

## Étude prospective :

# La sécurité de l'information au Grand Duché du Luxembourg en 2010.

### Résumé

Le présent document expose le résultat d'une réflexion structurée, menée par 18 **professionnels du domaine de la Sécurité de l'Information** qui se sont attachés à **analyser l'évolution spécifique du domaine de la Sécurité de l'Information au Grand-Duché de Luxembourg d'ici 2010.**

En fonction de l'horizon ciblé, ces professionnels ont construit ensemble un scénario d'évolution pour le domaine de la Sécurité de l'Information. Ce scénario décrit les évolutions des déterminants de l'évolution de la Sécurité de l'information à horizon 2010. La mesure de l'impact de ce scénario sur des métiers en lien avec le domaine permettra d'en identifier les compétences clés. Des rapports propres à chacun des métiers sont disponibles : [www.abilitic.eu](http://www.abilitic.eu)

En tous 40 experts auront été mobilisés afin de mener cette réflexion prospective sur le domaine de la Sécurité de l'information et sur les 4 métiers étudiés.

**Mots-clés :** anticipation, prospective, Sécurité de l'information, formation, innovation

CITI

Centre de Recherche Public Henri Tudor  
29, Avenue John F.Kennedy  
L-1855 Luxembourg - Kirchberg  
Tél.: +352 42 59 91 - 333  
ax: +352 42 48 99

Rédigé par Duan Hua<sup>1</sup>, Bertrand Meunier<sup>2</sup>, Frédéric Girard<sup>3</sup>, Alex Durand<sup>4</sup>

<sup>1</sup> [duan.hua@tudor.lu](mailto:duan.hua@tudor.lu) - Expert méthode

<sup>2</sup> [bertrand.meunier@tudor.lu](mailto:bertrand.meunier@tudor.lu) - Chef de projet

<sup>3</sup> [frédéric.girard@tudor.lu](mailto:frédéric.girard@tudor.lu) - Reviewer

<sup>4</sup> [alex.durand@tudor.lu](mailto:alex.durand@tudor.lu) - Reviewer

[www.citi.tudor.lu](http://www.citi.tudor.lu)

## Remerciements

L'équipe du projet Abilitic adresse ses remerciements à :

MONSIEUR **Yuri AUFFINGER**, Cabinet Reisch & Verlainé

MONSIEUR **Philippe BACH**, Fortis Banque Luxembourg

MONSIEUR **Roland BOMBARDELLA**, Haut Commissariat à la protection nationale

MONSIEUR **Malike BOUAOUD**, IT WORKS

MONSIEUR **Thorsten BRAUN**, Luxinnovation.lu

MONSIEUR **Philippe DANN**, UBIZEN

MADAME **Muriel DEBIENNE**, ING

MONSIEUR **Charles DELBRASSINE**, IT WORKS

MONSIEUR **Jean - Marie DEOM**, Banque du Luxembourg

MONSIEUR **Alexandre DULAUNOY**, SES ASTRA

MONSIEUR **Raymond FABER**, Ministère de l'Economie et du Commerce Extérieur

MONSIEUR **Frédéric GIRARD**, CRP Henri Tudor

MONSIEUR **David HAGEN**, CSSF

MONSIEUR **Emile HAZAN**, Avocat

MONSIEUR **Olivier HEMROULLE**, Ubizen

MONSIEUR **Romain HILBERT**, Dimension Data Luxembourg

MONSIEUR **Jean-Philippe HUMBERT**, OLAS

MONSIEUR **Jean-Yves KAYSER**, Chambre des Métiers

MONSIEUR **Belkacem KECHICHEB**, CRP Henri Tudor

MONSIEUR **Djamel KHADRAOUI**, CRP Henri Tudor

MONSIEUR **Michel LAURENT**, Electrolux Luxembourg

MONSIEUR **Cédric MAUNY**, TELINDUS

MONSIEUR **Laurent MELLINGER**, SECARON

MONSIEUR **René MOES**, Police Grand-Ducale du Luxembourg

MADAME **Clara MULLER**, P&T

MADAME **Sandrine MUNOZ**, BIL

MADAME **Noelle PELTIER**, CRP Henri Tudor

MONSIEUR **PIERRE-BEAUSSE Cyril**, ALLEN & OVERY

MONSIEUR **POGGI Sébastien**, CRP Henri Tudor

MONSIEUR **ROSEVEGUE Alexandre**, BNB Parisbas

MONSIEUR **SOTIRI Erwin**, LG Avocats

MONSIEUR **LE GOUEFF Stéphan**, LG Avocats

MONSIEUR **STEICHEN Pascal**, Ministère de l'Economie et du Commerce  
Extérieur

MONSIEUR **Thomas TAMISIER**, CRP Gabriel LIPPMANN

MADAME **Florence THIEL**, Crédit agricole

MONSIEUR **François THILL**, Ministère de l'Economie et du Commerce  
Extérieur

MONSIEUR **Jean TRIMBOUR**, Luxinnovation.lu

MONSIEUR **Johan VAN DAMME**, Cours Européenne des Comptes

MONSIEUR **Stéphane WALRAVE**, Intrasoft International SA

MONSIEUR **Pierre WEIMERSKIRCH**, Commission Nationale pour la  
Protection des Données

Pour leur contribution, et leur participation active à cette réflexion sur la sécurité de  
l'information à Grand Duché du Luxembourg.

## Tables des matières.

<b>Introduction</b>	.....	<b>5</b>
<b>Méthodologie</b>	.....	<b>6</b>
<b>Le profil professionnel : rappel méthodologique</b>	.....	<b>7</b>
<b>Les trajectoires d'évolution de la sécurité de l'information</b>	.....	<b>8</b>
<b>1. Les déterminants de l'évolution de la sécurité de l'information.</b>	.....	<b>8</b>
• Recensement des déterminants	.....	8
• Sélection des déterminants clés	.....	10
<b>2. L'espace morphologique</b>	.....	<b>13</b>
<b>3. Le scénario de compromis</b>	.....	<b>14</b>
• Sélection du scénario probable	.....	14
• Sélection du scénario d'évolution souhaitable	.....	16
• Construction du scénario d'évolution de compromis	.....	18
<b>Le plan d'actions</b>	.....	<b>20</b>
<b>Conclusion</b>	.....	<b>26</b>
<b>Annexes</b>	.....	<b>27</b>
<b>Références</b>	.....	<b>34</b>

## Introduction

A partir de 2003, le Centre de Recherche Public Henri TUDOR a souhaité développer une expertise en matière d'utilisation des outils qui sont ceux de la prospective (Godet, 2001) et de l'exploration des futurs longs. Le choix a été fait d'exploiter ces outils pour la conception et le développement de démarches d'anticipation des futurs « moyens » qui soient participatives et structurées. Participatives, car elles réunissent en présentiel une communauté d'experts ayant pour objectif d'exprimer, partager et évaluer leurs idées. Structurées, car elles mobilisent de manière amendée les outils traditionnels de la prospective pour l'évaluation et la sélection des idées.

C'est dans ce cadre que le Centre de Recherche Public Henri TUDOR a défini une démarche d'anticipation des compétences. Celle-ci a pour objectif d'identifier aujourd'hui les compétences qui seront essentielles dans l'exercice d'un métier/d'une fonction à moyen terme (3-5 ans). Les résultats de cette démarche doivent alimenter les organismes de formation afin qu'ils puissent adapter au plus tôt et au plus près leurs programmes de formation. Afin d'atteindre l'objectif, il est nécessaire de dégager au préalable une trajectoire d'évolution pour le(s) métier(s) ou la fonction visée ainsi que les moyens de s'y préparer ou d'y parvenir.

Le présent document a donc pour objectif de montrer qu'il est possible d'envisager la construction d'une telle trajectoire d'évolution, plus spécifiquement dans le domaine de la sécurité de l'information au Grand-Duché de Luxembourg. Le document présente également le plan d'actions que les professionnels du domaine de la sécurité de l'information devraient suivre dès maintenant afin de se préparer ou de pro-agir vis-à-vis de la trajectoire d'évolution définie.

Le document se compose de quatre parties :

Une première partie est consacrée à l'exposé de la démarche prospective déployée par le Centre Henri Tudor auprès de 40 experts en sécurité de l'information au Luxembourg.

La deuxième partie porte sur le rappel des choix méthodologiques réalisés pour construire les profils professionnels des métiers sélectionnés dans le domaine de la Sécurité de l'Information.

La troisième partie présente la construction du scénario de compromis qui décrit une trajectoire unique d'évolution pour le domaine de la sécurité de l'information.

Enfin, la dernière partie porte sur la construction du plan d'actions à mettre en oeuvre dès maintenant pour s'ajuster sur la trajectoire choisie pour 2010.

## Méthodologie

La démarche prospective proposée a pour premier objectif d'anticiper les évolutions possibles de la sécurité de l'information au Luxembourg à 3-5 ans, et d'identifier des actions permettant soit de se préparer vis-à-vis du futur probable, soit de pro-agir pour la réalisation d'un futur souhaité. Son second objectif<sup>1</sup> est de détecter les futurs besoins en compétences de métiers du domaine de la sécurité de l'information d'ici 2010. Quatre métiers ont été identifiés par les partenaires publics et privés du CRP Henri Tudor comme étant critiques<sup>2</sup> :

1. L'auditeur en sécurité de l'information
2. Le consultant en sécurité de l'information
3. Le juriste en sécurité de l'information
4. Le chargé de monitoring des incidents IT.

En réponse à ces besoins les organismes de formation seront en mesure de concevoir et de proposer une offre de formation adaptée aux besoins du marché.

Pour cela, il est rappelé brièvement quelles sont les phases clés à partir desquelles il est possible de déployer la démarche d'anticipation. A ce titre, il est indiqué que l'expertise du Centre Henri Tudor repose sur une démarche composée de 3 étapes:

### Etape 1 : Description du métier

**Objectif** : Formaliser le **profil professionnel** pour chacun des 4 métiers

#### **Démarche** :

- Recherche d'informations sur les pratiques de chaque métier en Europe, et notamment au Luxembourg
- Groupe de travail et entretiens avec des « experts » de la sécurité de l'information ayant une vision de l'exercice de chaque métier.

### Etape 2 : Evolution du métier

**Objectif** : Anticiper les déterminants clés de l'évolution de la sécurité de l'information d'ici 3-5 ans. Identifier une trajectoire unique d'évolution pour le domaine : **Le scénario de compromis.**

**Démarche** : 3 séances de groupe de travail réunissant :

- Professionnels du secteur privé.
- Des représentants du ministère de l'économie, de la Commission Nationale pour la protection des données, du Haut commissariat à la protection nationale.
- Des experts ayant une vision de la législation liée à la sécurité de l'information, juriste, représentant de la police grand ducale.

### Etape 3 : Anticipation des compétences

**Objectif** : Anticiper les compétences actuelles et nouvelles qui seront essentielles dans l'exercice de chacun des métiers identifiés.

#### **Démarche** :

Une séance de groupe de travail réunissant le même type d'acteurs.

Les résultats obtenus en matière d'anticipation des compétences du métier de Manager logistique seront présentés en fonction des trois étapes de la démarche.

---

<sup>1</sup> Les compétences clés de chacun des métiers identifiés sont présentées dans des rapports spécifiques à chaque métier.

<sup>2</sup> Ces quatre métiers ont été sélectionnés sur base d'une évaluation du besoin en compétences et en formations à horizon 2010.

## Le profil professionnel : rappel méthodologique

Le profil professionnel décrit le travail que les professionnels accomplissent dans le cadre de leur métier ou de leur profession. Chacun des métiers est présenté en termes **d'activité, de tâche, de capacité nécessaire et de compétence**. L'idée à travers cette structuration est d'exprimer un niveau de granularité de plus en plus fin dans les expressions utilisées.

- En effet, le métier est tout d'abord découpé en **activité**. Ces activités correspondent à des blocs thématiques, des prérogatives qui sont de la responsabilité du métier étudié. Une activité comprend dans le cadre du profil professionnel un ensemble d'actions visant à l'accomplissement d'un travail déterminé.

- Ces activités sont ensuite déclinées en plusieurs **tâches**. Ces dernières sont par conséquent appréhendées comme une subdivision de l'activité ; une action réalisée dans le cadre de l'activité.

- Les tâches, exprimées par des actions génériques, sont explicitées dans les **capacités nécessaires**. Ces dernières, lorsque cela est nécessaire permettent d'appréhender au mieux ce qu'il est attendu par le métier pour une tâche donnée. Elles facilitent la contextualisation des compétences à mettre en œuvre pour réaliser une tâche.

- Enfin, la notion de **compétence** est définie comme un ensemble de savoirs, savoir-faire, savoir-être et savoirs technologiques à mettre en œuvre pour accomplir une tâche. Les savoirs et savoirs technologiques sont formulés par des expressions nominatives, les savoir être par des qualificatifs, et les savoir-faire correspondent à des actions précises à réaliser.

Le détail des profils professionnels est présenté dans les rapports spécifiques à chaque métier.

# Les trajectoires d'évolution de la sécurité de l'information

## 1. Les déterminants de l'évolution de la sécurité de l'information.

### ➤ Recensement des déterminants

Le profil d'évolution présente les déterminants de l'évolution du domaine de la sécurité de l'information, la première tâche est d'amener les experts à les identifier. Au total, 46 déterminants(cf. Figure 1) ont été recensés lors d'un brainstorming. Ils correspondent aux déterminants qui « à priori » expliqueront l'évolution de la sécurité de l'information au Luxembourg. Les experts ont réparti ces déterminants en 6 classes : économique, organisationnelle, socio-culturelle, législative ou réglementaire, technologique et politique.

Les participants ont recensé en priorité des déterminants en lien avec l'environnement législatif de la sécurité de l'information. Cette catégorie se détache particulièrement des autres par le nombre de déterminants recensés (11). Elle représente donc l'axe principal de changement pour le métier.

La répartition des déterminants se fait de manière homogène entre les catégories Socioculturel, technologique, organisationnel et économique avec entre 9 et 7 déterminants pour chacune d'elles.

Enfin la classe politique est la moins représentée avec seulement 3 déterminants.

Figure 1 : Liste des déterminants :

Législatif		Socioculturel	Organisationnel	Technologique	Economique	Politique
Absence d'application des sanctions sur les entreprises en raison de l'impact sur le tissu économique	Loi SOX : obligation de transparence pour les problèmes de sécurité	Augmentation des compétences et connaissances de tout utilisateur par rapport à son outil informatique et donc réduction de la fracture numérique	Prise de conscience et diffusion de l'information par le changement de service ou d'entreprise du personnel	Assurance qualité: utilisation des moyens permettant d'assurer la qualité du service mis à disposition	Connaissance des attaques de manière confidentielle dans les secteurs touchés	Absence d'une entité d'assistance (CERT)
Diffusion des informations sur les risques encourus	Le législateur luxembourgeois promeut la sécurité de l'information : <b>en punissant ceux qui y portent atteinte</b> (Sanctions pénales liées à la divulgation des données personnelles prévue pour les responsables des données à caractère personnel supérieures à celles prévues pour l'attaquant)	Evolution brutale en cas de catastrophe numérique (ex: 11 septembre)	Intégration du risk management à tous les niveaux de l'entreprise quelque soit sa taille, son secteur d'activité	Assurer l'interopérabilité des technologies à développer afin d'en améliorer la diffusion	Evolution des budgets en fonction de la conjoncture économique	Déploiement des nouvelles technologies sur l'initiative du gouvernement et des entreprises
Association des sanctions pénales en cas d'attaque subie permet de développer la SI dans les entreprises		Gain important via sensibilisation des grands et moyens acteurs, qui décline avec la taille décroissante des entreprises	Intégrer la sécurité dans le cadre d'une demande qualité	Exigence de solutions de sécurité va évoluer et les moyens technologiques et services vont devoir s'adapter	Une majorité d'entreprises n'est pas correctement sécurisée	Implication des ISP tout en respectant leur immunité
Evolution de la législation ou de la réglementation (circulaire CSSF)	Le législateur luxembourgeois promeut la sécurité de l'information : <b>en punissant ceux qui ne se sécurisent pas suffisamment</b> (Sanctions pénales liées à la divulgation des données personnelles prévues pour les responsables des données à caractère personnel supérieures à celles prévues pour l'attaquant)	La convergence: axe d'attaque commun (internet) pour des services différents et des enjeux différents	La chaîne économique en amont va imposer les procédures sécurité aux sous-traitants et partenaires économiques	La SI des grands acteurs économiques doivent prendre en compte les lacunes de sécurité provenant de leurs clients	Multiplication des attaquants en raison des profits possibles	
Peu de jurisprudence en matière de sécurité de l'information		Les Systèmes d'information et de communication (SIC) deviennent des infrastructures critiques au même titre que l'eau et l'électricité	Augmentation de la qualité des formations des personnes qui travaillent dans le domaine de la Sécurité de l'information et intégration de la veille technologique dans leur activité	Manque de réactivité et de prise de responsabilités des ISP (Internet Service Providers) au Luxembourg	Influence de la conjoncture économique sur l'application de la sécurité de l'information	
Imposer la mise en place d'un niveau de sécurité minimum dans les entreprises		La prise de conscience de l'ensemble des acteurs liés à la sécurité de l'information		Recul des liaisons câblées au profit des liaisons sans fil : augmentation des difficultés de traçage		
Relative impunité pour l'auteur de l'attaque : Pas de poursuite ou des difficultés à l'identifier et à le poursuivre (surtout à l'étranger)	Textes réglementaires mis en place sont clairs au Luxembourg mais il y a un manque de prise en charge de la part des ISP	L'Interopérabilité des technologies de la sécurité de l'Information devient un argument commercial	Augmentation des transactions en ligne	Evolution des technologies	La sécurité comme argument marketing	
		Marketing de la peur à adapter en fonction de la cible	Sensibilisation par les pouvoirs publics et les associations	Vitesse d'adaptation et de réaction: métiers, besoins et demandes évoluent	Silence des entreprises sur les attaques subies	
		Prise de consciences par l'expériences des autres	Piratage interne			

## ➤ Sélection des déterminants clés

Les dimensions recensées qui influencent la sécurité de l'information sont nombreuses et interdépendantes. C'est pourquoi, la deuxième tâche est d'identifier les plus essentielles d'entre elles, c'est-à-dire celles qui sont les plus importantes, et parmi celles-ci, les plus dominantes, c'est-à-dire celles qui sont les plus influentes et les moins dépendantes d'entre elles.

### Pré-sélection des 20 déterminants les plus importants

Les participants au groupe de travail ont réalisé des évaluations individuelles sur le critère d'importance, qui ont permis à l'équipe d'animateurs de sélectionner les 20 déterminants considérés par les experts comme les plus importants (cf. figure 2).

Figure 2 : Liste des 20 déterminants les plus importants

Liste des 20 déterminants les plus importants dans l'explication de l'évolution de la sécurité de l'information au Grand Duché du Luxembourg H : 2010.		
n°	Intitulé	Classe
1	Absence d'une entité d'assistance (CERT)	Politique
2	Assurer l'interopérabilité des technologies de la sécurité de l'information à développer afin d'en améliorer la diffusion	Technologique
3	Augmentation de la qualité des formations des personnes qui travaillent dans le domaine de la Sécurité de l'information et intégration de la veille Technologique dans leur activité	Organisationnel
4	Augmentation des compétences et connaissances de tout utilisateur par rapport à son outil informatique et donc réduction de la fracture numérique	Socio culturel
5	Connaissance des attaques de manière confidentielle dans les secteurs touchés	Economique
6	Diffusion des informations sur les risques encourus	Législatif
7	Evolution brutale en cas de catastrophe numérique (ex: 11 septembre)	Socio culturel
8	Evolution de la législation ou de la réglementation (circulaire CSSF)	Législatif
9	Evolution des budgets consacrés à la Sécurité de l'information en fonction de la conjoncture économique	Economique
10	Evolution des technologies	Technologique
11	Implication des ISP tout en respectant leur immunité	Politique
12	Imposer la mise en place d'un niveau de sécurité minimum dans les entreprises	Législatif
13	Intégration du risk management à tous les niveaux de l'entreprise quelle que soit sa taille	Organisationnel
14	Intégrer la sécurité dans le cadre d'une demande qualité	Organisationnel
15	La chaîne économique en amont va imposer les procédures sécurité aux sous-traitants et partenaires économiques	Organisationnel
16	Le législateur luxembourgeois promeut la sécurité de l'information : en punissant <b>ceux qui ne se sécurisent pas suffisamment</b>	Législatif
17	Les Systèmes d'information et de communication (SIC) deviennent des infrastructures critiques au même titre que l'eau et l'électricité	Socio culturel
18	Nécessité d'une garantie de confidentialité lors de la divulgation d'informations relatives à une attaque ou plus généralement à un risque (ajouté par le groupe d'experts lors de l'atelier 2)	Economique
19	Sensibilisation par les pouvoirs publics et les associations	Organisationnel
20	Une majorité d'entreprises n'est pas correctement sécurisée	Economique

## **Sélection des 10 déterminants essentiels**

Les relations d'influence entre les 20 déterminants les plus importants ont ensuite été évaluées par chaque expert du groupe de travail. Ces évaluations ont permis d'isoler les 10 déterminants les plus dominants, c'est-à-dire les plus influents et les moins dépendants (cf. figure 3). Ils sont vraiment essentiels dans l'explication de l'évolution de la sécurité de l'information (Analyse structurelle – Godet, 2001) et la réflexion collective doit donc se concentrer sur leurs évolutions.

**Figure 3 : Sélection des 10 déterminants les plus importants et les plus dominants**

n°	Intitulé	Classe	Description
1	Absence d'une entité d'assistance (CERT)	Politique	Absence au Luxembourg d'une entité chargée du reporting des incidents de sécurité et d'aider éventuellement à porter plainte
2	Assurer l'interopérabilité des technologies de la sécurité de l'information à développer afin d'en améliorer la diffusion	Technologique	Peu d'interopérabilité pour les technologies émergentes Importance de l'interopérabilité pour les technologies qui s'imposent lenteur des institutions qui font des normes Réticence des entreprises qui veulent imposer leur format propriétaire pour garder un avantage concurrentiel
3	Evolution brutale en cas de catastrophe numérique (ex: 11 septembre)	Socioculturel	Le GDL est fort dépendant des autres pays Impact de catastrophe important compte tenu de la dépendance vis à vis des systèmes d'information
4	Evolution de la législation ou de la réglementation	Législatif	Disposition indirecte qui impose la mise en place d'un niveau de sécurité suffisant. Cette disposition sera variable en fonction de la nature de l'information. (Actuellement seules les données personnelles sont concernées.) Il n'y a pas d'obligation universelle de sécurité (variable selon la nature de l'information) L'absence de circulaire CSSF, CAA ou d'une autre entité réglementaire est dommageable car elle peut faire évoluer la situation.
5	Evolution des technologies	Technologique	Sécurité peu prise en compte dans la conception des nouveaux logiciels Technologies évoluent plus vite que la sécurité (ex: RFID)
6	Implication des ISP tout en respectant leur immunité (titre VI De la loi du 14/08/2000 sur le commerce électronique)	Politique	Absence de contrôle a priori pour le ISP confidentialité de la sécurité des communications électroniques Peu d'implication des ISP (voire aucune) peu d'auto réglementation ou de code de conduite
7	Intégration du risk management à tous les niveaux de l'entreprise quelle que soit sa taille, son secteur d'activité	Organisationnel	L'intégration du risk Management varie en fonction des domaines d'activité, de la taille des entreprises, de leur nationalité. Grande hétérogénéité. Certains pays ont tendance à investir d'avantage dans le RM
8	Intégrer la sécurité dans le cadre d'une demande qualité	Organisationnel	Les systèmes de gestion de la sécurité utilisent les mêmes méthodes que les systèmes de gestion de la qualité Peu d'intégration entre qualité et sécurité: en émergence (ex: Bâle II, Sox, loi sur la protection des données au GDL, préconisent l'intégration qualité/sécurité
9	Les Systèmes d'information et de communication (SIC) deviennent des infrastructures critiques au même titre que l'eau et l'électricité	Socioculturel	Dans ce contexte de prise d'importance essentielle des Systèmes d'Information, la sécurité de l'information devient un élément primordial à prendre en compte et à mettre en place. Criticité relative des SIC: on peut encore se passer de la SIC
10	Sensibilisation par les pouvoirs publics et les associations	Organisationnel	La sensibilisation existe mais reste faible. Le gouvernement prend au sérieux l'importance de cette sensibilisation

## 2. L'espace morphologique

Les déterminants clés essentiels à l'évolution du système sont maintenant connus. C'est à partir de ces dix déterminants que les experts vont envisager plusieurs pistes d'évolution pour le domaine de la sécurité de l'information.

L'espace morphologique décrit le champ des futurs possibles, c'est-à-dire l'ensemble des états qui pourraient caractériser demain la situation de chaque déterminant clé.

Les experts ont formulé des idées concernant la situation actuelle aussi bien que la situation future de chaque déterminant clé (cf. Annexe 2). Cette étape fournit la base de réflexion nécessaire à la construction de l'espace morphologique. En effet, les idées caractérisant la situation actuelle sont utilisées pour fixer l'état central du futur. Il correspond au maintien en 2010 de la situation actuelle. Les idées sur la situation future sont ensuite exploitées afin de fixer plusieurs états du futur qui constituent des déviations par rapport à la situation centrale.

Cette démarche appliquée à l'ensemble des 10 déterminants clés a permis de spécifier un total de 30 états possibles du futur (cf. Appendice 2), ce qui autorise la construction de 52 488 ( $2 \times 3^8 \times 4$ ) combinaisons d'états ou scénarii exploratoires caractérisant la situation de la sécurité de l'information au Grand-Duché à l'horizon 2010.

### 3. Le scénario de compromis

Le scénario de compromis décrit le chemin ou combinatoire de compromis associant un état du futur parfois probable d'autres fois souhaitable à chaque déterminant clé. Les experts interrogés procèdent à l'élaboration des scénarii d'évolution probable et souhaitable à partir de l'espace morphologique, pour ensuite sélectionner le scénario unique de compromis.

#### ➤ Sélection du scénario probable

Le scénario d'évolution probable décrit la combinaison d'états probables du futur pour les 10 déterminants essentiels. Il est donc constitué des hypothèses d'évolution les plus probables. C'est le scénario qui, selon les experts, a le plus de chances de se réaliser à l'horizon 2010.

Pour cela, les experts ont apprécié individuellement le degré de réalisation<sup>3</sup> des différentes hypothèses d'évolution. Pour chaque déterminant, l'hypothèse considérée comme la plus probable par le groupe de travail a ainsi pu être sélectionnée par l'équipe d'animateurs. La combinaison des 10 états sélectionnés constitue le scénario d'évolution probable des facteurs pour l'horizon 2010 (cf. figure 4 et Appendice 2).

L'analyse montre qu'aucun état probable ne correspond à une situation dégradée en 2010 par rapport à la situation actuelle. La plupart des états probables sélectionnés décrivent une situation d'amélioration. Comme aucun état probable ne correspond à une situation dégradée par rapport à la situation actuelle, les experts ont, « a priori », une vision optimiste du futur. Cependant, à 2 reprises, l'évolution probable correspond à une situation d'inertie par rapport à la situation actuelle.

---

<sup>3</sup> Les experts répondent à la question : « Pouvez-vous indiquer pour chacune des évolutions le degré de probabilité pour que celle-ci se réalise à l'horizon 2010 ? ». L'échelle de notation à utiliser est : 1- Très peu probable, 2 - Peu probable, 3 - Probable, 4 - Très probable.

**Figure 4 : Scénario d'évolution probable de la Sécurité de l'information**

## Scénario d'évolution probable

Intitulés des déterminants	Hypothèses d'évolution
Absence d'une entité d'assistance (CERT)	En 2010, émergence d'une entité d'assistance (CERT) au GDL.
Implication des Internet Service Provider (ISP) ou Fournisseurs d'Accès Internet (FAI) tout en respectant leur immunité (titre VI De la loi du 14/08/2000 sur le commerce électronique)	En 2010 les pouvoirs publics et /ou l'existence d'une jurisprudence impliqueront les ISP dans la Sécurité de l'information.
Evolution brutale en cas de catastrophe numérique (ex: 11 septembre)	En 2010, l'impact d'éventuelles catastrophes numériques restera important en raison de la dépendance du GDL par rapport aux systèmes d'informations.
Assurer l'interopérabilité des technologies de la sécurité de l'information à développer afin d'en améliorer la diffusion	En 2010, en l'absence de normalisation, il n'y aura que des standards de fait qui s'imposeront via des technologies qui auront un certain degré de maturité
Evolution des technologies (prise en compte des problématiques sécurité)	En 2010, il y aura une prise en compte de la sécurité lors de la conception des technologies. (Privacy Enhanced Technology).
Les Systèmes d'information et de communication (SIC) deviennent des infrastructures critiques au même titre que l'eau et l'électricité	En 2010 la criticité des SIC sera de plus en plus importante au même titre que des ressources primaires (eau électricité) : forte dépendance de la part des entreprises/organisations vis à vis des SIC
Intégrer la sécurité dans le cadre d'une demande qualité	En 2010, il y aura une émergence de l'intégration qualité/sécurité grâce à des initiatives gouvernementales. (ex : Bâle II, SOX, loi sur la protection des données au GDL)
Intégration du risk management à tous les niveaux de l'entreprise quelle que soit sa taille, son secteur d'activité	En 2010 l'intégration du Risk Management sera plus homogène grâce à la promotion du RM et à la prise de conscience des entreprises.
Sensibilisation par les pouvoirs publics et les associations aux risques en matière de Sécurité de l'Information	En 2010, les pouvoirs publics et les associations intensifieront la sensibilisation à la SI. (multiplication des cibles)
Evolution de la législation ou de la réglementation : imposer la mise en place d'un niveau de sécurité minimum dans les entreprises	En 2010, les autorités compétences (administratives et/ou réglementaires) imposeront la mise en place d'un niveau de sécurité minimum et/ou certaines règles de sécurité aux entreprises de certains secteurs (exemple du secteur financier qui un secteur régulé)

➤ Sélection du scénario d'évolution souhaitable

Le scénario d'évolution souhaitable décrit la combinaison d'états souhaitables du futur pour les 10 déterminants essentiels. Il est constitué des hypothèses d'évolution les plus souhaitables au développement de la sécurité de l'information.

Les experts ont évalué individuellement leur degré de préférence<sup>4</sup> vis-à-vis de la réalisation des différentes hypothèses d'évolution. L'analyse des évaluations permet la sélection d'un état souhaitable du futur par facteur. La juxtaposition des états sélectionnés correspond au scénario d'évolution souhaitable des déterminants pour l'horizon 2010 (cf. Tableau 5 et Appendice 2).

Au niveau de ce scénario, il est utile de noter l'envie d'évoluer et la volonté collective d'améliorer la situation actuelle. En effet, aucun état du futur caractérisant l'inertie demain vis-à-vis de la situation actuelle n'est perçue comme souhaitable par le collectif d'experts. Dans tous les cas, l'hypothèse d'évolution souhaitable correspond à une situation d'amélioration voire d'amélioration extrême. Trois états sont caractérisés par la convergence entre probable et souhaitable. Ces 3 hypothèses retenues correspondent à des états d'amélioration ou d'améliorations extrêmes ce qui traduit une véritable volonté d'améliorer la situation accompagnée d'une mise en évidence de la tendance actuelle en ce qui concerne ces 2 déterminants. (Evolution des technologies et al sensibilisation des pouvoirs publics et des associations)

---

<sup>4</sup> Les experts répondent à la question : « Pouvez-vous indiquer pour chacune des évolutions à quel degré vous souhaitez que celle-ci se réalise ? ». L'échelle de notation à utiliser est : 1- Très peu souhaitable, 2 - Peu souhaitable, 3 - Souhaitable, 4 - Très souhaitable.

**Figure 5 : Scénario d'évolution souhaitable de la Sécurité de l'information**

## Scénario d'évolution souhaitable

Intitulés des déterminants	Hypothèses d'évolution
Absence d'une entité d'assistance (CERT)	En 2010, un CERT sera l'interlocuteur privilégié des acteurs de la SI au GDL.
Implication des Internet Service Provider (ISP) ou Fournisseurs d'Accès Internet (FAI) tout en respectant leur immunité (titre VI De la loi du 14/08/2000 sur le commerce électronique)	En 2010 l'auto régulation et la mise en place de codes de conduite va impliquer les ISP dans la sécurité de l'information.
Evolution brutale en cas de catastrophe numérique (ex: 11 septembre)	En 2010, l'impact d'éventuelles catastrophes numériques sera réduit grâce à une amélioration de l'analyse des risques et de la gestion des crises. (multiplication des procédures et des tests de fiabilité des systèmes, redondances des moyens informatiques)
Assurer l'interopérabilité des technologies de la sécurité de l'information à développer afin d'en améliorer la diffusion	En 2010 la normalisation internationale et/ou l'open source favorisera(ont) la mise en place et l'usage de standards.
Evolution des technologies (prise en compte des problématiques sécurité)	En 2010, il y aura une prise en compte de la sécurité dès la phase de conception des technologies. (Privacy Enhanced Technology).
Les Systèmes d'information et de communication (SIC) deviennent des infrastructures critiques au même titre que l'eau et l'électricité	En 2010 la criticité des SIC sera de plus en plus importante au même titre que des ressources primaires(eau électricité) : forte dépendance de la part des entreprises/organisations vis à vis des SIC
Intégrer la sécurité dans le cadre d'une demande qualité	En 2010, il y aura une convergence de la qualité/sécurité grâce à l'intégration de la sécurité dans les normes qualité. (ISO)
Intégration du risk management à tous les niveaux de l'entreprise quelle que soit sa taille, son secteur d'activité	En 2010, l'intégration du risk management se fera de manière généralisé dans les entreprises via l'apparition de normes internationales
Sensibilisation par les pouvoirs publics et les associations aux risques en matière de Sécurité de l'Information	En 2010, les pouvoirs publics et les associations intensifieront la sensibilisation à la SI. (multiplication des cibles)
Evolution de la législation ou de la réglementation : imposer la mise en place d'un niveau de sécurité minimum dans les entreprises	En 2010, la législation imposera un niveau de sécurité minimum global aux entreprises tout en préservant compétitivité économique du GDL.

➤ Construction du scénario d'évolution de compromis

Enfin, experts du groupe de travail confrontent les scénarii probable et souhaitable dans l'objectif d'élaborer un scénario unique : le scénario de compromis (cf. figure 6). Il décrit une combinaison associant un état du futur soit probable soit souhaitable à chaque déterminant clé. En effet, maintenant que le groupe de travail sait différencier ce qui a la plus grande probabilité de se produire (scénario probable) de ce qu'il désire (scénario souhaitable), il devient possible de procéder à un arbitrage entre les deux situations pour retenir une unique hypothèse d'évolution par déterminant.

Le scénario de compromis de la sécurité de l'information reflète la convergence entre le probable et le souhaitable dans 3 situations. Dans ce cas, l'évolution la plus bénéfique au domaine de la sécurité de l'information est aussi celle qui, selon les experts, a le plus de chances de se réaliser. La question du choix ne se pose donc pas, puisqu'il n'y a pas d'écart entre l'état du futur probable et l'état du futur souhaitable. Ainsi, les experts pressentent qu'en 2010 il y aura une prise en compte de la sécurité des la phase de conception des technologies. (Privacy Enhanced Technology). Traduisant une tendance actuelle à la prise en compte de la sécurité en amont ce qui permettra d'améliorer le niveau global de la sécurité de l'information. Il est également envisagé qu'en 2010 la criticité des SIC sera de plus en plus importante au même titre que des ressources primaires(eau électricité) : forte dépendance de la part des entreprises/organisation vis à vis des SIC. Ainsi les experts expriment leur préoccupation quant à la protection des SIC et s'inscrivent dans une démarche pré active en identifiant les moyens et les actions permettant de se préparer en cas de crises éventuelles. Enfin les experts ont identifié une implication grandissante des pouvoirs publics et les associations qui devraient intensifier la sensibilisation à la SI d'ici à 2010. (multiplication des cibles)

Lorsqu'un décalage entre probable et souhaitable est observé pour un déterminant, l'état probable du futur est retenu si le collectif d'experts juge qu'il ne dispose pas d'une marge d'actions suffisante avant 2010 pour atteindre l'état souhaitable. L'examen du scénario de compromis montre que cette propriété caractérise une seule situation. Ainsi les experts estiment qu'il est probable que d'ici 2010 le GDL connaisse l'émergence d'une entité d'assistance (CERT). Il faut noter que la création d'un CERT est fortement souhaitée par les experts mais que sa mise en place reste complexe compte tenu de l'horizon de temps donné.

Il est aussi identifié qu'en 2010, en l'absence de normalisation, il n'y aura que des standards de fait qui s'imposeront via des technologies qui auront un certain degré de maturité. Cette hypothèse d'évolution est assez révélatrice d'une certaine inertie et de l'absence de prise, sur la mise en place de normes concernant la sécurité de l'information.

Il est également identifié qu'en 2010 l'intégration du Risk Management sera plus homogène grâce à la promotion du RM et à la prise de conscience des entreprises. Il est improbable que le RM soit imposé aux travers de normes internationales au sein des entreprises. Par conséquent des actions à l'échelle nationales devront être envisagées. Cette évolution met en évidence la une connaissance de l'importance du Risk management de la part des professionnels de la sécurité de l'information et surtout une volonté de le déployer dans les entreprises.

Enfin 2010, les autorités administratives et réglementaires imposeront la mise en place d'un niveau de sécurité minimum et/ou certaines règles de sécurité aux entreprises de certains secteurs (ex: secteur financier) secteurs régulés

La mise en place d'un niveau de sécurité minimum ne pourra pas se faire pour l'ensemble des entreprises au GDL et se limitera à des secteurs sensibles uniquement.

Figure 6 : Scénario de compromis de la Sécurité de l'information

Scénario de Compromis	
Déterminants retenus	Hypothèses
Absence d'une entité d'assistance (CERT)	En 2010, émergence d'une entité d'assistance (CERT) au GDL. <b>(Probable)</b>
Implication des Internet Service Provider (ISP) ou Fournisseurs d'Accès Internet (FAI) tout en respectant leur immunité (titre VI De la loi du 14/08/2000 sur le commerce électronique)	En 2010 l'auto régulation et la mise en place de codes de conduite va impliquer les ISP dans la sécurité de l'information. <b>(Souhaitable)</b>
Evolution brutale en cas de catastrophe numérique (ex: 11 septembre)	En 2010, l'impact d'éventuelles catastrophes numériques sera réduit grâce à une amélioration de l'analyse des risques et de la gestion des crises. (multiplication des procédures et des tests de fiabilité des systèmes, redondance des moyens informatiques) <b>(Souhaitable)</b>
Assurer l'interopérabilité des technologies de la sécurité de l'information à développer afin d'en améliorer la diffusion	En 2010, en l'absence de normalisation, il n'y aura que des standards de fait qui s'imposeront via des technologies qui auront un certain degré de maturité <b>(Probable)</b>
Evolution des technologies (prise en compte des problématiques sécurité)	En 2010, il y aura une prise en compte de la sécurité des la phase de conception des technologies. (Privacy Enhanced Technology). <b>(Probable=Souhaitable)</b>
Les Systèmes d'information et de communication (SIC) deviennent des infrastructures critiques au même titre que l'eau et l'électricité	En 2010 la criticité des SIC sera de plus en plus importante au même titre que des ressources primaires(eau électricité) : forte dépendance des organisations/entreprises vis à vis des SIC <b>(Probable=Souhaitable)</b>
Intégrer la sécurité dans le cadre d'une demande qualité	En 2010, il y aura une convergence de la qualité/sécurité grâce à l'intégration de la sécurité dans les normes qualité. (ISO) <b>(Souhaitable)</b>
Intégration du risk management à tous les niveaux de l'entreprise quelle que soit sa taille, son secteur d'activité	En 2010 l'intégration du Risk Management sera plus homogène grâce à la promotion du RM et à la prise de conscience des entreprises. <b>(Probable)</b>
Sensibilisation par les pouvoirs publics et les associations	En 2010, les pouvoirs publics et les associations intensifieront la sensibilisation à la SI. (multiplication des cibles) <b>(Probable=Souhaitable)</b>
<b>Evolution de la législation ou de la réglementation : imposer la mise en place d'un niveau sécurité de minimum dans les entreprises</b>	En 2010, les autorités compétences (administratives et/ou réglementaires) imposeront la mise en place d'un niveau de sécurité minimum et/ou certaines règles de sécurité aux entreprises de certains secteurs (exemple du secteur financier qui un secteur régulé). <b>(Probable)</b>

## Le plan d'actions

Le scénario d'évolution de compromis correspond au choix par les experts d'une trajectoire d'évolution unique de moyen terme. Il convient maintenant de réfléchir aux actions qui permettront soit de se préparer face à, soit de pro-agir pour la réalisation de cette trajectoire. Pour chaque type d'évolution associée au scénario de compromis, le groupe de travail a donc proposé une série d'actions.

F1 - ABSENCE D'UNE ENTITÉ D'ASSISTANCE (CERT)	
Etat du futur Probable	Actions de préparation à la réalisation d'une situation d'amélioration
En 2010, émergence d'une entité d'assistance (CERT) au GDL.	<ol style="list-style-type: none"> <li>1. D'ici 2007 : création d'un CERT national grâce à la volonté politique, financements publics nécessaires.</li> <li>2. Proposer aux entreprises de collaborer</li> <li>3. Les pouvoirs publics peuvent imposer une collaboration des entreprises</li> <li>4. Un organisme de type CERT pourrait être imposé pour récolter des informations auprès des entreprises</li> <li>5. L'anonymat et la confidentialité assurée par les pouvoirs publics faciliteraient le volontariat</li> <li>6. Les pouvoirs publics doivent exiger la récolte des informations pour les infrastructures critiques: énergie, transport, alimentation, télécommunications, santé, place financière</li> <li>7. CERT doit apporter une haute valeur ajoutée en diffusant de l'information.</li> <li>8. Veille sécurité, sensibilisation des entreprises</li> <li>9. Echanges internationaux et échanges avec d'autres CERT</li> <li>10. Le volontariat des entreprises pour collaborer avec le CERT dépend largement de sa capacité à "gagner leur confiance"</li> <li>11. 2007 : Création d'un Gov CERT</li> <li>12. Avant 2010 : CIP(Critical Infrastructure Protection) CERT</li> <li>13. Au delà d'un CERT.lu : le CERT devient l'interlocuteur privilégié des acteurs de la SI.</li> </ol>

(ligne 1 – description du facteur ; colonne 1 - Etat du futur retenu ; colonne 2 - actions formulées)

**F2 - IMPLICATION DES ISP TOUT EN RESPECTANT LEUR IMMUNITÉ (TITRE VI DE LA LOI DU 14/08/2000 SUR LE COMMERCE ÉLECTRONIQUE)**

<b>Etat du futur Souhaitable</b>	<b>Actions pro-actives pour la réalisation d'une situation améliorée et souhaitée</b>
<p>En 2010 l'auto régulation et la mise en place de codes de conduite va impliquer les ISP dans la sécurité de l'information.</p>	<ol style="list-style-type: none"> <li>1. L'implication doit venir de manière volontaire de la part des ISP ou des organisations représentatives telles que l'ISPA(International Service Provider Association), APSI (Association des professionnels de la Société de l'Information)</li> <li>2. Intervention de l'ILR(Institut Luxembourgeois de Régulation) ou des pouvoirs publics.</li> <li>3. Pression de l'opinion publique, (pression économique) en raison d'une dégradation de l'image d'Internet.</li> <li>4. Changement du cadre législatif :</li> <li>5. Dans un premier temps, changement du cadre communautaire. (ex législation du RU dans le cadre des télécommunications, RIP ACT 2000)</li> <li>6. Statut des ISP pour leur permettre de collaborer dans les actions de sécurité de l'information. L'immunité ne pourra être respectée que si une directive européenne est mise en place.</li> </ol>

**F3 - ÉVOLUTION BRUTALE EN CAS DE CATASTROPHE NUMÉRIQUE (EX: 11 SEPTEMBRE)**

<b>Etat du futur Souhaitable</b>	<b>Actions pro-actives pour la réalisation d'une situation améliorée et souhaitée</b>
<p>En 2010, l'impact d'éventuelles catastrophes numériques sera réduit grâce à une amélioration de l'analyse des risques et de la gestion des crises. (multiplication des procédures et des tests de fiabilité des systèmes, redondance des moyens informatiques)</p>	<ol style="list-style-type: none"> <li>1. Harmoniser l'approche de l'analyse des risques</li> <li>2. Harmoniser le vocabulaire sécurité</li> <li>3. Diffuser les procédures de communication en temps de crise (comment communiquer)</li> <li>4. Identifier les acteurs, les opérateurs des infrastructures critiques à joindre en cas de crise :mise en place d'un BCP (Business continuity plan) national</li> <li>5. l'occurrence d'une catastrophe numérique de grande ampleur permettrait une prise de conscience immédiate des acteurs de la SI</li> <li>6. Sur l'initiative du HCPN (Haut Commissariat à la Protection Nationale) il faudra faire un état des lieux national (cf. harmonisation de l'analyse des risques) : Reporting des incidents, menaces, vulnérabilité, probabilité, impact.</li> <li>7. Identification des services primordiaux à mettre en place prioritairement (procédures BCP)</li> <li>8. Identification des services primordiaux à remettre en place prioritairement en cas de catastrophe. (idée de mettre en réserve pour pouvoir relancer la machine)</li> </ol>

F4 - ASSURER L'INTEROPÉRABILITÉ DES TECHNOLOGIES DE LA SÉCURITÉ DE L'INFORMATION À DÉVELOPPER AFIN D'EN AMÉLIORER LA DIFFUSION	
Etat du futur Probable	Actions de préparation à la réalisation d'une situation d'inertie
En 2010, en l'absence de normalisation, il n'y aura que des standards de fait qui s'imposeront via des technologies qui auront un certain degré de maturité	<ol style="list-style-type: none"> <li>1. Promouvoir l'usage de standard</li> <li>2. Sensibilisation des acteurs majeurs de l'industrie (clients et surtout les fournisseurs)</li> </ol>

F5 - ÉVOLUTION DES TECHNOLOGIES	
Etat du futur probable et souhaitable	Actions de préparation pour la réalisation d'une situation attendue et souhaitée
En 2010, il y aura une prise en compte de la sécurité dès la phase de conception des technologies. (Privacy Enhanced Technology).	<ol style="list-style-type: none"> <li>1. Formation des personnes chargées du développement des technologies.</li> <li>2. Identification des risques et prise en compte dans le cahier des charges</li> <li>3. Suivi, maintenance et mise à jour après le lancement du produit ou de la technologie.</li> <li>4. Sensibilisation à l'intégration / Prise en compte de standard de sécurité dans le cycle de développement</li> </ol>

F6 - LES SYSTÈMES D'INFORMATION ET DE COMMUNICATION (SIC) DEVIENNENT DES INFRASTRUCTURES CRITIQUES AU MÊME TITRE QUE L'EAU ET L'ÉLECTRICITÉ	
Etat du futur probable et souhaitable	Actions de préparation pour la réalisation d'une situation attendue et souhaitée
En 2010 la criticité des SIC sera de plus en plus importante au même titre que des ressources primaires(eau électricité) : forte dépendance des organisations/entreprises vis à vis des SIC	<ol style="list-style-type: none"> <li>1. Formation ou sensibilisation des personnes</li> <li>2. Créer des redondances, des sites secondaires (dans une optique de remplacement)</li> <li>3. Mise en place de contrôle de l'état des systèmes (monitoring, intégration d'exigences de qualité)</li> <li>4. Garantir la sécurité physique des infrastructures</li> <li>5. Préconiser la certification selon la norme ISO 27001</li> </ol>

F7 - INTÉGRER LA SÉCURITÉ DANS LE CADRE D'UNE DEMANDE QUALITÉ	
Etat du futur Souhaitable	Actions pro-actives pour la réalisation d'une situation améliorée et souhaitée
En 2010, il y aura une convergence de la qualité/sécurité grâce à l'intégration de la sécurité dans les normes qualité. (ISO)	<ol style="list-style-type: none"> <li>1. Participer à la normalisation et préconiser la certification.</li> <li>2. Le Luxembourg appartient au SC(sous-comité) 27 : Il devra y participer en favorisant la prise en compte ou l'intégration de la sécurité dans les normes ISO</li> </ol>

F8 - INTÉGRATION DU RISK MANAGEMENT À TOUS LES NIVEAUX DE L'ENTREPRISE QUELLE QUE SOIT SA TAILLE, SON SECTEUR D'ACTIVITE	
Etat du futur Probable	Actions de préparation à la réalisation d'une situation d'inertie
En 2010 l'intégration du Risk Management sera plus homogène grâce à sa promotion et à la prise de conscience des entreprises.	<ol style="list-style-type: none"> <li>1. Pour les secteurs régulés, les régulateurs peuvent imposer la mise en place du risk management et certains modes de gestion du risk management.</li> <li>2. Promouvoir des standards spécifiques</li> <li>3. Formation : intégrer le Risk management dans les formations</li> <li>4. L'amont de la chaîne économique va imposer l'intégration de Règles spécifiques en RM aux sous traitants</li> <li>5. Donc en découle une professionnalisation croissante de l'organisation des entreprises</li> </ol>

F9 - SENSIBILISATION PAR LES POUVOIRS PUBLICS ET LES ASSOCIATIONS	
Etat du futur Souhaitable	Actions pro-actives pour la réalisation d'une situation améliorée et souhaitée
En 2010, les pouvoirs publics et les associations intensifieront la sensibilisation à la SI. (multiplication des cibles)	<ol style="list-style-type: none"> <li>1. Volonté politique</li> <li>2. Financements publics</li> <li>3. Formation --&gt; intégration de la SI dans toutes les formations professionnelles voire même scolaires</li> <li>4. Sensibilisation aux risques et à la criminalité informatique (conséquences)</li> <li>5. Intensifier les initiatives existantes</li> <li>6. Relancer et promouvoir la certification: e-privacy, e-commerce certified</li> </ol>

F10 - EVOLUTION DE LA LÉGISLATION OU DE LA RÉGLEMENTATION	
Etat du futur Probable	Actions de préparation à la réalisation d'une situation d'inertie
<p>En 2010, les autorités compétentes (administratives et réglementaires) imposeront la mise en place d'un niveau de sécurité minimum et/ou certaines règles de sécurité aux entreprises de certains secteurs (exemple du secteur financier qui est un secteur régulé)</p>	<ol style="list-style-type: none"> <li>1. Pas possible d'imposer une sécurité technique minimum (pas technique)</li> <li>2. Réforme de la loi qui régit la sécurité nationale prévoit certains éléments adaptés</li> <li>3. Le niveau de sécurité minimum peut-être un argument de compétitivité</li> <li>4. Rôle incitateur des régulateurs et des pouvoirs publics en général pour promouvoir ces dispositions réglementaires</li> <li>5. Influence de normes internationales qui imposeraient la mise en place de niveau minimal de sécurité</li> <li>6. Groupes de travail internationaux (commission européenne, ISO, IETF, ETSI)</li> <li>7. Certains opérateurs privés, associations privées (VISA, Mastercard qui imposent des règles qui ont des valeurs quasi réglementaires (PCI)</li> <li>8. Le poids de ces groupes de travail ou de ces opérateurs privés engendre une réglementation de fait</li> </ol>

Les actions recensées couvrent un éventail très large en termes d'application allant de l'implication de nouveaux acteurs ou la montée en puissance d'autres, la sensibilisation/formations ou des modifications législatives et normatives à entreprendre.

Ainsi il a été identifié des actions de formation auprès des professionnels de la sécurité mais également auprès du grand public et notamment une volonté de formation plus proche de la sensibilisation auprès des jeunes en ce qui concerne les risques associés à la SI.

La sensibilisation est un élément essentiel en ce qui concerne les actions d'améliorations qui doivent être menées. Les experts ont déclaré que la sécurité de l'information peut être affectée par une méconnaissance des utilisateurs et pourrait donc être améliorée par une meilleure sensibilisation des utilisateurs en ce qui concerne les enjeux de la sécurité. Il est préconisé de mettre en place des actions de sensibilisation pour le grand public, les entreprises. Ces actions pourront se faire ou être favorisée par une implication accrue des pouvoirs publics, des associations ou de la législation.

Ce qui nous amène à une autre thématique d'actions à mettre en place qui concerne la mise en place d'un réseau.

Les experts interrogés ont déclaré le caractère essentiel du développement d'un réseau et la mobilisation d'un ensemble d'acteurs concernés par la sécurité de l'information. Cela se matérialise par l'implication des autorités de régulation des pouvoirs publics et des associations dans des actions de sensibilisation, dans la mise en place de normes et de standards, l'implication des autorités la création d'un Computer Emergency Response Team qui serait amené dans les années qui viennent à devenir l'interlocuteur privilégié des acteurs de la sécurité de l'information. Cette implication servirait également à favoriser la collaboration des Internet Service Providers(ISP) et des entreprises dans le reporting et le suivi des incidents.

Dans le cas des normes et de la législation, les associations et les autorités de régulation sont identifiées comme les interlocuteurs à impliquer prioritairement.

Certains groupes de travail internationaux ou opérateurs privés(ex : Payment Card Industry - Data Security Standard) peuvent également imposer des standards améliorant la sécurité de l'information.

Une autre source d'amélioration de la sécurité serait l'intégration de pratiques tel le risk management.

## Conclusion

La réflexion prospective menée par le groupe d'experts de la sécurité de l'information a abouti à la spécification d'un scénario unique d'anticipation des changements essentiels auxquels pourraient être confrontés d'ici à 2010 les professionnels de ce domaine et à la formulation d'un plan d'actions favorisant ou permettant de faire face à sa réalisation. Les actions recensées constituent une véritable base de réflexion pour la définition d'une stratégie à moyen terme pour le développement de la sécurité de l'information au Grand-Duché du Luxembourg à horizon 2010.

Ainsi des actions de formation et de sensibilisation des professionnels et du grand public permettraient d'améliorer le niveau de sécurité de l'information en amont. Ces démarches reposent sur une implication des autorités de régulations, des associations et des pouvoirs publics qui pourront favoriser la mise en place de ces actions. L'implication de ces acteurs interviendrait également en termes de législation, de normes et surtout dans la mise en place d'un CERT au Luxembourg.

Les opérateurs privés (entreprises, Internet Services Providers...) pourront également être à la base d'améliorations en termes de standards (Payment Card Industry-Data Security Standard), de contribution au reporting et de suivi des incidents.

Enfin des actions de préparation devront être entreprises dans les années à venir afin d'améliorer la gestion des crises (identification et création en doublons des infrastructures critiques)

Cette réflexion, montre que la sécurité de l'information est considérée comme étant une thématique particulièrement essentielle pour l'activité économique du Grand Duché du Luxembourg. Il a également été mis en évidence une véritable volonté des acteurs de la sécurité de l'information d'améliorer la situation surtout d'impliquer les autorités de régulation, les pouvoirs publics nationaux et surtout de s'ouvrir à l'international en termes de standards, d'implication et de participation à des groupes de travaux (commission européenne, ISO, IETF, ETSI) et d'intégration des best practices.

## Annexes

### Annexe 1 : Liste des déterminants de l'évolution de la sécurité de l'information 1/2

Liste des déterminants de l'évolution de la sécurité de l'information au Grand Duché du Luxembourg H : 2010.		
n°	Intitulé	Classe
10	Connaissance des attaques de manière confidentielle dans les secteurs touchés	Economique
15	Evolution des budgets en fonction de la conjoncture économique	Economique
20	Influence de la conjoncture économique sur l'application de la sécurité de l'information	Economique
25	La sécurité comme argument marketing	Economique
34	Multiplication des attaquants en raison des profits possibles	Economique
43	Silence des entreprises sur les attaques subies	Economique
45	Une majorité d'entreprises n'est pas correctement sécurisée	Economique
1	Absence d'application des sanctions sur les entreprises en raison de l'impact sur le tissu économique	Législative
3	Association des sanctions pénales en cas d'attaque subie permet de développer la SI dans les entreprises	Législative
12	Diffusion des informations sur les risques encourus	Législative
14	Evolution de la législation ou de la réglementation (circulaire CSSF)	Législative
19	Imposer la mise en place d'un niveau de sécurité minimum dans les entreprises	Législative
27	Le législateur luxembourgeois promeut la sécurité de l'information : en punissant <b>ceux qui ne se sécurisent pas suffisamment</b> (Sanctions pénales liées à la divulgation des données personnelles prévue pour les responsables des données à caractère personnel supérieures à celles prévues pour l'attaquant)	Législative
28	Le législateur luxembourgeois promeut la sécurité de l'information : en punissant <b>ceux qui y portent atteinte</b> (Sanctions pénales liées à la divulgation des données personnelles prévue pour les responsables des données à caractère personnel supérieures à celles prévues pour l'attaquant)	Législative
31	Loi SOX : obligation de transparence pour les problèmes de sécurité	Législative
35	Peu de jurisprudence en matière de sécurité de l'information	Législative
41	Relative impunité pour l'auteur de l'attaque : Pas de poursuite ou des difficultés à l'identifier et à le poursuivre (surtout à l'étranger)	Législative
44	Textes réglementaires mis en place sont clairs au Luxembourg mais il y a un manque de prise en charge de la part des ISP	Législative
6	Augmentation de la qualité des formations des personnes qui travaillent dans le domaine de la Sécurité de l'information et intégration de la veille technologique dans leur activité	Organisationnelle
8	Augmentation des transactions en ligne	Organisationnelle
21	Intégration du risk management à tous les niveaux de l'entreprise quelque soit sa taille	Organisationnelle
22	Intégrer la sécurité dans le cadre d'une demande qualité	Organisationnelle
23	La chaîne économique en amont va imposer les procédures sécurité aux sous-traitants et partenaires économiques	Organisationnelle
36	Piratage interne	Organisationnelle
37	Prise de conscience et diffusion de l'information par le changement de service ou d'entreprise du personnel	Organisationnelle
42	Sensibilisation par les pouvoirs publics et les associations	Organisationnelle
2	Absence d'une entité d'assistance (CERT)	Politique

## Annexe 1 : Liste des déterminants de l'évolution de la sécurité de l'information 2/2

Liste des déterminants de l'évolution de la sécurité de l'information au Grand Duché du Luxembourg H : 2010.		
n°	Intitulé	Classe
11	Déploiement des nouvelles technologies à l'initiative du gouvernement et des entreprises	Politique
18	Implication des ISP tout en respectant leur immunité	Politique
7	Augmentation des compétences et connaissances de tout utilisateur par rapport à son outil informatique et donc réduction la fracture numérique	Socioculturelle
13	Evolution brutale en cas de catastrophe numérique (ex: 11 septembre)	Socioculturelle
17	Gain important via sensibilisation des grands et moyens acteurs qui décline avec la taille décroissante des entreprises	Socioculturelle
24	La convergence: axe d'attaque commun (internet) pour des services différents et des enjeux différents	Socioculturelle
29	Les Systèmes d'information et de communication (SIC) deviennent des infrastructures critiques au même titre que l'eau et l'électricité	Socioculturelle
30	L'Interopérabilité des technologies de la sécurité de l'Information devient un argument commercial	Socioculturelle
33	Marketing de la peur à adapter en fonction de la cible	Socioculturelle
38	La prise de conscience de l'ensemble des acteurs liés à la sécurité de l'information	Socioculturelle
39	Prise de consciences par l'expériences des autres	Socioculturelle
4	Assurance qualité: utilisation des moyens permettant d'assurer la qualité du service mis à disposition	Technologique
5	Assurer l'intéropérabilité des technologies à développer afin d'en améliorer la diffusion	Technologique
9	Exigence de solutions de sécurité va évoluer et les moyens technologiques et services vont devoir s'adapter	Technologique
16	Evolution des technologies	Technologique
26	La SI des grands acteurs économiques doivent prendre en compte les lacunes de sécurité provenant de leurs clients	Technologique
32	Manque de réactivité et de prise de responsabilités des ISP (Internet Service Providers) au Luxembourg	Technologique
40	Recul des liaisons câblées au profit des liaisons sans fil : augmentation des difficultés de traçage	Technologique
46	Vitesse d'adaptation et réaction: métiers, besoins et demandes évoluent	Technologique

## Annexe 2 : Espace morphologique de la sécurité de l'information 1/3

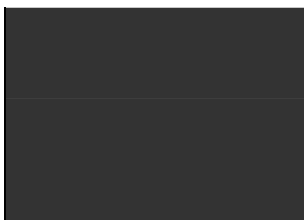
### Espace Morphologique : Sécurité de l'Information H : 2010

Déterminant	Hypothèses d'évolution			
	A	B	C	D
<b>Absence d'une entité d'assistance (CERT)</b>	En 2010 il n'y aura pas d'entité d'assistance (CERT) au Grand Duché du Luxembourg.	En 2010, émergence d'une entité d'assistance (CERT) au GDL.	En 2010, un CERT sera l'interlocuteur privilégié des acteurs de la SI au GDL.	
<b>Implication des Internet Service Provider (ISP) ou Fournisseurs d'Accès Internet (FAI) tout en respectant leur immunité (titre VI De la loi du 14/08/2000 sur le commerce électronique)</b>	En 2010 l'implication des ISP dans la Sécurité de l'information et dans le contrôle des sources d'information restera faible.	En 2010 les pouvoirs publics et /ou l'existence d'une jurisprudence impliqueront les ISP dans la Sécurité de l'information.	En 2010 l'auto régulation et la mise en place de codes de conduite va impliquer les ISP dans la sécurité de l'information.	
<b>Evolution brutale en cas de catastrophe numérique (ex: 11 septembre)</b>	En 2010, l'impact d'éventuelles catastrophes numériques va s'aggraver en raison d'une augmentation de la dépendance du GDL par rapport aux systèmes d'informations (statut d'infrastructure primaire) et de la multiplication et la complexification des points attaquables.	En 2010, l'impact d'éventuelles catastrophes numériques restera important en raison de la dépendance du GDL par rapport aux systèmes d'informations.	En 2010, l'impact d'éventuelles catastrophes numériques sera réduit grâce à une amélioration de l'analyse des risques et de la gestion des crises. (multiplication des procédures et des tests de fiabilité des systèmes, redondance des moyens informatiques)	

## Annexe 2 : Espace morphologique de la sécurité de l'information 2/3

### Espace Morphologique : Sécurité de l'Information H : 2010

Déterminant	Hypothèses d'évolution			
	A	B	C	D
<b>Assurer l'interopérabilité des technologies de la sécurité de l'information à développer afin d'en améliorer la diffusion</b>	En 2010 la préservation par les entreprises de leur avantage concurrentiel sera un frein à l'interopérabilité des technologies à développer.	En 2010, en l'absence de normalisation, il n'y aura que des standards de fait qui s'imposeront via des technologies qui auront un certain degré de maturité	En 2010 la normalisation internationale et/ou l'open source favorisera(ont) la mise en place et l'usage de standards.	
<b>Evolution des technologies</b>		En 2010 la sécurité sera peu prise en compte dans la conception des technologies. (ex : nouveaux logiciels)	En 2010, il y aura une prise en compte de la sécurité des technologies. (Privacy Enhanced Technology).	En 2010, la sécurité sera prise en compte dans les logiciels développés mais sera freinée par la protection de la vie privée.
<b>Les Systèmes d'information et de communication (SIC) deviennent des infrastructures critiques au même titre que l'eau et l'électricité</b>		En 2010 les SIC garderons un niveau de criticité relatif : on pourra encore se passer des SIC.	En 2010 la criticité des SIC sera de plus en plus importante au même titre que des ressources primaires(eau électricité) : forte dépendance des organisations/entreprises vis à vis des SIC	

<p><b>Intégrer la sécurité dans le cadre d'une demande qualité</b></p>	<p>En 2010, l'intégration qualité/sécurité restera marginale.</p>	<p>En 2010, il y aura une émergence de l'intégration qualité/sécurité grâce à des initiatives gouvernementales. (ex : Bâle II, SOX, loi sur la protection des données au GDL)</p>	<p>En 2010, il y aura une convergence de la qualité/sécurité grâce à l'intégration de la sécurité dans les normes qualité. (ISO)</p>	
--	---	---	--	---

## Annexe 2 : Espace morphologique de la sécurité de l'information 3/3

### Espace Morphologique : Sécurité de l'Information H : 2010

Déterminant	Hypothèses d'évolution			
	A	B	C	D
<b>Intégration du risk management à tous les niveaux de l'entreprise quelle que soit sa taille, son secteur d'activité</b>	En 2010 l'intégration du Risk Management sera hétérogène en fonction de la taille de l'entreprise, de son domaine d'activité ou de sa nationalité.	En 2010 l'intégration du Risk Management sera plus homogène grâce à sa promotion et à la prise de conscience des entreprises.	En 2010, l'intégration du Risk management se fera de manière généralisée dans les entreprises via l'apparition de normes internationales	
<b>Sensibilisation par les pouvoirs publics et les associations</b>	En 2010, le degré de sensibilisation à la SI par les pouvoirs publics et les associations, restera faible.	En 2010, les pouvoirs publics et les associations intensifieront la sensibilisation à la SI. (multiplication des cibles)	En 2010, l'intégration de la SI par le grand public diminuera le besoin de sensibilisation. (intégration de la SI dans les formations professionnelles)	
<b>Evolution de la législation ou de la réglementation : imposer la mise en place d'un niveau sécurité de minimum dans les entreprises</b>	En 2010, il n'y aura pas d'obligation universelle de mise en place d'un niveau de sécurité minimum. (sauf pour les données personnelles)	En 2010, les autorités compétentes (administratives et réglementaires) imposeront la mise en place d'un niveau de sécurité minimum et/ou certaines règles de sécurité aux entreprises de certains secteurs (ex: secteur financier) secteurs régulés	En 2010, la législation imposera un niveau de sécurité minimum global aux entreprises sans prendre en compte la préservation de la compétitivité économique du GDL.	En 2010, la législation imposera un niveau de sécurité minimum global aux entreprises tout en préservant compétitivité économique du GDL.



## Références

1. Durand A., (2004), “Anticiper l'évolution des compétences en Technologie de l'Information et de la Communication : une application au métier d'entrepreneur de construction”, Centre de Recherche Public Henri Tudor, Luxembourg.
2. Durand A., (2005), "Module d'assistance au lancement des Comités d'Accompagnement de Plate-forme d'innovation du CITI", Centre de Recherche Public Henri Tudor, Luxembourg.
3. Ehrlich I. and Becker G., (1972), “Market Insurance, Self Insurance and Self Protection, Journal of Political Economy, 40.
4. Fericelli A.-M, (2001), “Théorie de la décision”, Dictionnaire des Sciences Economiques, PUF.
5. Godet M., (2001), “Manuel de prospective stratégique”. Dunod.