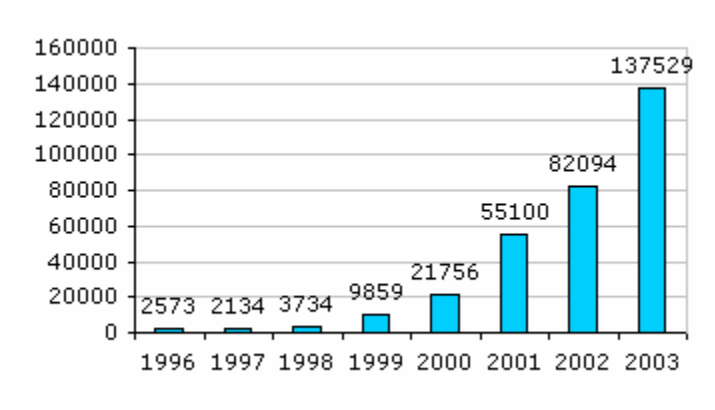
KMO-IT centrum
Informatie Technologie voor KMO's

IT

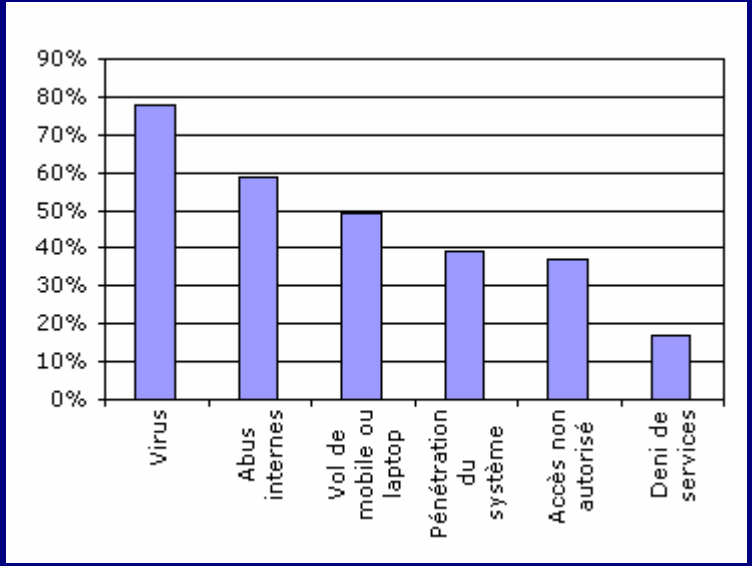




IS incidents

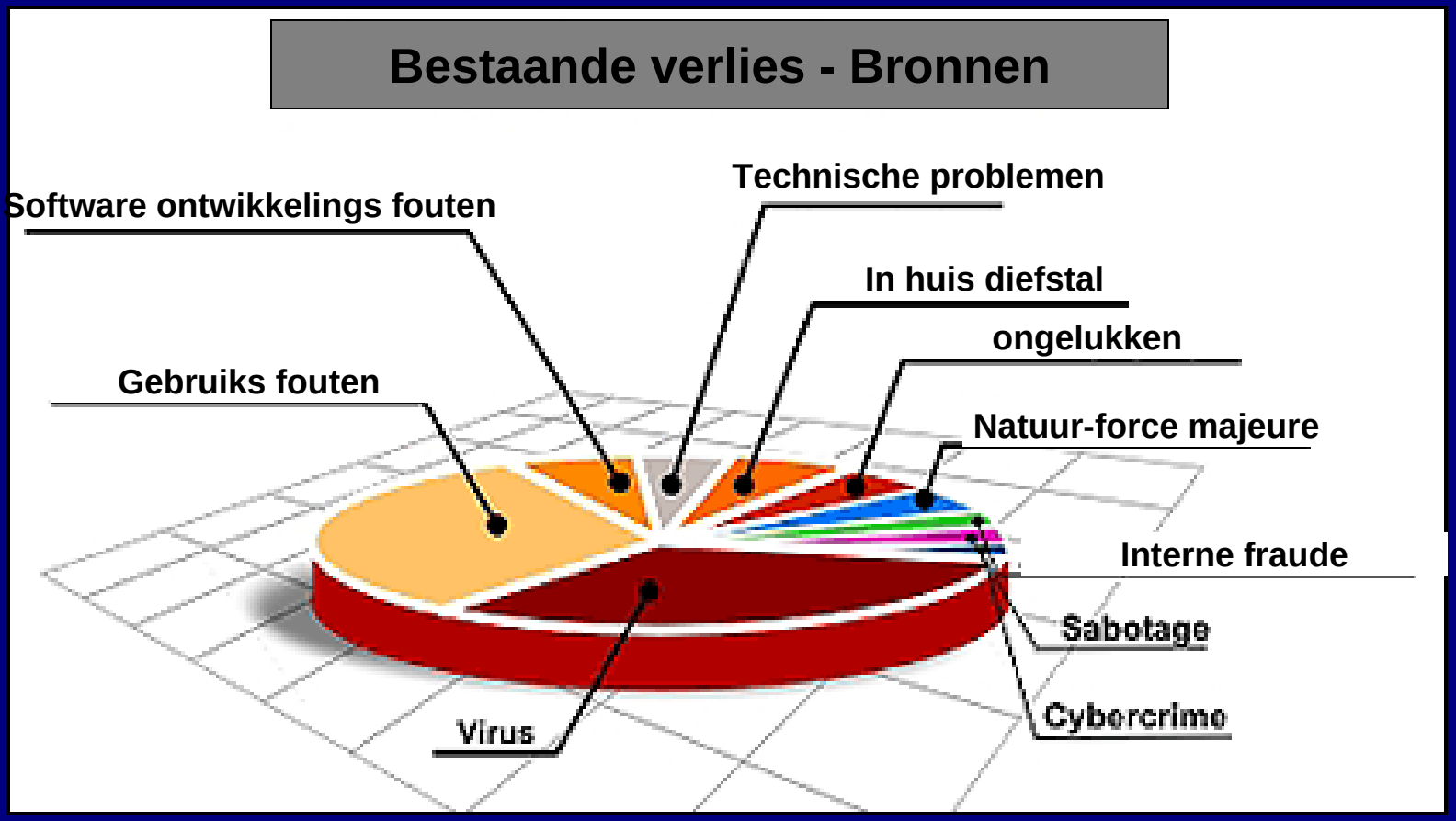


Source CERT http://www.cert.org



CSI/FBI 2004 Computer Crime and Security Survey Results (source: http://www.gocsi.com)

IT


Bestaande verlies - Bronnen
Software ontwikkelings fouten
Technische problemen
In huis diefstal
ongelukken
Gebruiks fouten
Natuur-force majeure
Interne fraude
Sabotage
Cybercrime
Virus

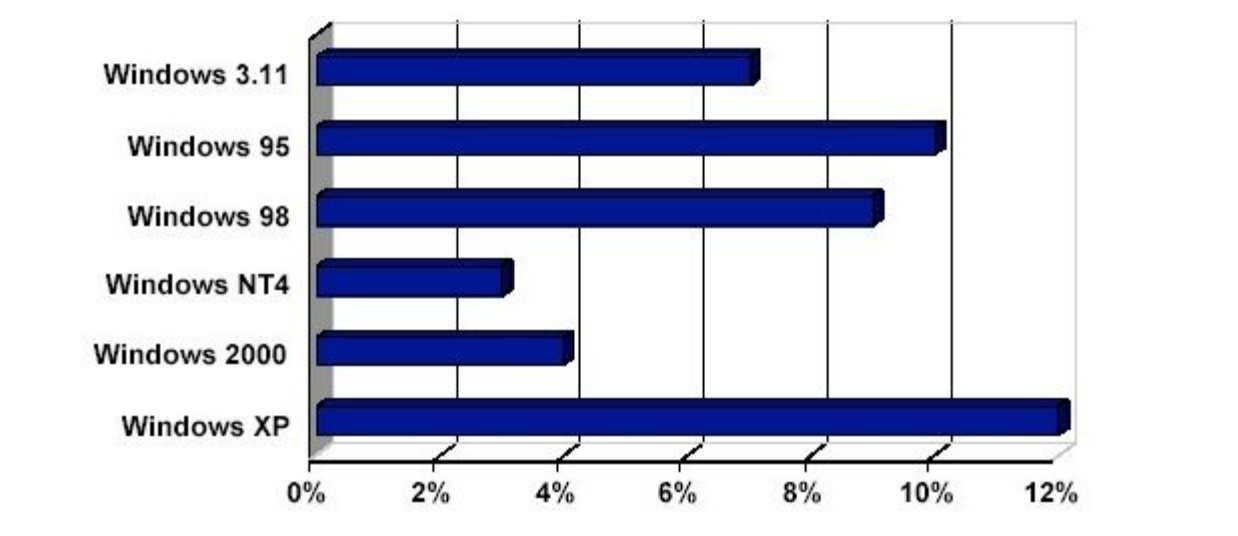
Microcost study – September 2004 – op 1.282.357 PC's over 7 landen in Europa

	Administratif	Industriel	Service	Général
Windows 3.11	750	0	0	750
Windows 95	151 141	44 002	9 616	204 758
Windows 98	175 380	13 204	172 839	361 423
Windows NT 4.0	6 901	26 809	123 646	157 355
Windows 2000	9 570	421 606	102 027	533 203
Windows XP	3 181	0	21 687	24 868
Nombre total	346 923	505 621	429 815	1 282 357

4 weken testing

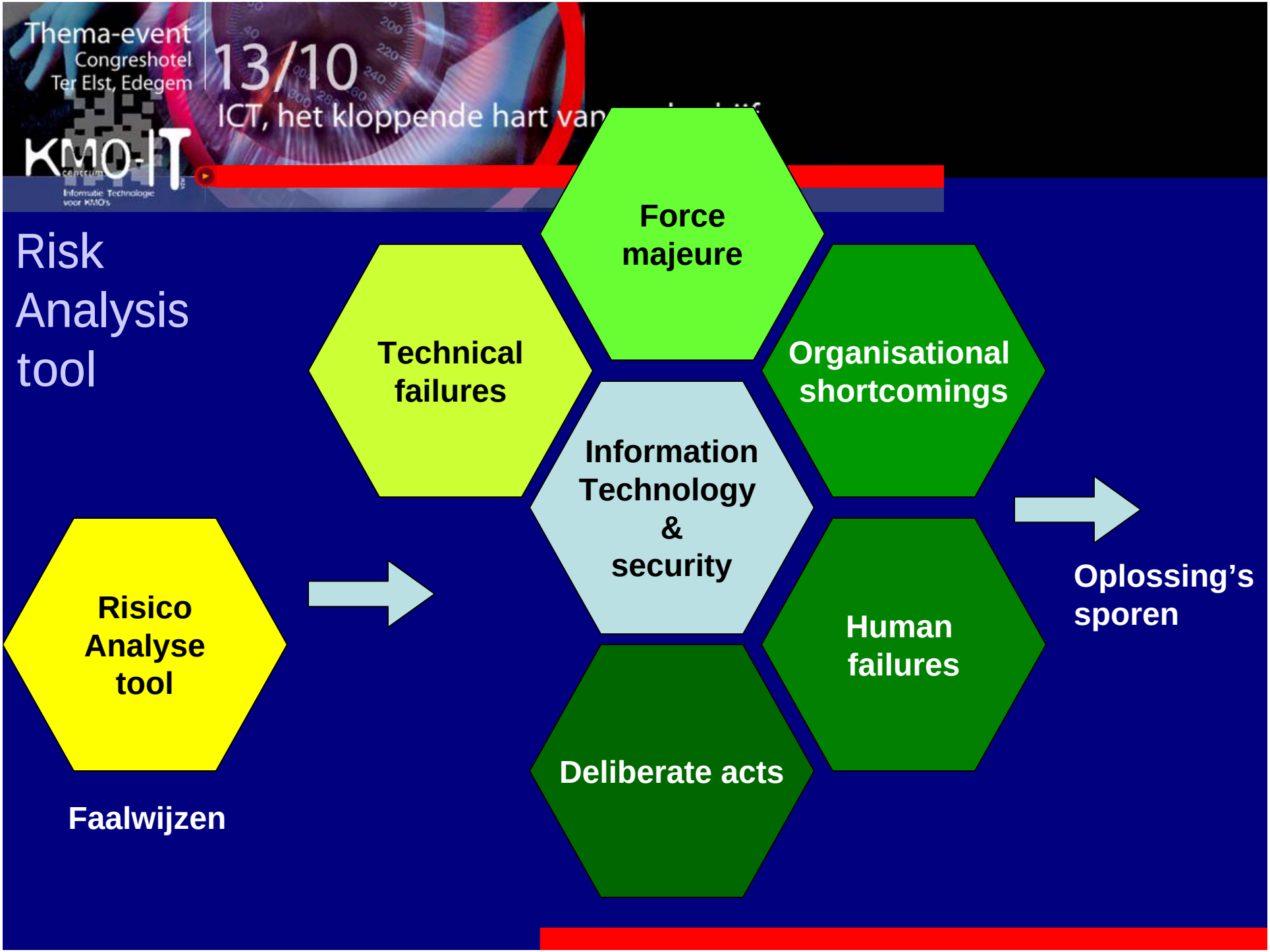
Source Microcost study – www.microcost.com

Microcost study – 2004 – op 1.282.357 PC's over Europa

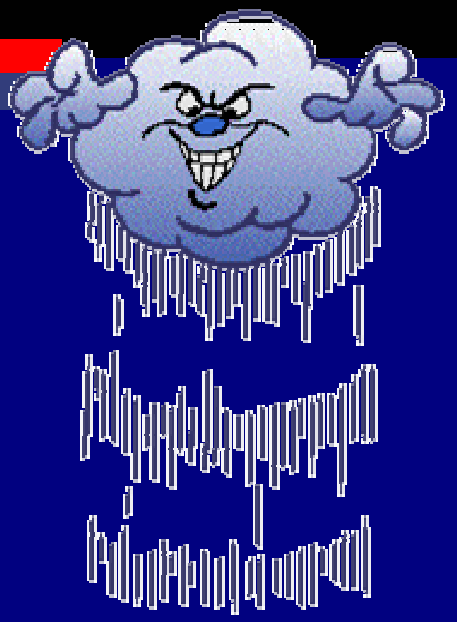


Graphic of incidents, per OS, during the testing period.
An incident is an event that stops operators normal activities or Requires a reset of machine.

Source Microcost study – www.microcost.com


Thema-event
Congreshotel
Ter Elst, Edegem
13/10
ICT, het kloppende hart van
KMO-IT centrum
Informatie Technologie voor KMO's
Risk Analysis tool
Force majeure
Technical failures
Organisational shortcomings
Information Technology & security
Human failures
Deliberate acts
Risico Analyse tool
Faalwijzen
Oplossing's sporen

Risico analyse 5 themas:



- Force majeure (14 areas):
- Lighting
- Storm
- Fire
- Light
- Magnetic fields
- ...

Risico analyse 5 themas:

- Organisation shortcomings(97 Areas):
  - » Rules en Procedures
  - » Uncontrolled use of ressources
  - » Security flaws
  - » Access security.
  - » Weaknesses in contracts (subcont.)
  - » Change & configuration mgt.
  - » ...

Risico analyse 5 themas:

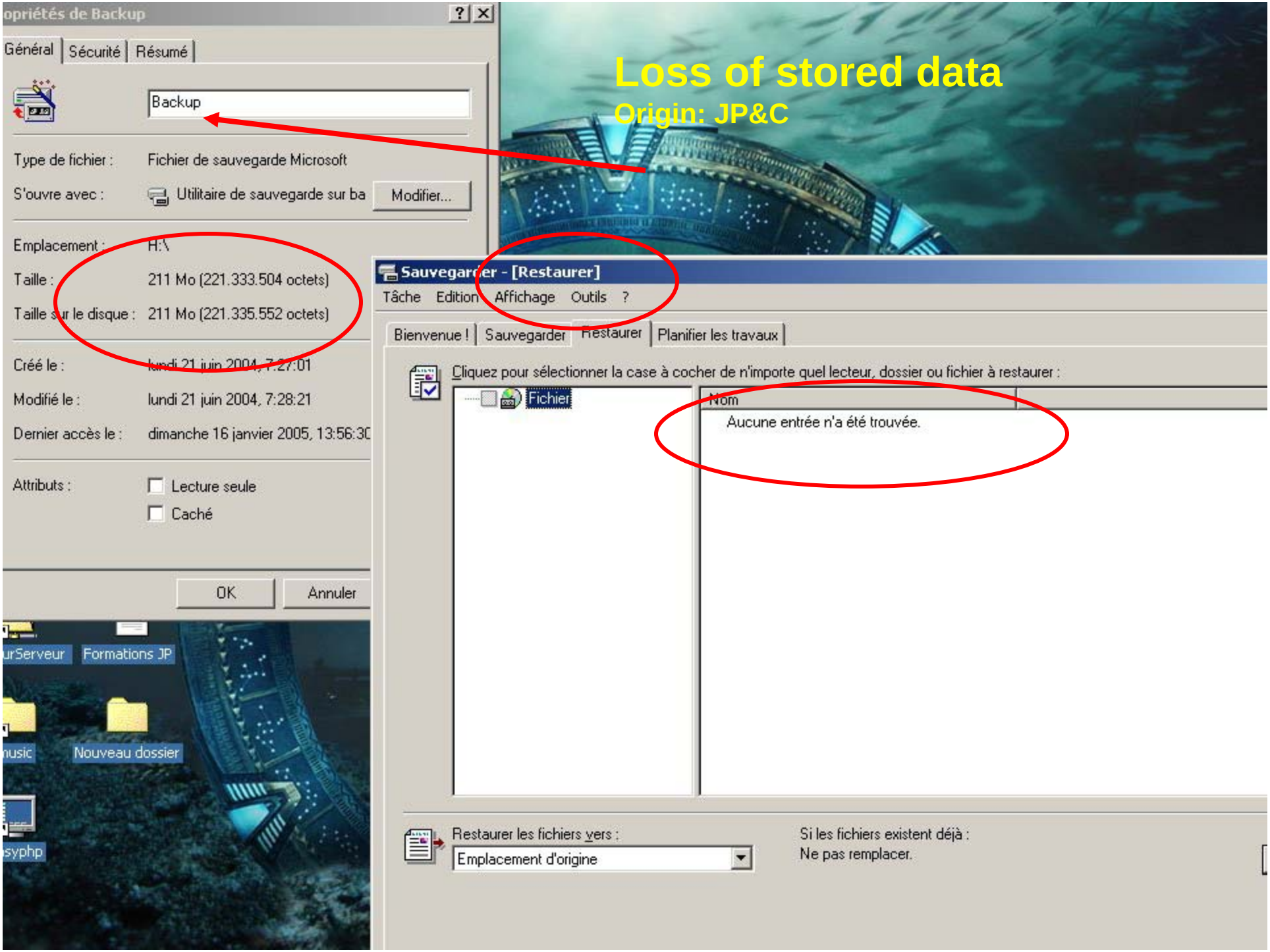
- Deliberate acts (111 areas):
  - » hacking
  - » sabotage
  - » Social engineering
  - » Access security.
  - » Misuse of vulnerabilities
  - » Line tapping
  - » Attacks
  - » ….

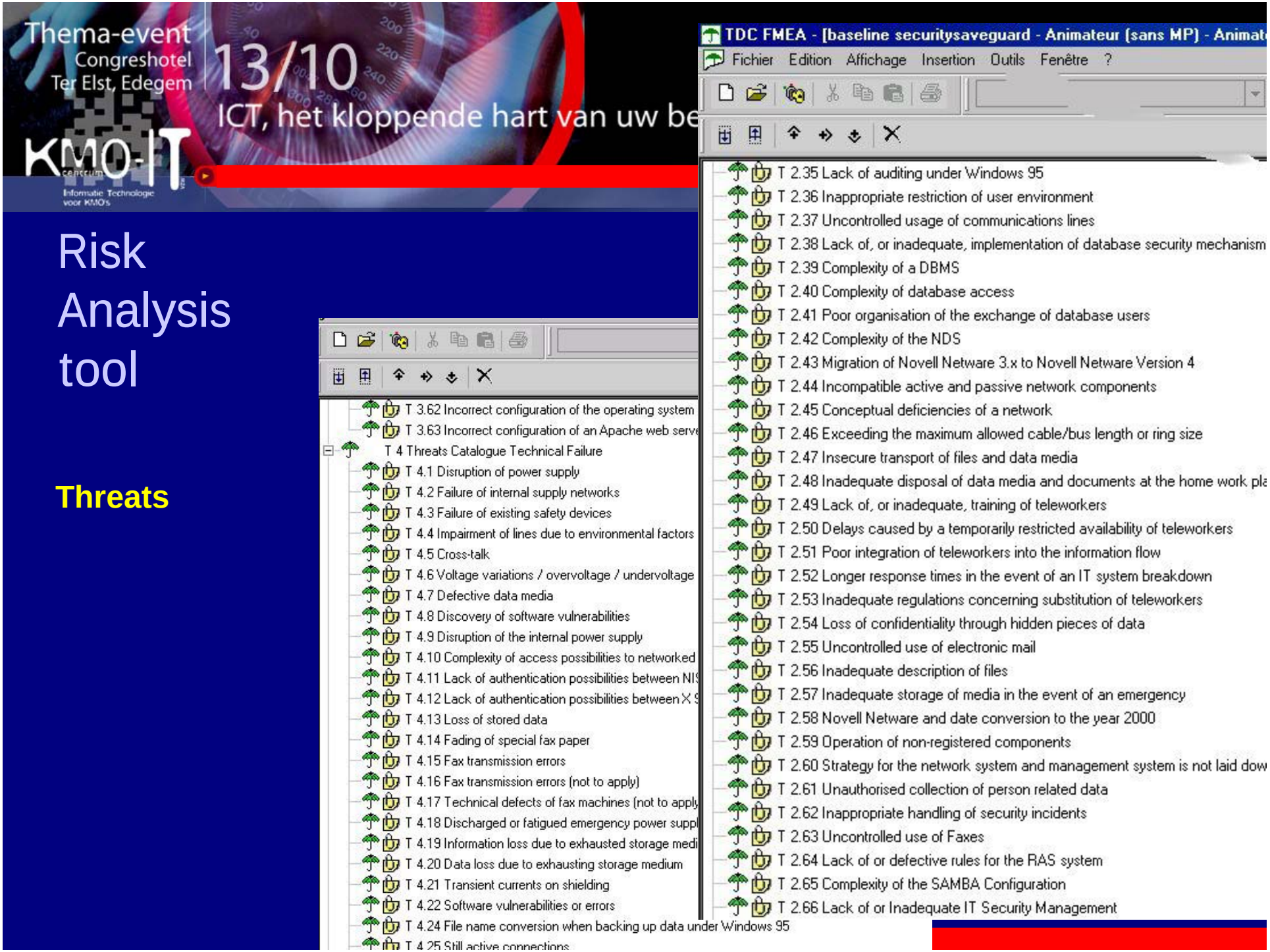
Risico analyse 5 themas:

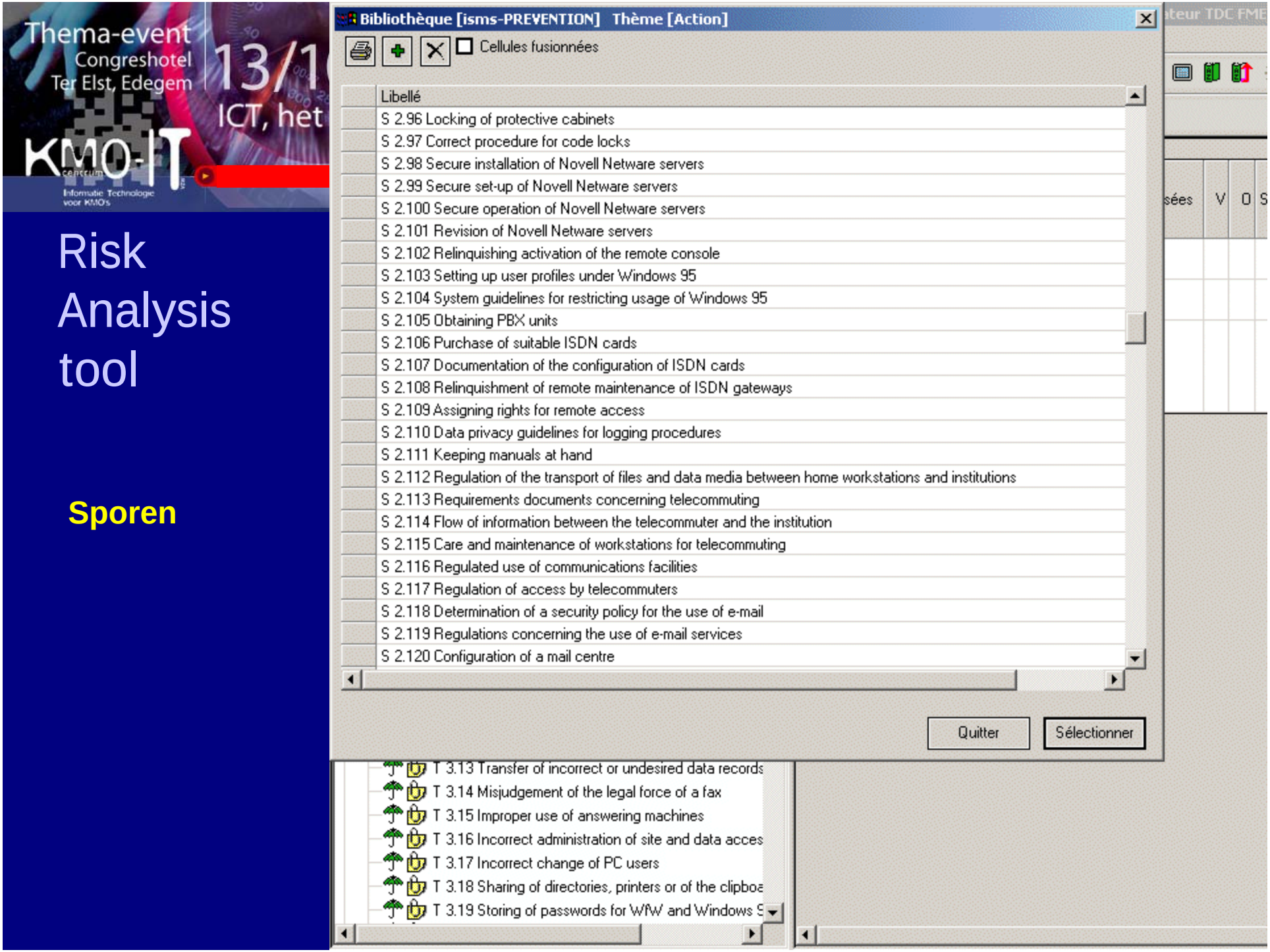
- Human failures (63 areas):
- Oups!...
- Negligent use of data or equip.
- Loss of data or media
- Hazards created by cleaning or externals
- Improper use of remote access
- ....

Risico analyse 5 themas:

- Technical failures (44 areas):
- Failure of safety devices
- Defective data media
- Loss of stored data
- Software conception errors
- Undocumented functions
- Databases corruption
- Exhausting storage media (size, age,...)
- ...


opriétés de Backup
Général
Sécurité
Résumé
Backup
Type de fichier :
Fichier de sauvegarde Microsoft
S'ouvre avec :
Utilitaire de sauvegarde sur ba
Modifier...
Emplacement :
H:\
Taille :
211 Mo (221.333.504 octets)
Taille sur le disque :
211 Mo (221.335.552 octets)
Créé le :
lundi 21 juin 2004, 7:27:01
Modifié le :
lundi 21 juin 2004, 7:28:21
Dernier accès le :
dimanche 16 janvier 2005, 13:56:30
Attributs :
Lecture seule
Caché
OK
Annuler
Loss of stored data
Origin: JP&C
Sauvegarder - [Restaurer]
Tâche
Edition
Affichage
Outils
?
Bienvenue !
Sauvegarder
Restaurer
Planifier les travaux
Cliquez pour sélectionner la case à cocher de n'importe quel lecteur, dossier ou fichier à restaurer :
Fichier
Nom
Aucune entrée n'a été trouvée.
Restaurer les fichiers vers :
Emplacement d'origine
Si les fichiers existent déjà :
Ne pas remplacer.
urServeur
Formations JP
Nouveau dossier


Thema-event
Congreshotel
Ter Elst, Edegem
13/10
ICT, het kloppende hart van uw be
KMO-IT centrum
Informatie Technologie voor KMO's
Risk Analysis tool
Threats
TDC FMEA - [baseline securitysaveguard - Animateur (sans MP) - Animat
Fichier Edition Affichage Insertion Outils Fenêtre ?
T 2.35 Lack of auditing under Windows 95
T 2.36 Inappropriate restriction of user environment
T 2.37 Uncontrolled usage of communications lines
T 2.38 Lack of, or inadequate, implementation of database security mechanism
T 2.39 Complexity of a DBMS
T 2.40 Complexity of database access
T 2.41 Poor organisation of the exchange of database users
T 2.42 Complexity of the NDS
T 2.43 Migration of Novell Netware 3.x to Novell Netware Version 4
T 2.44 Incompatible active and passive network components
T 2.45 Conceptual deficiencies of a network
T 2.46 Exceeding the maximum allowed cable/bus length or ring size
T 2.47 Insecure transport of files and data media
T 2.48 Inadequate disposal of data media and documents at the home work pla
T 2.49 Lack of, or inadequate, training of teleworkers
T 2.50 Delays caused by a temporarily restricted availability of teleworkers
T 2.51 Poor integration of teleworkers into the information flow
T 2.52 Longer response times in the event of an IT system breakdown
T 2.53 Inadequate regulations concerning substitution of teleworkers
T 2.54 Loss of confidentiality through hidden pieces of data
T 2.55 Uncontrolled use of electronic mail
T 2.56 Inadequate description of files
T 2.57 Inadequate storage of media in the event of an emergency
T 2.58 Novell Netware and date conversion to the year 2000
T 2.59 Operation of non-registered components
T 2.60 Strategy for the network system and management system is not laid dow
T 2.61 Unauthorised collection of person related data
T 2.62 Inappropriate handling of security incidents
T 2.63 Uncontrolled use of Faxes
T 2.64 Lack of or defective rules for the RAS system
T 2.65 Complexity of the SAMBA Configuration
T 2.66 Lack of or Inadequate IT Security Management
T 3.62 Incorrect configuration of the operating system
T 3.63 Incorrect configuration of an Apache web serve
T 4 Threats Catalogue Technical Failure
T 4.1 Disruption of power supply
T 4.2 Failure of internal supply networks
T 4.3 Failure of existing safety devices
T 4.4 Impairment of lines due to environmental factors
T 4.5 Cross-talk
T 4.6 Voltage variations / overvoltage / undervoltage
T 4.7 Defective data media
T 4.8 Discovery of software vulnerabilities
T 4.9 Disruption of the internal power supply
T 4.10 Complexity of access possibilities to networked
T 4.11 Lack of authentication possibilities between NI
T 4.12 Lack of authentication possibilities between X 9
T 4.13 Loss of stored data
T 4.14 Fading of special fax paper
T 4.15 Fax transmission errors
T 4.16 Fax transmission errors (not to apply)
T 4.17 Technical defects of fax machines (not to apply
T 4.18 Discharged or fatigued emergency power suppl
T 4.19 Information loss due to exhausted storage medi
T 4.20 Data loss due to exhausting storage medium
T 4.21 Transient currents on shielding
T 4.22 Software vulnerabilities or errors
T 4.24 File name conversion when backing up data under Windows 95
T 4.25 Still active connections


Thema-event
Congreshotel
Ter Elst, Edegem
13/1
ICT, het
KMO-IT centrum
Informatie Technologie voor KMO's
Risk Analysis tool
Sporen
Bibliothèque [isms-PREVENTION] Thème [Action]
Cellules fusionnées
Libellé
S 2.96 Locking of protective cabinets
S 2.97 Correct procedure for code locks
S 2.98 Secure installation of Novell Netware servers
S 2.99 Secure set-up of Novell Netware servers
S 2.100 Secure operation of Novell Netware servers
S 2.101 Revision of Novell Netware servers
S 2.102 Relinquishing activation of the remote console
S 2.103 Setting up user profiles under Windows 95
S 2.104 System guidelines for restricting usage of Windows 95
S 2.105 Obtaining PBX units
S 2.106 Purchase of suitable ISDN cards
S 2.107 Documentation of the configuration of ISDN cards
S 2.108 Relinquishment of remote maintenance of ISDN gateways
S 2.109 Assigning rights for remote access
S 2.110 Data privacy guidelines for logging procedures
S 2.111 Keeping manuals at hand
S 2.112 Regulation of the transport of files and data media between home workstations and institutions
S 2.113 Requirements documents concerning telecommuting
S 2.114 Flow of information between the telecommuter and the institution
S 2.115 Care and maintenance of workstations for telecommuting
S 2.116 Regulated use of communications facilities
S 2.117 Regulation of access by telecommuters
S 2.118 Determination of a security policy for the use of e-mail
S 2.119 Regulations concerning the use of e-mail services
S 2.120 Configuration of a mail centre
Quitter
Sélectionner
T 3.13 Transfer of incorrect or undesired data records
T 3.14 Misjudgement of the legal force of a fax
T 3.15 Improper use of answering machines
T 3.16 Incorrect administration of site and data acces
T 3.17 Incorrect change of PC users
T 3.18 Sharing of directories, printers or of the clipboa
T 3.19 Storing of passwords for WfW and Windows