

UNIVERSITE DE LAUSANNE

UNIVERSITE DE GENEVE

ECOLE DES HAUTES ETUDES COMMERCIALES

**LA VALEUR ECONOMIQUE
DE LA
SECURITE INFORMATIQUE**

MEMOIRE

Par

Fenna FELLRATH

DEA en Droit, Criminalité et Sécurité des Nouvelles Technologies 2003

1.	Avant-Propos	3
2.	Le Contexte	4
2.1	Introduction.....	4
2.2	Etat des lieux.....	5
3.	Méthodes et Techniques.....	10
3.1	Introduction.....	10
3.2	L'analyse des risques	10
3.3	L'approche mathématique	11
3.3.1	La première génération	11
3.3.2	La deuxième génération.....	12
3.3.3	Best Practices	13
3.3.4	La troisième génération.....	13
3.3.5	Conclusion	14
3.4	'Hummer'	15
3.5	'Hoover'	16
3.6	La loi du ROSI décroissant	16
3.7	Conclusion	17
4.	Les méthodes normatives et les standards.	19
4.1	Introduction.....	19
4.2	Cadre	19
4.3	ISO 17799	21
4.4	Gestion de la Qualité.....	23
4.5	La législation.....	25
4.5.1	Le droit pénal	25
4.5.2	Protection de la personnalité et protection des données	27
4.6	Le Marché	28
4.7	Conclusion	29
5.	La Pratique	30
5.1	Introduction.....	30
5.2	Shell	30
5.2.1	L'Analyse mathématique	31
5.2.2	La Stratégie	31
5.2.3	Le Déploiement.....	31
5.3	NUON.....	32
5.4	Conclusion	33
6.	Conclusion Générale	34
7.	Bibliographie.....	35
8.	Annexe A	37

1. Avant-Propos

La question relative à la mesure du rapport sur investissement (désigné après par '*Return On Security Investment*') des solutions de sécurité de systèmes d'information devient de plus en plus pertinente si on regarde les développements dans le monde, l'économie globale et l'informatique.

Nous proposons de faire un inventaire des événements et des développements qui ont fait des solutions de sécurité une nécessité, avant de traiter le 'ROSI' des solutions de sécurité des systèmes informatique et la nécessité d'une politique de sécurité. En pratique il s'avère très difficile d'utiliser le ROSI des solutions pour des systèmes intégrés, complexes et souvent dispersés à travers le monde. Dans ces cas les outils normatifs et qualitatifs jouent un rôle prépondérant. Ils sont plus adaptés au développement d'une stratégie de sécurité informatique. Une telle stratégie peut apporter une valeur économique à une entreprise qui dépasse largement le ROSI d'un outil particulier.

Le développement exponentiel de la législation et des régulations d'industrie obligent les entreprises à sécuriser leur environnement informatique et télécommunications. En effet, l'Internet, moyen important pour faciliter les contacts avec les partenaires, les clients et les fournisseurs, permet à s'ouvrir au marché global, mais une telle ouverture augmente les risques pour les systèmes informatiques et le fonctionnement des entreprises.

La nécessité commerciale d'une telle ouverture au marché global vis à vis le danger encouru avec les systèmes d'information et des télécommunications expose clairement la position des entreprises aujourd'hui. Ils ont le choix '*between a rock and a hard place*'!

Notre étude se termine par deux cas pratiques d'entreprises qui présentent une démarche et un état de sécurité assez différents et représentatifs de la situation actuelle.

2. Le Contexte

2.1 Introduction

Voici plus de 30 ans que Peter Drucker dans *'The Age of Discontinuity'*¹ a identifié quatre sources de discontinuité :

- l'explosion des nouvelles technologies
- la globalisation de l'économie
- la croissance du pluralisme
- la propagation de la connaissance.

Mai 1968, la crise pétrolière des années '70, le trou dans l'ozone, l'activisme environnemental (Greenpeace), furent les premiers signes de changement et de discontinuité de l'ère de l'après-guerre. Couplé à l'évolution de l'informatique et plus tard de l'Internet, ces évènements sont à l'origine de la globalisation, marquant un changement de notre société.

Les problèmes informatiques engendrés par le passage à l'an 2000 ont été à leur temps un signal d'alarme, personne n'avait vraiment une idée précise de l'amplitude du danger, dont les conséquences ont été relativement bien maîtrisés.

La conscience sécuritaire fut réellement éveillée par les évènements du 11 septembre 2001 à New York. Les attaques n'ont pas seulement détruit les 'Twin Towers', poumon économique de New York, en faisant des milliers de victimes, mais elles ont stoppé la plus grande économie mondiale pendant un certain laps de temps, et ont eu pour résultat une récession économique globale suivi d'une restructuration complète de l'industrie, où même les entreprises non impliquées dans l'attentat ont perdu des parts de marché ou ont vu leur valeur diminuer.² L'interdépendance des infrastructures et l'interconnectivité globale s'est manifestée d'une façon dramatique à cette occasion.

Kevin J. Soo Hoo dans son 'Working paper 'How much is enough? A Risk-Management Approach to Computer Security' de juin 2000 mettait déjà en garde contre une telle catastrophe :

¹ Peter F. Drucker, *The Age of Discontinuity : Guidelines to our Changing Society* (Harper & Row 1969)

² Ralph W. Shrader, Mike Mc Connell, Booz Allen Hamilton, *Security and Strategy in the Age of Discontinuity* (Strategy and Business Issue 26).

*'...the need to ascertain a more accurate quantitative picture of the country's infrastructure security posture, potential vulnerability to computer-related attacks, and overall risk is of pivotal importance not only to security resource allocation decisions but to the stability of an infrastructure that plays a large and growing role in the economy and society.'*³

La très forte augmentation des attaques des systèmes informatiques ainsi que leur rapide prolifération demande une vigilance toujours plus conséquente au niveau des entreprises. Les malveillances internes sont également en recrudescence et comptent, selon certaines recherches, pour 75% des attaques vécues maintenant.⁴

2.2 Etat des lieux

Tous ces faits posent un problème de sécurité pour les entreprises dans un climat économique difficile. Pour survivre il faut créer un système de sécurité basé sur trois principes primaires qui sont par nature interdépendant, soit

- sécuriser les employés
- protéger les opérations critiques de l'entreprise pour en assurer la continuité
- sécuriser les réseaux

Le but est de mettre en œuvre une sécurité stratégique globale: «une sécurité achevée dans un environnement ouvert intégrée dans le contexte d'une stratégie de l'entreprise visant croissance et profit. »⁵

C'est l'état idéal qui est décrit et qui demande une adaptation ainsi qu'une évolution continue prenant en compte l'ensemble des trois principes. Aujourd'hui, cet objectif ressemble encore trop à un vœu pieu.

Le «*Global Information Security Survey 2002* » de Ernst & Young donne un bon aperçu des problèmes de sécurité dans les entreprises. Ces données sont source d'inquiétude. Les principaux problèmes sont les suivants:

- Seulement 40 % des entreprises pensent être capable de détecter une attaque;
- 40 % des entreprises n'analysent pas les accidents de sécurité informatique;
- 75% des entreprises ont été pénalisées par des interruptions de systèmes imprévues;

³ How much is enough? A Risk-Management Approach to Computer Security, Kevin J.Soo Hoo, CRISP June 2000, page 68.

⁴ Ernst & Young, Global Information Security Survey 2002.

⁵ Ralph W. Shrader, Mike Mc Connell, Booz Allen Hamilton, Security and Strategy in the Age of Discontinuity (Strategy and Business Issue 26).

- Seulement 53% des entreprises possèdent des procédures pour garantir la continuité des services;
- Seulement 41% des entreprises s'inquiètent des attaques internes;
- Moins de 50% des entreprises ont des programmes de sensibilisation et de formation axées sur la sécurité.

Les décisions sécuritaires des systèmes informatiques et télécommunications devraient être coordonnées avec la stratégie de l'entreprises surtout parce que l'informatique est devenue critique et stratégique pour le fonctionnement de l'entreprise. Pourtant dans 45% des entreprises la responsabilité pour la continuité de l'entreprise pèse sur l'informatique plutôt que sur les « *business units* ». Ainsi un fossé psychologique est créé: la sécurité est de la responsabilité de l'informatique: 'on y est pour rien'.

L'enquête montre que la plus grande activité de l'investissement sécuritaire se trouve dans les domaines de la sécurité dite minimale: les anti-virus, le management de l'accès et les pare-feux. Avec des utilisateurs insuffisamment formés, des procédures de gestion non optimales, l'implémentation de ces outils risque de ne pas être très efficace.

Comme l'analyse des attaques ne se fait pas dans 40% des cas, les entreprises risquent d'avoir des dommages latents ainsi que des modifications non voulues de leur sécurité (ouvertures de ports pour un usage ultérieur, etc...). Seulement 40% ont admis avoir subi une attaque de réseau, Internet ou données.

Selon certaines études, environ 75% des attaques sont d'origine internes à l'entreprise alors que seules 41% des entreprises entreprennent des mesures adéquates.

Seulement un tiers des entreprises se sentent très concernées par l'observation des régulations de l'industrie et de la législation. Ceci, malgré l'attention croissante pour la protection de la sphère privée et des données de la part des législateurs.

Les interruptions de fonctionnement de l'entreprise citées dans l'enquête sont causés dans 56% des cas par des problèmes du matériel et de logiciels et dans 49% des cas par les moyens de télécommunication.

L'étude française de Clusif ⁶ démontre en gros les mêmes failles dans la sécurité informatique.

⁶ Etude et statistiques sur la sinistralité informatique en France, Club de la Sécurité des Systèmes d'Information Français, Année 2002.

*‘Si les moyens humains, organisationnels, techniques, sont globalement en augmentation, la conception et la mise en place d’une stratégie globale de sécurité restent encore trop marginales. A l’heure d’une ouverture marquante des systèmes et d’une dépendance forte, la prise de conscience des risques liés est insuffisante.’*⁷

L’étude démontre *‘que la stabilité des moyens mis en œuvre pour la sécurité logique mise en parallèle avec l’ouverture marquante des systèmes d’information montre le caractère insuffisant du développement des politiques de sécurité et d’outils idoines.’*⁷

Il est intéressant de noter que cette étude a révélé une taille critique pour une politique de sécurité. A partir de 200 salariés 68% des entreprises ont défini une telle politique et à partir de plus de 500 salariés 85% !⁸

La mise en œuvre de plans de secours et de plans de réactions pour garantir la continuité de l’activité est en place chez environ un tiers des répondants. Ce qui est inférieur aux 53% présentés dans l’étude de Ernst & Young .⁹

Aujourd’hui, la sécurité et la protection de la sphère privée sont perçues comme les obstacles les plus importants pour l’évolution de la connectivité. Pourtant, la connectivité et la sécurité sont des conditions sine qua non pour survivre dans cette économie globalisée. Dans le marché mondial un certain niveau de sécurité devient un avantage concurrentiel, voire une ‘condition sine qua non’ juridique¹⁰ ou de l’établissement de la confiance¹¹ dans et pour les relations avec les partenaires et les clients.¹²

Le ‘CSI/FBI Computer Crime and Security Survey 2003’¹³ démontre la fréquence et le coût de cybercriminalité aux Etats-Unis. Les répondants sont surtout des professionnels en sécurité ce qui donne un éclairage plus profond des problèmes de sécurité que les autres deux études où l’accent est mis plutôt sur la dimension économique pour l’entreprise. C’est une étude annuelle qui se réalise déjà depuis huit ans. Cela a l’avantage de pouvoir décerner des tendances et développements. Ce qui frappe cette année, c’est que le total des pertes rapportées a diminué de 56% comparé à l’an 2002. Ce qui correspond assez bien avec le chiffre de 2001 et avant. Les données importantes de cette étude montrent que comme précédemment, le vol d’information

⁷ Idem 6, page 19.

⁸ Idem 6, page 15.

⁹ Idem 6, page 18.

¹⁰ Cf. Health Insurance Portability and Accountability Act

¹¹ Nick Mansfield, The future of information security: eBusiness Assurance powerpoint presentation

¹² Informationweek.com ‘Retailers report Sale bounce using Security Certificate. URL:

<http://www.informationweek.com/story/showArticle.jhtml?articleID=8800552>

¹³ Eighth Annual CSI/FBI Computer Crime and Security Survey, Computer Security Institute 2003.

propriétaire est à l'origine de la plus grande perte financière ; le crime qui coûte le plus cher aux entreprises étant le déni de service. La perte causée par la fraude financière a beaucoup diminué. Les attaques les plus fréquentes sont causées par les virus et les abus internes. Les répondants ne sont en général pas favorables à l'engagement de personnes déjà condamnés pour faute de piratage d'informatique dite des 'hackers' reformés. Les incidents rapportés à la police ou autre institut judiciaire restent minoritaire (30%). Généralement, ils ne sont pas rapportés par peur d'une publicité négative résultant d'un tel rapport, et de l'avantage compétitif qui pourrait en découler pour les concurrents. Une grande partie des entreprises choisissent une solution civile plutôt que pénale.

Les sources d'attaque sont surtout les 'hackers' et les employés malveillants, mais on voit aussi un pourcentage important d'espionnage industriel par des concurrents et des pays étrangers. Le taux de détection des attaques montre que même les spécialistes ont souvent du mal à les découvrir. Les coûts de la cybercriminalité sont donnés dans le tableau suivant. Ces chiffres même approximatifs, sont utiles pour pouvoir calculer un retour sur investissement pour les solutions de sécurité informatique mais aussi pour donner une estimation de la valeur économique de la sécurité informatique.

The Cost of Computer Crime

The following table shows the aggregate cost of computer crimes and security breaches over a 48-month period

In 2003, 75% of our survey respondents acknowledged financial losses, but only 47% could quantify the losses.

How Money Was Lost

	Lowest Reported				Highest Reported				Average Losses				Total Annual Losses			
	00	01	02	03	00	01	02	03	00	01	02	03	00	01	02	03
Theft of proprietary info.	\$1K	\$100	\$1K	\$2K	\$25M	\$50M	\$50M	\$35M	\$3,032,818	\$4,447,900	\$6,571,000	\$2,699,842	\$66,708,000	\$151,230,100	\$170,827,000	70,195,900
Sabotage of data of networks	1K	100	1K	500	15M	3M	10M	2M	969,577	199,350	541,000	214,521	27,148,000	5,183,100	15,134,000	5,148,500
Telecom eavesdropping	200	1K	5K	1K	500K	500K	5M	50K	66,080	55,375	1,205,000	15,200	991,200	886,000	346,000	76,000
System penetration by outsider	1K	100	1K	100	5M	10M	5M	1M	244,965	453,967	226,000	56,212	7,104,000	19,066,600	13,055,000	2,754,400
Insider abuse of Net access	240	100	1K	100	15M	10M	10M	6M	307,524	357,160	536,000	135,255	27,984,740	35,001,650	50,099,000	11,767,200
Financial fraud	500	500	1K	1K	21M	40M	50M	4M	1,646,941	4,420,738	4,632,000	328,594	55,996,000	92,935,500	115,753,000	10,186,400
Denial of service	1K	100	1K	500	5M	2M	50M	60M	108,717	122,389	297,000	1,427,028	8,247,500	4,283,600	18,370,500	65,643,300
Virus	100	100	1K	40	10M	20M	9M	6M	180,092	243,835	283,000	199,871	29,171,700	45,288,150	49,979,000	27,382,340
Unauthorized insider access	1K	1K	2K	100	20M	5M	1.5M	100K	1,124,725	275,636	300,000	31,254	22,554,500	6,064,000	4,503,000	406,300
Telecom fraud	1K	500	1K	100	3M	8M	100K	150K	212,000	502,278	22,000	50,107	4,028,000	9,041,000	6,015,000	701,500
Active wiretapping	5M	0	0	5K	5M	0	0	700K	5M	0	0	352,500	5,000,000	0	0	705,000
Laptop theft	500	1K	1K	2400	1.2M	2M	5M	2M	58,794	61,881	89,000	47,107	10,404,300	8,849,000	11,766,500	6,830,500
Total Annual Losses												265,337,990	377,828,700	455,848,000	201,797,340	

CSI/ FBI 2003 Computer Crime and Security Survey
Source: Computer Security Institute

Les trois études citées montrent au niveau global, Français et Américain, l'état des lieux concernant l'implantation des outils et des politiques de sécurité. Il y a encore des grandes lacunes très importantes causées en très grande partie par ignorance et naïveté et par le fait que les formes et variations de la criminalité se développent tellement vite qu'il est difficile de les suivre avec des parades efficaces.

Pour ne donner qu'un petit exemple récent : Mardi 19 août 2003 le ver '*Blaster*' infiltre les systèmes Microsoft en utilisant une faille de Windows, vendredi 22 août 2003 le ver '*Sobig*' utilise des ordinateurs personnels pour engorger le réseau Internet. Ces attaques font des victimes partout dans le monde et causent surtout des problèmes au niveau de la sécurité des données personnelles qui pourraient être transmises après que le ver se soit infiltré. Les coûts engendrés sont surtout relatifs au temps nécessaire lié à vérifier les dégâts et remettre en ordre les systèmes. L'auteur de '*Sobig*' avait ouvert un compte chez un fournisseur d'accès Internet avec une carte de crédit volée, sept minutes avant de lancer le ver! On s'aperçoit que la criminalité sur Internet devient très sophistiquée et les auteurs courent relativement peu de risque d'être appréhendés.

Dans ce contexte le problème central est de pouvoir se procurer une défense, et mettre en place un système de sécurité. Quel en est alors le coût et qu'est-ce qu'un tel système peut apporter à l'organisation qui le met en œuvre? Pour chaque entreprise il s'agit d'une question primordiale compte tenu du contexte économique difficile dans lequel elle évolue. Une vue plus large s'impose sur la valeur économique d'une politique de sécurité qui, en tant que telle, peut avoir un impact bien plus bénéfique que le rapport sur investissement des outils de sécurité.

3. Méthodes et Techniques

3.1 Introduction

Afin d'appréhender les méthodes et techniques pour calculer le retour sur investissement des outils de sécurité, il faut établir un cadre de travail. La littérature distingue les approches mathématiques quantitatives et les méthodes normatives qualitatives. L'approche mathématique est plus adaptée au calcul du retour sur investissement des outils de sécurité, tandis que les méthodes normatives qualitatives s'adressent plutôt à la politique de sécurité à adopter par les entreprises. Aux Etats-Unis la demande pour une approche mathématique 'sûre' me semble plus élevée qu'en Europe où les méthodes qualitatives jouissent d'une certaine popularité. On peut constater en 'surfant' sur le Net que le retour sur investissement (*Return On Investment*) est utilisé par tous les développeurs de logiciel comme outil de vente. Nous verrons ensuite qu'en effet, le ROI d'un produit n'est pas trop difficile à calculer. Alors qu'assurer l'intégrité d'un environnement informatique sécurisé est plus difficile à réaliser.

3.2 L'analyse des risques

L'analyse des risques est une partie majeure des deux approches. Une analyse des risques comprend l'identification et évaluation des valeurs, l'évaluation des niveaux de menaces contre celles-ci, les impacts et les vulnérabilités de biens et valeurs.¹⁴

La gestion du risque connaît trois étapes:

- l'identification du risque et la probabilité d'occurrence;
- puis la hiérarchisation: l'établissement de la criticité (fréquence x gravité);
- et dernièrement la protection : mettre en place des parades.¹⁵

Il faut protéger le système informatique, mais ce n'est pas le but en soi. Il faut créer un environnement ouvert, stable et sûr dans lequel l'entreprise puisse fonctionner de manière optimale, avec un budget en rapport. Comme dans l'introduction, la sécurité informatique est devenue un facteur primordial pour pouvoir fonctionner avec succès

¹⁴ ISO/IEC TR 133352.1997, page 9, AFNOR 2002. ISO/IEC 17799 :2000 (E), page 1,AFNOR 2002.

¹⁵ Bertrand Lathoud, DEA en Droit, Criminalité et Sécurité des Nouvelles Technologies, cours du 27 Mars 2003.

dans un monde économique dirigé par une ouverture totale et globale à travers l'Internet. De plus, comme présenté dans l'état des lieux cette ouverture pose le plus grand risque sécuritaire. Trouver le juste milieu avec les méthodes et techniques existants constitue le défi de toute entreprise et non seulement celui du responsable informatique comme c'est encore trop souvent le cas.

3.3 L'approche mathématique

Le '*working paper*'¹⁶ de Kevin Soo Hoo donne probablement l'exemple le plus détaillé d'une approche mathématique. Avant de proposer un modèle mathématique pour pouvoir calculer les coûts des outils de sécurité il donne un aperçu de l'évolution des méthodes depuis 1979 environ. Il identifie trois générations de méthodes, sa proposition fait partie de la troisième.

Nous ne suivons pas cette distinction en générations parce que dans la pratique on trouve souvent un amalgame des trois méthodes. Pour la lisibilité nous traitons les propos de Soo Hoo dans l'ordre de sa thèse, puis nous revenons en détail sur les méthodes qualitatives normatives.

3.3.1 La première génération

La première génération est une méthode basée sur l'estimation annuelle de perte subie à cause des attaques informatiques ('*Annual Loss Expectancy*')¹⁷ du '*National Bureau of Standards*'. Le problème de cette approche est l'incapacité de distinguer des événements qui arrivent souvent mais ont un petit impact par rapport aux les événements qui arrive rarement mais pourraient avoir un impact important sur la sécurité informatique. Malgré la possibilité d'automatisation des calculs par ordinateur, le niveau de détail nécessaire rends cette méthode impraticable. Le niveau de détail nécessaire de cette méthode, combiné avec la vision qu'un système informatique devrait être à 100% sûr, rend l'effort titanesque. C'est une limite qu'on observe avec beaucoup de méthodes mathématiques.

¹⁶ How much is enough? A Risk-Management Approach to Computer Security, Kevin J.Soo Hoo , CRISP June 2000.

¹⁷ National Bureau of Standards, Guideline for Automatic Data Processing Risk Analysis, FIPS PUB 65 (Washington D.C. Us General Printing Office 1979).

3.3.2 La deuxième génération

Les méthodes de la deuxième génération prennent en compte les problèmes que posaient les méthodes de la génération précédente et visent essentiellement la facilité du déploiement et l'acceptation dans l'entreprise qui sont visés. Elles sont qualitatives et les problèmes de la complexité et de l'incertitude ne sont pas adressés.¹⁸ Soo Hoo distingue 4 approches : '*Integrated Business Risk-Management Framework*', les méthodes d'évaluation, les méthodes basées sur des scénarios et la méthode des meilleurs pratiques dite 'Best Practices'.¹⁹

La nouveauté importante introduite par l'*Integrated Business Risk-Management Framework* est, que les risques relatés à l'informatique sont considérés comme des risques de gestion en tant que tel. L'informatique sort désormais de son domaine strictement utilitaire pour devenir une force de valeur ajoutée reconnue, si elle est bien gérée. En plus l'importance de la sécurité de l'informatique prend une autre dimension dans cette optique. Ce changement de concept est très important pour le développement d'une stratégie de sécurité informatique adéquate dans la pratique.

Les méthodes d'évaluation se basent surtout sur la valeur des biens, leur mode de sécurisation, et sur le déploiement de la sécurité dans l'entreprise. Elles ne prennent pas en compte la fréquence et la probabilité du risque mais seulement des conséquences éventuelles. Cette approche qui n'inclut pas d'autres facteurs tels que les coûts et l'efficacité des mesures ou encore la fréquence des attaques, peut générer le risque d'une sur- ou sous-sécurisation des biens.²⁰

Les méthodes d'analyse des scénarios se basent sur des scénarios compromettant la sécurité d'un système informatique. Le danger est alors d'oublier ou de ne pas identifier des scénarios importants.²¹

¹⁸ Voir note 18, page 9.

¹⁹ Voir note 18, page 9 ss.

²⁰ Voir note 18, page 10.

²¹ Voir note 18, page 11.

3.3.3 Meilleures Pratiques²²

La méthode des meilleures pratiques est fondé sur le choix qu’au lieu de se fier à des données inadéquates ou à des expertises subjectives, il vaut peut-être mieux se baser sur les ‘best practices’ de l’industrie. Entre autres, il s’agit d’obtenir une protection efficace en cas de litige basé sur un fait de négligence. Le succès dépend largement des frais et de l’efficacité de l’approche. Un inconvénient de la méthode pourrait être que les meilleures pratiques deviennent un but en soi et non une démarche visant à maîtriser les risques réels. Pour l’instant les meilleures pratiques jouissent d’une grande popularité.

3.3.4 La troisième génération

Il y a trois contraintes qui expliqueraient une approche plus quantitative, selon Soo Hoo: les besoins d’assurance, les risques de responsabilité juridique et la concurrence.²³ Pour avoir la possibilité de mesurer, c’est à dire calculer le ROI, une méthode quantitative serait idéale. L’absence des données sur la fréquence, le caractère et l’impact des attaques d’où la probabilité des impacts pourrait être déduits, rend un calcul fiable presque impossible. Pour l’instant la réticence à publier les données sur les attaques subies, si ce n’est pas dû plutôt à une certaine ignorance, est très pénalisante pour les méthodes quantitatives.

Soo Hoo essaie de répondre à ce problème en avançant un cadre de décision analytique quantitatif en mettant l’accent sur la décision de gestion de risque. Il utilise le ‘*decision modeling*’ à la base.²⁴ L’avantage de ce modèle est l’adaptabilité au niveau de détail nécessaire ou souhaité.

La forme très mathématique suggère une certitude quantitative beaucoup plus élevée qu’elle ne l’est en réalité. Basé sur des décisions expertes, certes, mais quand même intuitives, le contenu des cellules reste aussi subjectif que dans le cas des méthodes de la deuxième génération. Nous pensons que son ‘*Computer Security Risk Model*’²⁵ n’est pas si simple qu’il le présente. L’exercice en soi est valable pour créer un consensus et faciliter le déploiement de la sécurité. Le nombre de variables nécessaires pour valider le modèle est non-négligeable et il faut parcourir les équations de chaque

²² Pour une description du développement des Best Practices voir, ‘Finding a language to address information security management’, ISO Bulletin December 2000, page 23.

²³ Voir note 18, page 12.

²⁴ Voir note 18, page 16 ss.

²⁵ Voir note 18, page 19.

variable, ce qui parvient vite à un exercice aussi laborieux que la première génération de méthodes engendraient. L'avantage de la méthode par contre, est qu'on arrive à un aperçu de l'ensemble du système plutôt qu'à une vue partielle liée à un certain risque, produit ou accident. C'est sans doute la plus value apportée par ce type d'approche.

Puis Soo Hoo explique quelques techniques d'analyse²⁶ avec des distributions de probabilité pour combler le manque des données pertinentes. Quand on ajoute les distributions de probabilités, le chemin à parcourir devient encore plus long et laborieux, voir difficile à réaliser.

Dans le Chapitre 3 Soo Hoo traite de la difficulté de trouver des données valables à utiliser dans ses modèles. Il utilise entre autres l'enquête du CSI/FBI. Le problème des données est qu'elles ne sont pas assez fiables pour donner une réponse statistiquement valable. Les termes ne sont pas définis de manière uniforme et il manque des conventions sur la façon de compter et répondre aux enquêtes. En plus il y a la spéculation sur les dommages engendré par un incident quand on parle des valeurs intangibles comme la réputation, la confiance etc. Il propose d'attaquer ce problème avec des distributions de probabilités pour rester plus ou moins efficace. En faisant cela, il introduit de nouveau une incertitude dans son équation.

Dans le Chapitre 4 il donne un exemple pratique de son analyse.

3.3.5 Conclusion

Nous pensons que le modèle quantitatif de Soo Hoo est valable au niveau académique. Le mérite de l'exercice se trouve dans l'utilisation du concept du '*Integrated Business Risk Management*', ce qui permet de présenter les décisions d'une façon complète et itérative. La complexité est plus facile à gérer. Le problème reste que les données à la base sont subjectives et manipulables faute d'existence des données pertinentes. La valeur pratique nous semble réduite, par la complexité de la démarche. L'avantage pour les entreprises est le fait que tout le système sécuritaire peut être intégré dans le modèle et que ce dernier semble donner une appréciation valable sur les investissements à faire et dans des domaines particuliers.

²⁶ Voir note 18, page 23 ss.

3.4 'Hummer'

Un exemple d'une analyse de scénario pour déterminer le ROI des outils de sécurité est le projet de l'Université de Idaho, codé '*Hummer*'.²⁷ Le but était de prouver que la détection d'une intrusion du moment de sa survenue, est plus efficace et moins cher que d'essayer de prévenir les attaques. La difficulté était de nouveau la désignation des coûts valides. Ils ont commencé par assigner des valeurs aux biens tangibles moins leur dépréciation et des valeurs relatives aux biens intangibles (par exemple A vaut trois fois plus que B). Les frais des attaques établis par le Département de la Défense et généralement acceptés, étaient utilisés. Ils ont calculé la perte annuelle à attendre, dite '*Annual Loss Expectancy*' (ALE).

$$ALE = (R-E) + T$$

R = le coût annuel pour remédier les conséquences des attaques subies

E = les économies faites en stoppant les attaques et les intrusions par biais de l'outil de détection d'intrusion.

T = le coût de l'outil de détection d'intrusion.

Pour vérifier le modèle ils ont attaqué leur prototype pour voir si les frais correspondaient avec les frais du modèle théorique. Pour arriver à une analyse du bénéfice il fallait juste contrôler si l'investissement déduit des dommages prévenus donnait une somme positive ce qui égale un retour sur investissement sécuritaire (*Return on Security Investment (ROSI)*).

En plus l'équipe voulait introduire l'analyse du ROSI dans le système '*Hummer*'. Ainsi '*Hummer*' pourrait décider lui-même si une attaque vaut la peine d'être stoppée. En stockant les données de '*Hummer*' on pourrait obtenir des indices valables sur le ROSI des outils de détection d'intrusion.

La simplicité du modèle est convaincante, mais il est clair qu'il reste de nombreuses outils et systèmes de sécurité à évaluer ainsi. Il faudrait élargir le projet sur des systèmes complexes et éparpillés pour savoir s'il le ROSI est encore positif. Ce qui est intéressant c'est qu'on voit une renaissance du '*Annual Loss Expectancy*' que Soo Hoo avait relégué au passé.

²⁷ Security ROI, Finally, a Real Return on Security Spending, Scott Berinato, CIO Magazine Feb. 15, 2002.

3.5 'Hoover'

Des chercheurs du Massachusetts Institute of Technology, de Stanford University et @Stake ont fait une étude basée sur une base de données 'Hoover' pour essayer de démontrer le concept intuitif que plus tôt on ajoute de la sécurité dans le processus du développement du logiciel, plus grand sera le ROSI.²⁸

Pendant 18 mois la base des données 'Hoover' a été alimentée avec des données sur la qualité et sécurité de logiciel. La présomption était qu'un bogue de sécurité n'est pas différente d'un autre bogue. Ce qui qualifiait la sécurité comme assurance de qualité et dans ce domaine il y avait une vaste base de données.

Le résultat montre que lorsque l'on ajoute de la sécurité au début du développement du software le ROSI est de 21%, alors qu'attendre jusqu'au stade d'implémentation descend le ROSI à 15% et dans la phase du test descend le ROSI jusqu'à 12%!

Cette étude est très valable pour ceux qui développent du logiciel propriétaire et pour ceux qui développent des logiciels commercial. La valeur ajoutée est que, finalement la sécurité est considérée comme partie intégrale de la qualité du logiciel.

3.6 La loi du ROSI décroissant

Une troisième étude mentionnée dans le même article du *CIO Magazine*²⁹ faite par chercheurs du Carnegie Mellon University est une analyse de la capacité de survie des systèmes réseau après attaque. L'étude mesure l'augmentation du niveau de sécurité quand on augmente l'investissement en sécurité.

Les chercheurs ont utilisé les données du CERT³⁰. Les variables utilisées étaient les sortes d'attaques, l'incidence des attaques, la probabilité, les dommages infligés, les parades utilisées et l'effectivité des parades. Ils ont construit un modèle de 'chien d'attaque' sur un réseau fictif et ont journalisé les effets sur le réseau en modifiant les paramètres. Un nouvel aspect était qu'ils ont mesuré les taux des incidents et les effets sur le réseau au lieu de prendre l'état de la sécurité comme une proposition binaire. L'état du réseau après attaque était qualificatif.

²⁸ Security ROI, Finally, a Real Return on Security Spending, Scott Berinato, CIO Magazine Feb. 15, 2002.

²⁹ Security ROI, Finally, a Real Return on Security Spending, Scott Berinato, CIO Magazine Feb. 15, 2002

³⁰ The CERT Coordination Centre, the first computer security response group.

Le résultat est que le ROSI augmente de manière décroissante. Ce résultat est intéressant du point de vue de preuve d'une attente intuitive. En investissant de plus en plus dans la sécurité, on crée forcément après un moment donné, un recouvrement partiel. Les auteurs résolvent ce problème en ajoutant une courbe d'indifférence, ce qui définit le point où l'investissement donné a apporté une protection satisfaisante au réseau.

De nouveau dans ces trois études plutôt pragmatiques le problème des données fiables est relevé. Pour l'instant c'est un problème qui risque de ne pas être résolu très vite, vu la réticence des entreprises de rapporter les incidents.³¹

3.7 Conclusion

Le concept de ROSI pose comme on a vu des problèmes pratiques mais reste un sujet très à cœur des entreprises gouvernées par les résultats trimestriels. Dans des articles plus récents on trouve de plus en plus l'acceptation des approximations. Pour vendre des projets de sécurité internes le ROSI reste souvent une équation convaincante. Mais la question d'une politique de sécurité reste dans ces cas là probablement ouverte.

Dans un article de *CSO Magazine* de décembre 2002³² l'importance du ROSI pour motiver le budget est de nouveau l'objet. La raison principale c'est la donnée de la recherche de l'économiste Frank J. Bernhard que 6 % de revenue sont à risque quand la sécurité n'est pas assurée, tandis que seulement 10 % du budget de l'informatique est investi dans la sécurité. Cette donnée est très intéressante et parce qu'elle démontre qu'un petit investissement en sécurité peut avoir un impact considérable sur le revenu.

Nous pensons que pour arriver à un ROSI utilisable il faut oublier la précision. Il faut prendre en compte la probabilité, qu'il faut chercher des données, le plus possible et partout. Il faut ensuite essayer de trouver l'information dans les autres départements et puis tenir compte des spécificités de l'industrie. Dans le calcul on retrouve l'approche '*Annual Loss Expectancy*', et une forme d'*Annual Loss Expectancy*' mitigée pour tenir compte des parades installées.³³

³¹ Voir note 15.

³² Calculated Risk, Scott Berinato, CSO Magazine December 2002. <http://www.csoonline.com/read/120902/calculate.html>

³³ Idem 32.

Le concept du ROSI est bien utilisé dans le monde commercial de la vente des produits de sécurité et le monde des services dans le domaine de la sécurité. Pour avoir des exemples il suffit d'entrer 'ROSI' ou 'ROI Sécurité' dans un moteur de recherche comme 'Google' et on retrouve des quantités de 'white papers', des études sur le sujet par rapport au produit. On peut trouver un article sur le ROI pour chaque produit de sécurité, mais il faut tenir compte de l'aspect commercial de cette information!

Les méthodes purement quantitatives donnent un ROSI dans le vrai sens du mot. Dans un article du magazine *Strategic Finance* de novembre 2002,³⁴ les auteurs argumentent que le ROI n'est pas le concept adéquat pour calculer le retour économique sur investissement, ils spécifient qu'on devrait utiliser plutôt le '*Internal Rate of Return*'. Ensuite ils démontrent qu'il ne faut pas essayer de maximaliser ce ratio, parce que même avec un investissement plus grand et un IRR plus petit, les économies peuvent être plus importantes à la fin. Il faut prendre en compte que le IRR se fait 'ex ante' et alors prévoir un audit 'ex post' pour vérifier les données.

Finalement, selon les auteurs, les entreprises doivent poursuivre un niveau optimal d'investissement dans la sécurité informatique au lieu de poursuivre une IRR ou ROSI.

Avec cette relativisation de l'importance d'un retour sur investissement des outils de sécurité, nous aimerions aborder le cadre plus large de valeur économique de la sécurité informatique. A notre avis le but de l'investissement dans la sécurité n'est pas 'd'achever un niveau optimal de l'investissement' mais surtout 'd'achever un niveau optimal de sécurité dans l'environnement économique de l'entreprise'.

³⁴ Return on Information Security Investment, Lawrence Gordon, Martin Loeb, *Strategic Finance Magazine*, November 2002. <http://www.strategicfinancemag.com/2002/11i.htm>

4. Les méthodes normatives et les standards.³⁵

4.1 Introduction

Pour arriver à une stratégie de sécurité de l'entreprise la simple addition des produits de sécurité ne suffira pas. Il faut avoir une vue d'ensemble qui permettra d'établir des priorités avec l'accent sur la continuité des processus clés de l'entreprise. Mais comme on a vu dans l'introduction les interdépendances avec des fournisseurs, partenaires, clients et les relations avec les employés poussent à un certain niveau de sécurité pour pouvoir opérer sur le marché. Les Etats cherchent de plus en plus à sécuriser l'infrastructure Internet dont leur économie est devenue dépendante à travers des législations et des développements des standards pour la sécurité.

4.2 Cadre³⁶

Les méthodes normatives et les standards de sécurité ont un schéma plus ou moins commun de base. Les accents peuvent être différents et les méthodes plus ou moins exhaustive. Les critères de sécurité généralement acceptés pour les systèmes d'information sont :

- Disponibilité
- Intégrité
- Confidentialité
- Authenticité
- Imputabilité

Les attaques informatiques visent à anéantir ou affaiblir une ou plusieurs de ces caractéristiques ou à exploiter une vulnérabilité de ces caractéristiques. Les vulnérabilités peuvent être objectives : due à la technologie utilisée, ou subjectives: due à des failles humaines. Les attaques utilisent souvent les deux combinés. La plus répandue est le '*social engineering*'. Ici l'auteur manipule par exemple un employé par téléphone pour pouvoir accéder à un système ou à une base de données. Un autre

³⁵ L'idée générale des méthodes normatives c'est de devenir un jour un standard. Comme il y beaucoup de méthodes normatives pas encore 'standard' et beaucoup de standards avec une application souvent géopolitique j'utilise les deux termes.

³⁶ Gestion de la sécurité des systèmes d'information, DEA – Droit, Criminalité et Sécurité des Nouvelles Technologies, Bertrand Lathoud, Cours du jeudi 13 mars 2003.

exemple c'est un employé malveillant qui introduit un virus dans le système de son employeur.

Le principe fondamental d'une politique de sécurité est de minimiser les pertes au niveau financier, du savoir-faire ou d'image et de permettre un usage efficace et économique des technologies en réduisant les risques technologiques et informationnels à un niveau acceptable pour l'entreprise.³⁷

Le processus clé est l'identification et l'analyse du risque, puis la mise en place des parades et la gestion du risque résiduel.

On peut distinguer cinq domaines d'application de la sécurité³⁸:

- La sécurité physique
- La sécurité logique
- La sécurité applicative
- La sécurité de l'exploitation
- La sécurité de télécommunications

Pour compléter ce cadre il faut mentionner les intervenants d'une stratégie sécuritaire. Les intervenants les plus importants sont les dirigeants. Pour motiver les autres acteurs : les utilisateurs, les conseillers juridiques, financiers et de ressources humaines, et les administrateurs de la sécurité, il est primordial que le comité de direction en prenne la responsabilité comme pour la stratégie de gestion.

Il y a une grande quantité des méthodes normatives. Les plus connues sont les normes internationales ISO 13335, ISO 15408 et ISO 17799, qui est issue des British Standard 7799. Il y a des standards nationaux dont le '*IT Baseline Protection Manual*' du Bundesamt für Sicherheit Information Technik allemand, les outils du Centre de la Sécurité des Télécommunications de Canada, du Direction Centrale de la Sécurité des Systèmes d'Information de France, et du National Institute for Standards and Technology des Etats Unis et le BS 7799 anglais. Il y des méthodes issues de l'université comme Octave de Carnegie Mellon University et finalement il y a les meilleures pratiques dont les GASSP, les GAISP et le BS 7799. En plus il y a beaucoup des guides sur le sujet comme '*The CERT Guide to System and Network Practices*'³⁹ et

³⁷ Idem note 35.

³⁸ Sécurité Internet. Stratégies et Technologies, S. Ghernaoui-Hélie. Dunod 2000. Page 45

³⁹ The CERT Guide to System and Network Practices, Julia H. Allen, 2001.

le *'NCSA Guide to Enterprise Security'*⁴⁰. Les deux derniers guides adressent surtout l'aspect technique de l'implémentation de la sécurité. Le *'Common sense guide for senior managers'* par l'Internet Security Alliance⁴¹, et *'The Standard of Good Practice for Information Security'*⁴² par l'Information Security Forum, qui compte parmi ses 255 membres les plus grandes sociétés au niveau mondial, adressent la nécessité d'une stratégie de sécurité au niveau de la direction. Beaucoup de ces standards se sont basés sur des meilleures pratiques. La grande utilisation et l'ubiquité de l'implantation des meilleures pratiques semblent démontrer que dans la pratique, ils se sont développés bien au-delà les limitations que Soo Hoo voit.⁴³

4.3 ISO 17799⁴⁴

La norme ISO 17799 est pour l'instant la méthode la plus acceptée malgré les oppositions initiales. Elle est basée sur British Standard 7799, mais contrairement au BS 7799 il n'y a pas de certification. Elle a été passée avec une procédure accélérée auprès de l'ISO et a été largement contestée par les grands pays qui avaient déjà leurs propres standards et les critiques sont relatives au fait qu'il n'y a pas de recommandations sur la manière d'implémenter la norme.

Etabli au Royaume Uni, elle est implantée dans beaucoup d'entreprises Anglo-Saxonnes. Puis dans les petits pays⁴⁵ qui l'avaient accepté dans le cadre de l'ISO. On constate qu'elle est propagée par des associations issues des grandes entreprises mondiales qui influencent à leur tour la politique.⁴⁶ Ainsi elle semble de devenir un standard de fait et de réseau. Par exemple: Aux Etats-Unis la compagnie d'assurance Arthur J. Gallagher & Co demande l'application de la norme pour pouvoir conclure une assurance contre les cyberrisques!⁴⁷ De plus l'Information Security Forum offre un

⁴⁰ NCSA Guide to Enterprise Security, Michel E. Kabay, 1996

⁴¹ <http://www.isalliance.org/>

⁴² <http://www.isfsecuritystandard.com/>

⁴³ Idem note 18, page 12

⁴⁴ ISO/IEC 17799: 2000, International Standards Organisation/International Electrotechnical Commission.

⁴⁵ Pour la Suisse la norme a été adoptée sans changement dans la Norme suisse SN17799 : 2001.

⁴⁶ Pour plus d'information sur le développement de la norme voir : ISO Bulletin December 2000.

⁴⁷ <http://www.csoonline.com/read/030103/lite.html> Lettre de Peter Schindel, Vice President, Cyberrisk Services, Arthur J. Gallagher & Co.

outil de comparaison et d'analyse de la sécurité implémentée dans une entreprise qui permet aussi de se comparer à la norme ISO 17799.⁴⁸

La norme adresse trois sources de critères de sécurité:

- analyse de risques pour l'organisation: les menaces, les vulnérabilités, probabilité de l'occurrence et l'impact potentiel;
- les conditions légales, contractuelles et les régulations;
- les principes, objectifs et conditions de traitement de l'information internes à l'organisation, développés pour soutenir ses opérations.

L'analyse du risque, est la considération systématique des dommages aux affaires et la probabilité réaliste de l'occurrence. Il faut implémenter des contrôles enfin de s'assurer que les risques sont réduits à un niveau acceptable, contre un niveau de coûts en relation avec le risque réduit et les dommages en cas d'infraction de sécurité. Dans les dommages, il faut inclure les facteurs non monétaires comme par exemple la perte de réputation et de confiance. Pour faire une telle analyse de risque, l'application d'une méthode quantitative comme proposé par Soo Hoo⁴⁹ par exemple, est préférable pour avoir un aperçu détaillé. Mais ce n'est qu'une partie d'une stratégie sécuritaire. La norme insiste sur les facteurs critiques suivants:

- existence d'une politique de sécurité en adéquation avec les activités de l'organisation et les prestations attendues du système d'information;
- existence d'une démarche sécurité crédible et implantable. Elle doit être cohérente avec la culture de l'organisation et faire partie de sa stratégie;
- soutien visible et déclaré de la direction pour la mise en place des mesures de sécurité;
- bonne compréhension des exigences de la sécurité, de l'analyse et de la maîtrise des risques par les personnes chargées de l'implantation de la sécurité;
- diffusion des notions de sécurité à tous les échelons de l'organisation: direction et personnel;
- création et diffusion de directives de sécurité pour le personnel et pour les intervenants externes; diffusion de ces directives aux places de travail;
- accompagnement de la mise en place de la sécurité par une formation adéquate des utilisateurs;

⁴⁸ Information Security Survey, Information Security Forum
<http://www.ifssecuritystandard.com/survey/bench.htm>

⁴⁹ Idem note 18, page 15

- mise en place d'un système complet de mesure et d'audit pour évaluer le fonctionnement de la gestion de la sécurité et d'annoncer des problèmes et de suggestions d'amélioration.⁵⁰

La norme ne place pas seulement l'accent sur les aspects techniques mais évoque également l'importance des intervenants, les acteurs dans le processus de la sécurité. En plus elle prend en compte les conditions légales, contractuelles et normatives qui obligent à un certain niveau de sécurité. Pour maîtriser tous les aspects de la sécurité cette approche est devenue indispensable, ce qui est appuyé par les données des enquêtes mentionnées ci-dessus. La norme se positionne comme point de départ en soulignant qu'elle peut contenir des directives qui ne sont pas applicables dans des situations spécifiques ou alors qu'il peut être nécessaire d'en ajouter. Mais c'est une approche qui est beaucoup plus lourde et chère à suivre pour les entreprises. Ce qui explique probablement les données de Clusif où seulement les grandes entreprises ont une stratégie de sécurité en place.⁵¹ Si on regarde qui fait partie de l'International Security Forum, de l'International Security Alliance etc., on constate que ce sont toujours les mêmes grandes entreprises multinationales. Souvent ce sont les mêmes grandes entreprises qui sont gérées par les résultats financiers trimestriels et où le retour sur investissement joue le plus grand rôle. Tandis que calculer un retour sur investissement pour une stratégie de sécurité basée sur cette norme est encore beaucoup plus difficile que le retour sur les investissements des outils techniques parce-que il y a beaucoup plus de facteurs et valeurs non-tangibles concernées. Alors il y a probablement d'autres motivations qui justifient un tel investissement. Avant d'étudier les forces d'extérieur qui peuvent obliger cet investissement, il y a des motivations internes à l'organisation qui valident une stratégie sécuritaire.

4.4 Gestion de la Qualité

Au début des années '80 les entreprises se trouvaient dans une position comparable envers la gestion de la qualité, qu'elles se trouvent aujourd'hui envers la gestion de sécurité de l'information. L'ISO avait spécifié la Norme 9001 avec une procédure de certification. Le grand problème à l'époque était le même qu'aujourd'hui: Est-ce que cela vaut l'investissement ? Avec la qualité, on tombe dans les mêmes problèmes d'intangibilité des économies: comment peut-on mesurer la qualité? Est-ce qu'il existe

⁵⁰ Après la qualité, l'ISO s'attaque à la sécurité, Henri Carrera, IBCOM 1-2/03, pour la traduction compréhensive des 'critical success factors' de la norme ISO/IEC 17799 : 2000.

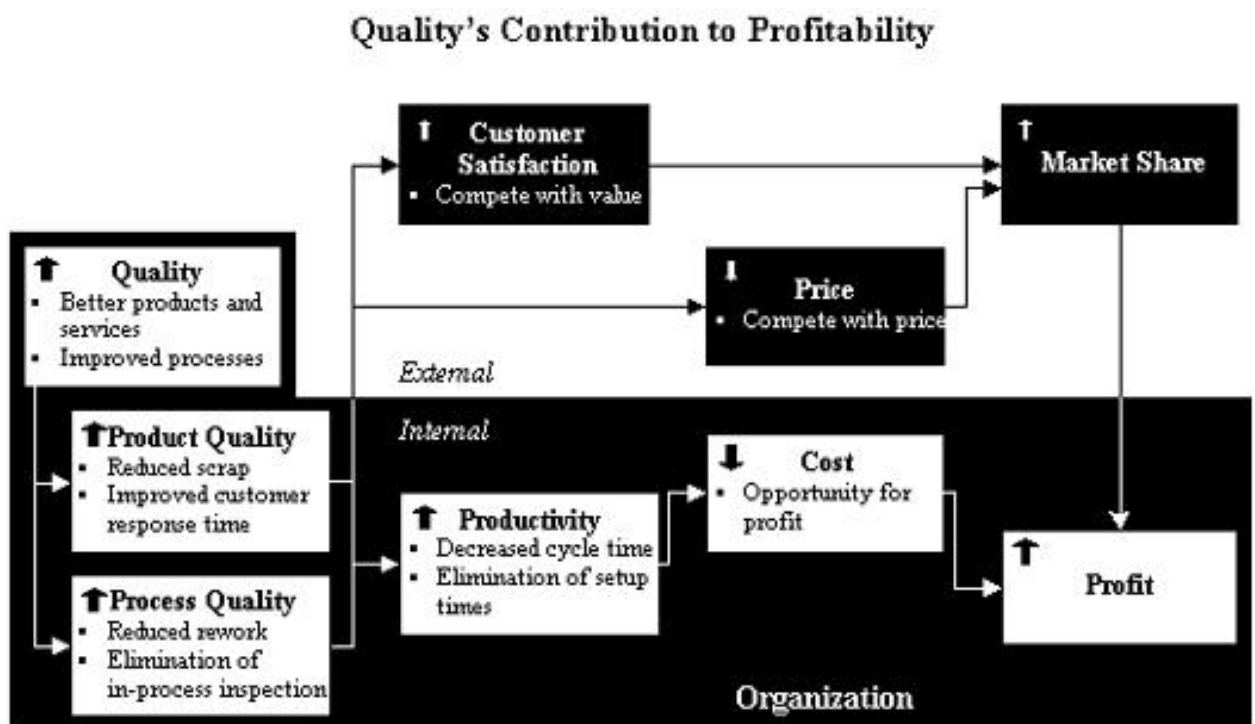
⁵¹ Idem note 10.

des garanties de succès? La seule indication que ça pouvait marcher était le fait que les Japonais utilisaient les principes de Deming⁵² et que leurs produits étaient devenus qualitativement supérieurs aux produits occidentaux, sans être plus chers. Ce qui posait un problème de compétition. Intuitivement il y avait beaucoup de motivations pour le faire, comme pour la sécurité mais il faut une base analytique pour convaincre les actionnaires. Entre temps il y a eu beaucoup de recherche, les données qui manquaient il y a vingt ans, existent aujourd’hui. Le schéma est relativement simple:

- La qualité d’un produit ou d’un service procure des clients et les retient;
- ces clients attirent des nouveaux clients par une publicité de type bouche à l’oreille;
- et il y a des clients des concurrents qui changent de marque.

Le résultat est une plus grande part de marché, plus de revenus et de profits. A l’autre bout du schéma, il y a la qualité de la production à des frais moindres, ce qui augmente également les profits.⁵³ La procédure pour déterminer les facteurs importants de la qualité est basée largement sur des enquêtes auprès des clients.⁵⁴

Le modèle ici dessous montre la contribution à la profitabilité de la qualité⁵⁵



⁵² <http://www.asq.org> Birth of Total Quality

⁵³ Return on Quality, Roland T. Rust, Anthony J. Zahorik, Timothy L. Keiningham, Irwin Professional Publishing© 1994, page 5.

⁵⁴ Idem 53, page 8.

⁵⁵ <http://www.asq.org/>

Aujourd'hui plus que 600.000 entreprises dans le monde sont certifiées ISO 9000. Finalement c'est souvent le marché qui a poussé les entreprises à la certification. Soit la concurrence, soit les partenaires d'affaires, soit les clients exigeaient la certification. La certification donnait et donne encore un avantage concurrentiel.

Assumer que les entreprises qui ont aujourd'hui une stratégie compréhensive de la sécurité sont tous certifiés ISO 9000 semble assez valable. Aujourd'hui, la qualité de leur produit/service est mis en danger par les attaques physiques et/ou informatiques. Surtout les grandes entreprises mondiales sont visées par les attaques, à cause de leur force médiatique. Ce qui ressort des enquêtes, c'est que l'attention des médias n'est pas forcément un bonus. La motivation interne qui les a amenée à prendre des devants dans les stratégies de sécurité se dessine alors. La sécurité fait partie intégrale de la qualité.

4.5 La législation

Une force d'extérieur qui oblige à l'investissement dans de la sécurité est la législation. L'informatique et l'Internet ont généré beaucoup de législations spécifiques, mais il ne faut pas oublier la législation existante qui est souvent parfaitement *'internetocompatible'*. Beaucoup de lois sont valides indépendamment du support. Il y a une neutralité technologique qui se traduit de manière efficace en: *'Ce qui est illégal 'off-line' reste illégal 'on-line!'*⁵⁶ Pourtant l'Internet a donné de nouvelles formes aux infractions et délits existants, son ubiquité facilite la diffusion rapide, son organisation permet un anonymat quasi total, ce qui rend le système juridique souvent impuissant. Le fait qu'il y des 'paradis légaux' partout dans le monde rend un système juridique efficace presque impossible. Pour l'instant on essaie quand même de trouver une solution internationale pour ces problèmes avec des traités et des conventions internationales. Quelques-uns de ces traités et conventions internationaux, souvent déjà adaptés par une législation nationale, obligent les entreprises à la conformité.

4.5.1 Le droit pénal

Dans le cadre du droit pénal le principe de Art. 1 Code Pénal Suisse (CPS) 'Pas de peine sans loi' ne facilite pas la poursuite des infractions. La technologie se développe tellement vite que la législation à de la peine à suivre. Formuler une loi qui capte une infraction aujourd'hui est possible, mais il existe probablement déjà des nouveaux

⁵⁶ Citation Prof. B. Cottier, Cours du droit du multimédia 21 mars 2003, DEA en Droit, Criminalité et Sécurité des Nouvelles Technologies.

moyens de la commettre qui ne sont pas encore connus. Car il n'est pas possible par principe, d'agir par analogie, c'est souvent impossible de poursuivre l'auteur. En plus la rédaction des lois pose un problème, car souvent le texte est tellement restrictif qu'on arrive pas non plus à qualifier l'infraction. Une autre restriction à l'efficacité est l'organisation internationale de l'Internet, qui permet à l'auteur de se cacher très facilement soit derrière une fausse identité, soit dans un pays avec des normes moins strictes (paradis légaux). La Convention sur la Cybercriminalité du Conseil de l'Europe⁵⁷ essaie:

'd'établir une politique pénale commune destinée à protéger la société de la criminalité dans le cyberspace, notamment par l'adoption d'une législation appropriée et par l'amélioration de la coopération internationale;'

estimant qu'une lutte bien menée contre la cybercriminalité requiert une coopération internationale en matière pénale accrue, rapide et efficace;

Convaincus que la présente Convention est nécessaire pour prévenir les actes portant atteinte à la confidentialité, à l'intégrité et à la disponibilité des systèmes informatiques, des réseaux et des données, ainsi que l'usage frauduleux de tels systèmes, réseaux et données, en assurant l'incrimination de ces comportements, tels que décrits dans la présente Convention, et l'adoption de pouvoirs suffisants pour permettre une lutte efficace contre ces infractions pénales, en facilitant la détection, l'investigation et la poursuite, quant à plan national qu'au niveau international, et en prévoyant de dispositions matérielles en d'une coopération internationale rapide et fiable;⁵⁸

Ce qui concerne les stratégies de la sécurité des entreprises, c'est surtout l'article 12 de cette convention concernant la responsabilité des personnes morales, qui est important:

Article 12 – Responsabilité des personnes morales

1 Chaque Partie adopte les mesures législatives et autres qui se révèlent nécessaires pour que les personnes morales puissent être tenues pour responsables des infractions établies en application de la présente Convention, lorsqu'elles sont commises pour leur compte par toute personne physique, agissant soit individuellement, soit en tant que membre d'un organe de la personne morale, qui exerce un pouvoir de direction en son sein, fondé:

A sur un pouvoir de représentation de la personne morale;

B sur une autorité pour prendre des décisions au nom de la personne morale;

C sur une autorité pour exercer un contrôle au sein de la personne morale.

⁵⁷ STE ? 185, Convention sur la Cybercriminalité 2001, Conseil de l'Europe.

⁵⁸ Idem note 57, voir le Préambule.

Outre les cas déjà prévus au paragraphe 1 du présent article, chaque Partie adopte les mesures qui se révèlent nécessaires pour s'assurer qu'une personne morale peut être tenue pour responsable lorsque l'absence de surveillance ou de contrôle de la part d'une personne physique mentionnée au paragraphe 1 a rendu possible la commission des infractions établies en application de la présence Convention pour le compte de ladite personne morale par une personne physique agissant sous son autorité.

Selon les principes juridiques de la Partie, la responsabilité d'une personne morale peut être pénale, civile ou administrative.

Cette responsabilité est établie sans préjudice de la responsabilité pénale des personnes physiques ayant commis l'infraction.

La responsabilité d'une entreprise pour les employés va très loin dans le sens qu'une entreprise doit installer des moyens de contrôle et de surveillance suffisants. Comme on a vu dans les données des enquêtes, cette protection n'est pas seulement valable vis à vis des tiers, mais autant pour l'entreprise elle-même. La valeur économique d'un tel investissement se trouve surtout dans la prévention des dégâts causés par des dommages et de réputation. Ici de nouveau on peut considérer que la taille de l'entreprise où l'employé a un certain anonymat est représentative pour nécessiter un tel investissement. Pour l'instant, la Convention n'est ratifiée que par trois pays: l'Albanie, la Croatie et l'Estonie.

4.5.2 Protection de la personnalité et protection des données

La législation visant la protection des données a aussi un impact sur la gestion des entreprises. Notamment la mise en place des sauvegardes devient impérative. La Convention pour la protection de personnes à l'égard du traitement automatisé de données à caractère personnel, STE ? 108 du Conseil de l'Europe de 1981 a comme but *'d'étendre la protection des droits et des libertés fondamentales de chacun, notamment le droit au respect de la vie privée, eu égard à l'intensification de la circulation à travers les frontières des données à caractère personnel faisant l'objet de traitements automatisés;*⁵⁹. Cette convention est suivie par quelques directives de la Communauté européenne à cet égard : la Directive relative à la protection à l'égard du traitement de données à caractère personnel et à la libre circulation de ces données⁶⁰ et la Directive 2002/58/CE du Parlement européen et du Conseil du 12 juillet 2002 concernant le traitement des données à caractère personnel et la protection de la vie

⁵⁹ Convention pour la protection de personnes à l'égard du traitement automatisé de données à caractère personnel, STE ? 108 du Conseil de l'Europe, 1981, préambule.

⁶⁰ Directive 95/46/EC du Parlement européen et du Conseil du 24 octobre 1995 relative à la protection à l'égard du traitement de données à caractère personnel et à la libre circulation de ces données.

privée dans le secteur des communications électroniques (directive vie privée et communications électroniques). La différence entre les deux est expliquée dans le préambule de la Directive 2002/58/CE :

La directive 95/46/CE du Parlement européen et du Conseil du 24 octobre 1995 relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données(4) exige que les États membres protègent les droits et les libertés des personnes physiques à l'égard du traitement des données à caractère personnel, et notamment le droit au respect de leur vie privée, afin d'assurer la libre circulation des données à caractère personnel dans la Communauté.

La présente directive vise à respecter les droits fondamentaux et observe les principes reconnus notamment par la charte des droits fondamentaux de l'Union européenne. En particulier, elle vise à garantir le plein respect des droits exposés aux articles 7 et 8 de cette charte.

Il est intéressant de noter que le législateur mentionne un but économique secondaire: la création d'un environnement sûr pour que l'utilisateur ait confiance dans l'utilisation des nouveaux services trans-frontalières.⁶¹ Les entreprises profiteront également d'une telle confiance.

En Suisse, cette législation et les conséquences pour l'industrie sont présentées dans le 'Guide relatif à la surveillance de l'utilisation d'Internet et du courrier électronique au lieu de travail.'⁶² Le problème de cette législation pour l'entreprise existe dans un conflit des objectifs. D'une part, l'entreprise est responsable pour chaque acte illégal des employés et doit installer un certain niveau de surveillance et de contrôle, d'autre part, elle doit faire attention à ne pas piétiner les droits fondamentaux de l'employé. Le Guide propose une mise en place des outils techniques, une formation des employés et un règlement sur l'utilisation de l'Internet. L'investissement demandé porte de nouveau sur des objets tangibles et non-tangibles. Il s'agit d'une obligation légale, donc l'investissement est obligatoire.

4.6 Le Marché

Une autre influence d'extérieur qui pousse à l'implémentation d'une stratégie de sécurité, c'est la confiance du marché. Les fournisseurs, partenaires, clients et employés ont besoin d'avoir une certaine confiance pour faire des affaires et 'se livrer'

⁶¹ Directive 2002/58/CE du Parlement européen et du Conseil du 12 juillet 2002 concernant le traitement des données à caractère personnel et la protection de la vie privée dans le secteur des communications électroniques (directive vie privée et communications électroniques), paragraphe 5.

⁶² Par le Préposé fédéral à la protection des données.

à l'utilisation des nouveaux produits. La réputation d'une entreprise a une valeur économique non-négligeable. En général c'est le fruit des années de travail, mais qui peut être très volatile.⁶³ La réputation est basée sur la qualité perçue. La sécurité fait partie intégrale de cette qualité, parce que la confiance se traduit en un sentiment de sécurité.

Pour un grand pourcentage des utilisateurs, il y a plutôt un manque de sécurité perçue autour de l'Internet et qui empêche d'utiliser des services Internet. Aujourd'hui si une entreprise arrive à établir une sécurité apparente dans le marché globale de l'Internet, elle dispose d'un avantage concurrentiel énorme. Cet avantage a un effet bénéfique sur la rentabilité de l'entreprise comparable à celui de la qualité.⁶⁴ En plus, les clients, partenaires ou la concurrence exigent un certain niveau de sécurité comme c'est le cas avec la qualité. Par exemple, Arthur J. Gallagher Assurances exige déjà la conformité à ISO 17799.⁶⁵

4.7 Conclusion

La norme ISO 17799 est très complète. Apparemment les meilleures pratiques fournissent une base d'expériences très vaste qui semble contenir en effet les meilleures solutions pour beaucoup de problèmes existants. La conformité à la législation par exemple est traitée explicitement.⁶⁶ Le fait de se conformer à un standard existant a probablement une influence positive sur le revenu. Car le temps gagné en profitant des expériences des autres peut être investi dans des affaires propres. C'est la raison probable du succès de la norme ISO 17799. Mais ce qui est valable pour un ne l'est pas forcément pour un autre. La norme reconnaît cette possibilité et propose une approche réaliste et pragmatique.⁶⁷

⁶³ Managing Brand Equity, David A. Aaker, the Free Press, 1991.

⁶⁴ Idem note 55.

⁶⁵ Idem note 47.

⁶⁶ Idem note 44, chapitre 12

⁶⁷ Idem note 44, Introduction XI

5. La Pratique

5.1 Introduction

Comment les entreprises gèrent-elles en pratique cette problématique ? Quelle est l'importance du ROSI dans la pratique ? Les enquêtes mentionnées dessus donnent déjà une idée de la place de la sécurité dans les entreprises et surtout sur les tendances et directions pour l'avenir. Nous avons vu que c'est surtout dans les grandes entreprises, qu'on trouve une stratégie de sécurité. Nous souhaitons illustrer cette perspective par la présentation de la gestion de la sécurité chez Shell . La plus-part des autres entreprises ont implémenté des solutions ad hoc, mais ne possèdent pas de vraie stratégie de la sécurité. Comme cas pratique de cette catégorie nous présentons NUON un fournisseur d'énergie néerlandais dans un marché d'électricité libéralisé.

5.2 Shell

La stratégie de sécurité est nommée '*Business Assurance*'⁶⁸. Elle est basée sur trois piliers:

- L'augmentation des menaces de virus, '*hackers*', fraude et espionnage;
- L'augmentation des attentes: des clients, partenaires, auditeurs et régulateurs;
- L'augmentation de l'exposition: la dépendance croissante aux technologies de l'informatique et des télécommunications, la connectivité croissante.

Le but de la stratégie est formulé dans le '*mission statement*' suivant:

- Protection de la réputation de l'entreprise, l'amélioration de la valeur de la marque, et l'optimisation de la gestion du risque.
- Prévention et minimalisation des impacts d'incidents et fournir des assurances aux intervenants.

Les risques identifiés concernent la confidentialité, la disponibilité et l'intégrité de l'information. Les risques législatifs sont la diligence pour les applications critique pour la sécurité, la protection de la vie privée et des données, les US Export contrôles des données, la protection des droits intellectuels et la protection des données sensibles.

⁶⁸ La présentation de Nick M. Mansfield 'The Future of Information Security: eBusiness Assurance, Shell Information Technology International, Lausanne 2003.

5.2.1 L'Analyse mathématique

Le défi chez Shell était de faire une analyse de risque mathématique. Le problème est que les applications d'affaires opèrent en vertical, ce qui donne une vue verticale de menace par scénario/application. Les infrastructures supportent plus qu'un processus d'affaires. Une analyse de vulnérabilités donnera une vue horizontale de l'infrastructure informatique et des télécommunication. En théorie il serait possible de faire une matrice des risques d'affaires (vertical) et vulnérabilités des technologies d'information et télécommunication (horizontal). En pratique, ce n'est pas envisageable à cause du nombre élevée d'applications d'affaires fonctionnant dans des environnements divers, et des milliers de composants de l'infrastructure. Ceci donne une explosion combinatoire qui n'est pas gérable. Shell a adopté le '*baseline approach*'⁶⁹ pour la sécurité parce que la diversité et la dispersion globale font que l'approche d'une analyse de risque classique n'est pas praticable.

Les '*business units*' construisent une vue pratique des dix plus grands risques d'affaires et les dix plus importantes vulnérabilités des technologies d'information et télécommunication avec un '*baseline approach*'. Après une analyse de risque est fait pour les exceptions. Une telle exception c'est le risque avec un grand impact mais faible probabilité d'occurrence, dont on doit particulièrement se préoccuper, parce que pour ce risque, il n'existe pas d'assurance.⁷⁰

5.2.2 La Stratégie

La stratégie de sécurité est de base un modèle sécuritaire ouvert en principe, mais avec des fermetures sélectives. Le concept central est le modèle de '*risk-acceptance*'. Shell a choisi le '*baseline approach*' d'ISO 17799 et utilise des processus de certification pour établir des domaines de confiance avec les partenaires d'affaires. Y sont incluses une protection des infrastructures critiques, une protection de la vie privée et des données et un déploiement des '*US Export Controls on Data*'.

5.2.3 Le Déploiement

Shell se conforme aux '*Industry Best Practices*' et va plus loin dans le déploiement de la sécurité que certains standards. Les exigences internes de rapport des incidents de sécurité sont liés à ceux des incidents de sûreté. Pour une société mondiale comme

⁶⁹ Finding a language to address information security management, ISO Bulletin December 2000, page 23.

⁷⁰ Cette information reçue de Nick Mansfield Shell SITI-ITPSNE.

Shell, ce processus fournit déjà une quantité non-négligeables des données adaptées à l'utilisation des méthodes analytiques quantitatives.

Shell est attentif au rôle de la confiance. La confiance entraîne la responsabilité. Il faut prouver qu'on mérite la confiance. Le cadre pour la conformité à la stratégie consiste en quatre outils :

- une politique de la Groupe avec un '*management system*' et un code de conduite;
- un manuel basé sur les directives dans le Code de conduite;
- des outils tactiques comme des contrats modèles, des manuels spécifiques et des '*Privacy Enhanced Tools*';
- des audits de conformité et la certification.

Pour le transfert des données dans des pays tiers le sujet des données doit consentir par écrit. En plus le Commissaire des données du pays de la CE concerné permet le transfert et notifie ces collègues.

5.3 NUON

Nuon est un fournisseur d'énergie néerlandais, qui a des opérations internationales. Nuon a 8000 employés. Ce n'est pas une entreprise mondiale comme Shell et on verra qu'en effet la gestion de la sécurité est moins cohérente et complète et ne fait pas partie d'une stratégie globale. Pour notre étude nous avons conçu un questionnaire⁷¹ que le responsable informatique a rempli.

Chez Nuon il n'y a pas pour l'instant de responsable pour toute la sécurité. Il n'y a pas de stratégie de sécurité compréhensive, mais il existe des manuels ponctuels sur l'utilisation de l'Internet, la vie privée et la protection des données.⁷² A cause de la crise économique le développement d'une stratégie compréhensive est pour l'instant arrêté. NUON utilise la norme ISO 17799 comme référence pour la stratégie. La sécurité se fait pour le moment avec du bon sens. ROSI ne joue pas de rôle dans le processus de décision. Nuon se conforme complètement à la législation et les régulations nationales.

⁷¹ Cf. Annexe A

⁷² Cf note 62.

5.4 Conclusion

Dans le cas pratique de Shell tous les aspects de la sécurité ont été passé en revue, les méthodes quantitatives et qualitatives, les meilleures pratiques, l'analyse des risques, la conformité à la législation et régulation, le rôle de la confiance, et enfin la certification et l'audit. Ils obligent certains partenaires à se certifier pour le domaine de confiance. La valeur économique de la sécurité pour ces partenaires est établie, malgré le fait que le retour sur investissement n'est pas vraiment sûr.

Il est intéressant de voir comme chaque méthode et chaque aspect à sa place dans ce monde complexe d'une telle société mondiale. Tout ce qui est valable est utilisé de façon pragmatique. On voit que le ROSI joue un rôle moins important dans l'ensemble et le responsable de la sécurité a donné un exemple d'un exercice qu'il a fait aux Etats-Unis pour justifier un programme d'amélioration de la sécurité. En fait la justification se trouvait dans un rapport critique issu d'un audit interne à la suite d'un audit critique externe nécessaire pour clôturer les comptes annuels. La motivation en général est une combinaison de diligence basée sur les standards d'industrie, les meilleures pratiques et des régulations. Dans ce cas, l'investissement est obligatoire!

Le cas de Nuon est probablement plus exemplaire de l'état actuel de la sécurité au sein des entreprises. Surtout quand on prend en considération les données des enquêtes mentionnées ici dessus, Nuon se situe vraiment bien là. La vision pragmatique des choses, on n'investit pas dans une stratégie de sécurité quand le marché ne le permet pas, va dans le sens de ROSI sans vraiment faire le calcul. Mais NUON est probablement un candidat à se trouver dans la position de fournisseur de Shell et être contraint à se conformer à un standard.

6. Conclusion Générale

On peut diviser une stratégie de sécurité en deux grandes parties: la partie technologique: les parades physiques et logiques contre les attaques physiques et logiques et la partie gestion: se conformer à la législation, la formation des employés, l'implication des fournisseurs et autres partenaires, l'assurance de la qualité dont la sécurité fait partie intégrale. La partie gestion a néanmoins aussi des conséquences au niveau technologique. Il peut être nécessaire d'implémenter des outils technologiques afin de permettre une gestion efficace.

L'implémentation des exigences sécuritaires légales et réglementaires sort du cadre d'autonomie de l'entreprise, pour cette implémentation la question d'un ROSI positif ne rentre pas dans l'équation. Pour tous les autres aspects, la question est valable, mais souvent très difficilement quantifiable.

Faire une analyse de risque de tous les risques encourus avec le système informatique avec la méthode Soo Hoo ou avec des autres analyses proposées par tous les entreprises de conseil informatique est valable. On peut alors mesurer le ROSI des outils de sécurité.

Parallèlement il faut consulter une méthode normative qualitative pour s'assurer qu'on n'a rien oublié de ce qui peut être nécessaire selon le cas. Mais les méthodes qualitatives normatives ne sont pas des panacées en toutes les circonstances. Et la valeur économique reste pour l'instant une quantité intuitive pour la plupart.

Implémenter une stratégie de sécurité ou sécuriser un système informatique, les deux demandent un investissement considérable et non seulement financier. Qu'il y ait un retour sur investissement qu'on peut plus ou moins calculer, dépend de la disponibilité des données fiables relatives aux incidents. La valeur économique d'une stratégie de sécurité dépend de beaucoup de facteurs de la gestion outre la mise en place de la sécurité, et peut être un critère important.

Une stratégie de sécurité est devenue un facteur de survie pour les entreprises mondiales, qui pour leur mode de travail sont dépendants de et exposés à l'Internet. Mais un système ou une stratégie de sécurité peut avoir une valeur économique que dans la combinaison avec du bon sens, de la diligence, et une gestion comme 'un bon père de famille'.

7. Bibliographie

1. Peter F. Drucker, *The Age of Discontinuity : Guidelines to our Changing Society* (Harper & Row 1969)
2. *Security and Strategy in the Age of Discontinuity* (Strategy and Business Issue 26) Ralph W. Shrader, Mike Mc Connell, Booz Allen Hamilton,.
3. *How much is enough? A Risk-Management Approach to Computer Security*, Kevin J.Soo Hoo, CRISP June 2000, page 68.
4. *Global Information Security Survey 2002*, Ernst & Young.
5. *Etude et statistiques sur la sinistralité informatique en France*, Club de la Sécurité des Systèmes d'Information Français, Année 2002.
6. *Health Insurance Portability and Accountability Act*
7. *Retailers report Sale bounce using Security Certificate*, Informationweek.com.
8. *Eighth Annual CSI/FBI Computer Crime and Security Survey*, Computer Security Institute 2003.
9. *ISO/IEC TR 133352.1997*, page 9, AFNOR 2002. *ISO/IEC 17799 :2000 (E)*, page 1,AFNOR 2002.
10. Bertrand Lathoud, *DEA en Droit, Criminalité et Sécurité des Nouvelles Technologies*, cours du 27 Mars 2003.
11. *Guideline for Automatic Data Processing Risk Analysis*, FIPS PUB 65, National Bureau of Standards, (Washington D.C. Us General Printing Office 1979).
12. *Finding a language to address information security management*, ISO Bulletin December 2000.
13. *Security ROI, Finally, a Real Return on Security Spending*, Scott Berinato, CIO Magazine Feb. 15, 2002.
14. *Calculated Risk*, Scott Berinato, CSO Magazine December 2002.
15. *Return on Information Security Investment*, Lawrence Gordon, Martin Loeb, Strategic Finance Magazine, November 2002
16. *The CERT Guide to System and Network Practices*, Julia H. Allen, 2001.
17. *NCSA Guide to Enterprise Security*, Michel E. Kabay, 1996
18. *ISO/IEC 17799: 2000*, International Standards Organisation/International Electrotechnical Commission.
19. *Lettre de Peter Schindel, Vice President, Cyberrisk Services*, Arthur J. Gallagher & Co.
20. *Information Security Status Survey*, Information Security Forum.
21. *Après la qualité, l'ISO s'attaque à la sécurité*, Henri Carrera, IBCOM 1-2/03

22. Return on Quality, Roland T. Rust, Anthony J. Zahorik, Timothy L. Keiningham, Irwin Professional Publishing® 1994
23. Convention sur la Cybercriminalité 2001, STE ? 185, Conseil de l'Europe
24. Convention pour la protection de personnes à l'égard du traitement automatisé de données à caractère personnel, STE ? 108 du Conseil de l'Europe, 1981, préambule.
25. Directive 95/46/EC du Parlement européen et du Conseil du 24 octobre 1995 relative à la protection à l'égard du traitement de données à caractère personnel et à la libre circulation de ces données.
26. Directive 2002/58/CE du Parlement européen et du Conseil du 12 juillet 2002 concernant le traitement des données à caractère personnel et la protection de la vie privée dans le secteur des communications électroniques (directive vie privée et communications électroniques), paragraphe 5.
27. Guide relatif à la surveillance de l'utilisation d'Internet et du courrier électronique au lieu de travail, le Préposé fédéral à la protection des données.
28. Managing Brand Equity, David A. Aaker, the Free Press, 1991
29. La présentation de Nick M. Mansfield 'The Future of Information Security: eBusiness Assurance, Shell Information Technology International, Lausanne 2003.
30. Sécurité Internet. Stratégies & technologies, S. Ghernaoui-Hélie, Dunod 2000.

8. Annexe A

Vragen m.b.t. de 'security' binnen IS bij NUON

1. Bestaat er bij NUON een CSO die de verantwoordelijkheid draagt voor de veiligheid zowel binnen IS als voor de rest van het bedrijf?
2. Zo ja, is er een algemeen veiligheidsbeleid waaraan alle medewerkers geacht worden actief deel te nemen?
3. Is er binnen een IS een 'security' strategie waarin de hoofd risico's m.b.t. de bedrijfsvoering en m.b.t. IS systemen bepaald zijn en worden geadresseerd?
4. Is daarvoor een bepaalde standaard gebruikt, zoals bijv. ISO 13335 of BS7799?
5. Het grootste probleem is de snelheid en voortdurende ontwikkeling in variatie binnen de aanvalsmogelijkheden. Heeft NUON een lange termijn visie t.a.v. daarvan ontwikkeld en hoe is de IS strategie daarop afgestemd?
6. Zowel in het kader van een algemeen veiligheidsbeleid als een afzonderlijk IS veiligheidsbeleid speelt de kosten-baten analyse bij investeringen een grote rol. Is er binnen NUON een kwantitatieve of een kwalitatieve benadering van dit probleem gebruikt, of een combinatie. Welke data zijn hiervoor gebruikt en wat voor rol hebben deze data gespeeld in het beslissingsproces?
7. Hebben de juridische ontwikkelingen, EC directieven en afgeleiden hiervan in de Nederlandse wetgeving een grote rol gespeeld in het proces?
8. Hebben marketing afwegingen, zoals vertrouwen van handelspartners, toeleveranciers en klanten in het privacybeleid van NUON, een rol gespeeld bij de beslissingen?
9. Maakt NUON deel uit van werkgroepen op dit gebied?