Offres de formation dans le domaine des cyber-risques (mesure 7 SNPC)

➢ **Résultat des interviews d'experts**

Bd de Pérolles 90 1700 Fribourg Switzerland T.+41 26 300 84 30 F.+41 26 300 97 94 www.iimt.ch iimt@unifr.ch

Contact
international institute for management in technology - iimt
Université de Fribourg
Boulevard de Pérolles 90
1700 Fribourg
Suisse
Suisse
Téléphone: +41 26 300 84 30
Fax: +41 26 300 97 94
Courriel: iimt@unifr.ch

Auteurs
Dominic Feichtner
Bernd Teufel
Stephanie Teufel

Table des matières

Liste des abréviations

BSI	Office fédéral pour la sécurité en matière de technologies de l'information
CAS	Certificate of Advanced Studies
CEO	Chief Executive Officer
CERT	Computer Emergency Response Team
C-Level	Premier niveau de direction d'une entreprise
CSIRT	Computer Security Incident Response Team
CSO	Chief Security Officer
(D)Dos	Déni de service distribué
DFAE	Département fédéral des affaires étrangères
IC	Infrastructures critiques
iimt	international institute of management in technology (Université de Fribourg)
ISACA	Information System Audit and Control Association
ISBO	Délégué à la sécurité informatique de la Confédération
ISO	International Organization for Standardization
MELANI	Centrale d'enregistrement et d'analyse pour la sûreté de l'information
OFCOM	Office fédéral de la communication
OFPER	Office fédéral du personnel
OFS	Office fédéral de la statistique
PME	Petites et moyennes entreprises
PSC	Prévention suisse de la criminalité
SANS	SANS Information Security Training
SAS	SAS Institute Inc.
SCOCI	Service national de coordination de la lutte contre la criminalité sur Internet
SNPC	Stratégie nationale de protection de la Suisse contre les cyberrisques
TI	Technologies de l'information
TIC	Technologies de l'information et de la communication
TP	Transports publics
UE	Union européenne
UPIC	Unité de pilotage informatique de la Confédération

1. Management Summary

La protection des infrastructures d'information et de communication contre les cyberrisques répond à un intérêt national. La sensibilisation de la société, en particulier des milieux économique et des autorités, constitue un facteur essentiel dans la gestion des risques.

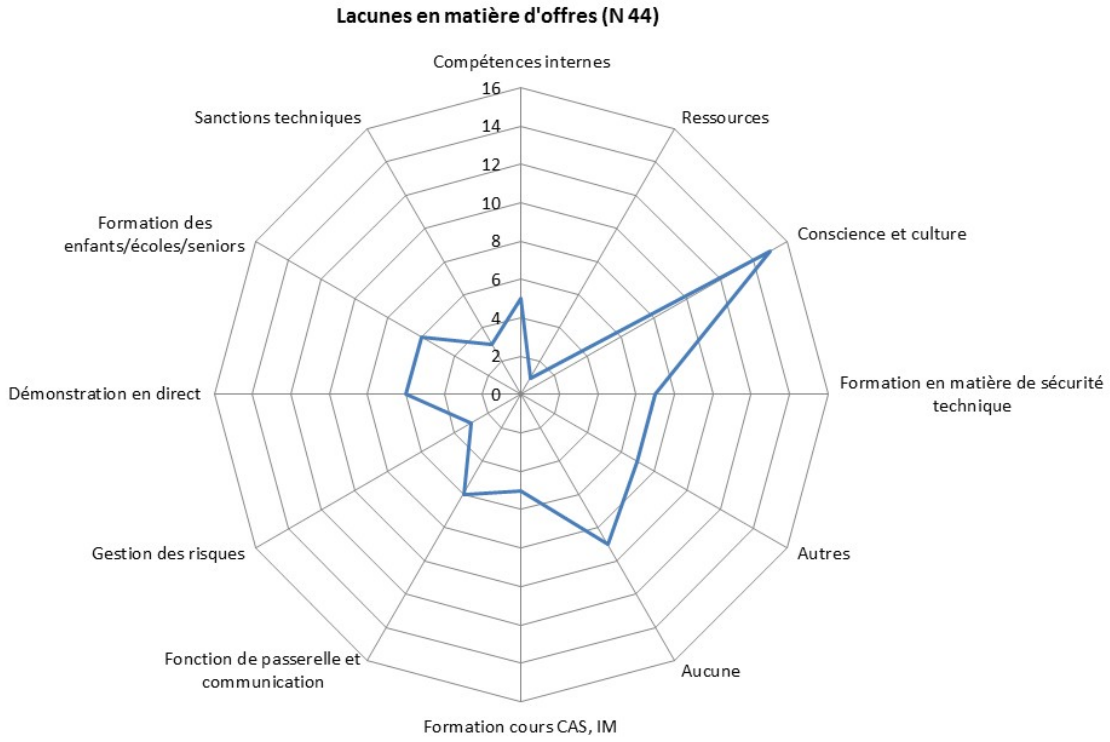
De manière générale, le terme "cyberrisques" comprend tous les types de risques liés aux technologies de l'information et de la communication (TIC). Il ne s'agit pas d'un risque en particulier, mais de la combinaison d'un ensemble de risques résultant des différentes technologies utilisées, des profils d'attaque ainsi que de circonstances extérieures, non influençables. L'appréciation des risques ne tient pas seulement compte des activités criminelles, mais aussi, par exemple, des catastrophes naturelles. A cet égard, il convient de distinguer les méthodes de défense et les méthodes de protection.

Dans un premier mandat, les groupes cibles ont été définis et spécifiés. A tous les niveaux de segmentation, des experts et de bons exemples dans ce champ thématique ont été identifiés. Parallèlement, un questionnaire pour l'enquête auprès des experts issus des groupes cibles a été élaboré.

Sur cette base, des experts issus de différents groupes cibles ont été interrogés sur la problématique des cyberrisques par l'Office fédéral de la communication (OFCOM), l'Unité de pilotage informatique de la Confédération (UPIC), economiesuisse et l'international institute of management in technology de l'Université de Fribourg (iimt).

L'enquête n'est pas représentative, mais elle dégage clairement des tendances et permet une meilleure compréhension du problème. Les experts interrogés proviennent principalement de l'économie et de l'administration. S'agissant des déclarations sur les lacunes en matière d'offres, cette approche qualitative, qui repose sur la participation exclusive de spécialistes hautement qualifiés, présente néanmoins une pertinence qui ne doit pas être sous-estimée. De manière générale, l'enquête a révélé qu'il existe une bonne conscience des risques. En revanche, les formations et en particulier leur utilisation semblent relativement peu connues, voire ignorées.

Des déclarations des groupes cibles issus de l'économie, de l'administration et de la population, on remarque que la soustraction de données et l'utilisation frauduleuse d'un dispositif de traitement de données semblent constituer les principaux cyberrisques tant pour les milieux de l'économie que pour l'administration. Le hacking et le déni de service (distribué) (DoS/DDoS) sont aussi mentionnés fréquemment, bien qu'il existe une certaine corrélation par exemple entre le hacking et la soustraction de données.



Comme le montre de graphique ci-dessus (voir illustration 8, p. 26), il existe parmi les lacunes mentionnées un déficit au niveau des formations proposées sur le marché libre. Les besoins sont manifestes dans la catégorie "Formation en culture de la sécurité et communication", ce qui se reflète en particulier dans la forte concentration sous "Conscience et culture".

2. Buts du projet

La protection des infrastructures d'information et de communication contre les cyberrisques répond à un intérêt national. Dans le cadre de la Stratégie nationale du Conseil fédéral pour la protection de la Suisse contre les risques cybernétiques (SNPC), tous les acteurs de l'économie, de la société et des autorités doivent être sensibilités aux cyberrisques et formés de sorte à pouvoir les reconnaître et prendre des mesures pour minimiser leur degré d'exposition. A cette fin, il convient de définir pour chaque groupe cible des compétences de base et des compétences clés pour la gestion des cyberrisques et d'augmenter le degré de connaissances à travers la publication d'exemples significatifs.

Dans le cadre d'un précédent projet[1], un guide d'interviews[2] a été conçu pour les entretiens avec les experts. Sur cette base, l'OFCOM, l'UPIC, economiesuisse et l'iimt ont menés des interviews sur le thème des cyberrisques avec des experts actifs dans différentes branches. Le but de ce nouveau mandat était de présenter et d'évaluer le matériel collecté. Le matériel a été complété par une autre interview d'experts (menée par l'iimt).

Les données collectées ont été assemblées et structurées de manière à permettre leur évaluation et leur représentation. Sur la base

- du rapport final de l'iimt rédigé à l'issue du premier mandat et
- des interviews d'experts menées par l'OFCOM, l'UPIC, economiesuisse et l'iimt,

celles-ci ont été évaluées et représentées en fonction des groupes cibles, compte tenu des exigences scientifiques.

A noter que les entretiens avec les experts a permis en outre d'identifier les cyberrisques pertinents, les compétences requises et les offres en formation pour chacun des groupes cibles.

Une démarche qualitative a été choisie comme modèle. Il convient donc de préciser explicitement qu'aucune conclusion représentative ne peut être tirée de ces résultats.

[1] D. Feichtner et al. NCS M7 Rapport final. iimt, Université de Fribourg, 2014.
[2] Voir annexe 1

3. Guide pour les interviews avec les experts

Le type d'interview choisi est l'interview guidée semi-structurée. Cette forme d'interview laisse la plus grande marge de réponse possible aux experts et permet d'identifier des modèles dans l'échantillon diversifié. Le but était que les interviews proprement dites soient les plus courtes possibles. Elles ont donc été réalisées en grande partie par téléphone.

Conformément aux buts du projet, l'enquête repose sur des critères qualitatifs. L'évaluation permet malgré tout de dégager des tendances et d'avoir une meilleure compréhension. Toutefois, avec l'échantillon choisi, il n'est pas possible de tirer des conclusions générales sur l'ensemble des groupes. Il n'en reste pas moins que l'approche qualitative, qui repose sur la participation exclusive de spécialistes hautement qualifiés, présente une pertinence qu'il ne faut pas sous-estimer et qu'elle fournit une base suffisante pour une enquête empirique ultérieure.

Le guide pour les interviews couvre les domaines suivants:

- Cyberrisques pertinents
- Compétences requises
- Bons exemples
- Lacunes en matière d'offres

Le questionnaire complet se trouve à l'aAnnexe 1 – s.

4. Plan d'enquête et description des groupes cibles

Les branches représentées dans l'illustration 1 ont été impliquées dans l'enquête. L'annexe 2 fournit plus de détails à ce propos.

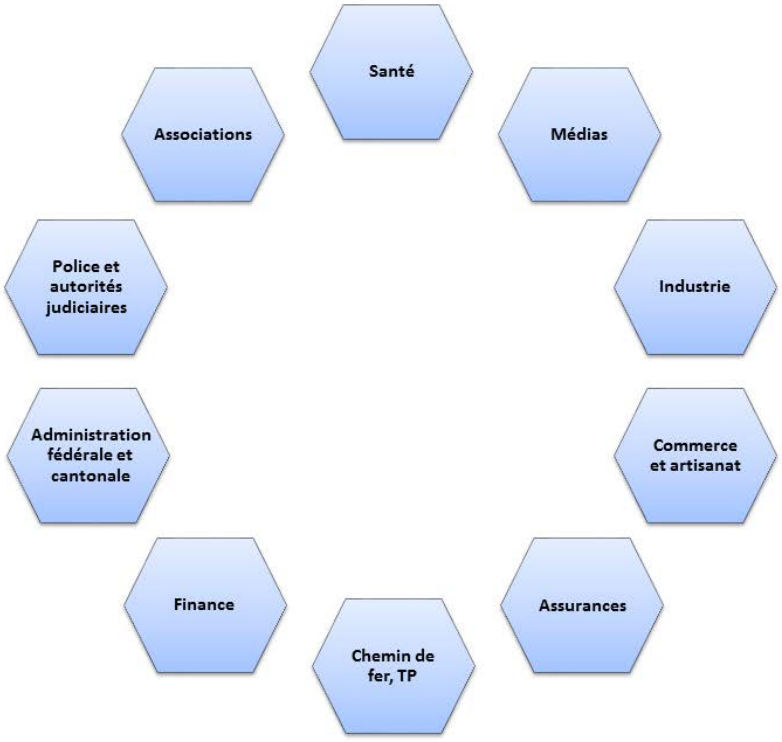


Illustration 1: Branches impliquées dans l'enquête

Afin d'identifier les offres en matière de formation des compétences, des entretiens avec des experts ont été menés pour chaque groupe cible. Cette approche qualitative ne permet toutefois pas de tirer de conclusion représentative. Ainsi, les offres de qualité en matière de formation recommandées par les experts pour leur groupe cible sont indiquées à titre d'exemples. La liste n'est pas exhaustive.

Le choix de la quarantaine d'experts s'est fait d'entente avec plusieurs personnes clés issues des groupes cibles. Au moins un entretien d'experts a été mené dans chaque groupe cible. Les personnes interrogées travaillent dans une organisation spécifique au groupe cible ou sont responsables, en tant qu'intermédiaires, de la transmission de contenus à ces groupes cibles (p. ex. les enseignants au titre d'intermédiaires pour les enfants et les jeunes). Afin d'éviter tout conflit d'intérêt à l'heure de recommander de bonnes offres de formation, les représentants des institutions de formation n'ont pas été interrogés.

Les entretiens avec les experts, qui se sont terminés en novembre 2014, ont été réalisés par l'organe de coordination SNPC (ISB/MELANI), l'OFCOM, le DFAE et l'association faîtière

economiesuisse. Sur mandat de l'OFCOM, l'iimt de l'Université de Fribourg a également conduit une enquête auprès d'une sélection de grandes entreprises et de PME.

Les enquêtes ont été menées en allemand ou en français, sous forme d'interviews personnelles, par téléphone ou par écrit, d'une durée d'une demi-heure. Un guide pour les interviews spécialement conçu par l'iimt a été utilisé. Il a été adapté en fonction des groupes cibles spécifiques[3].

[3] Voir annexe 1

5. Résumé de l'enquête auprès des experts

Illustration 2 ci-dessous montre la composition de l'échantillonnage. Les grandes entreprises sont surreprésentées (25% de l'échantillonnage), ce qui peut, sur l'ensemble, fausser les avis recueillis. En ce qui concerne la prise en compte des cyberrisques perçus, la distorsion est toutefois négligeable, vu que les avis tendent vers des résultats identiques dans tous les groupes cibles.

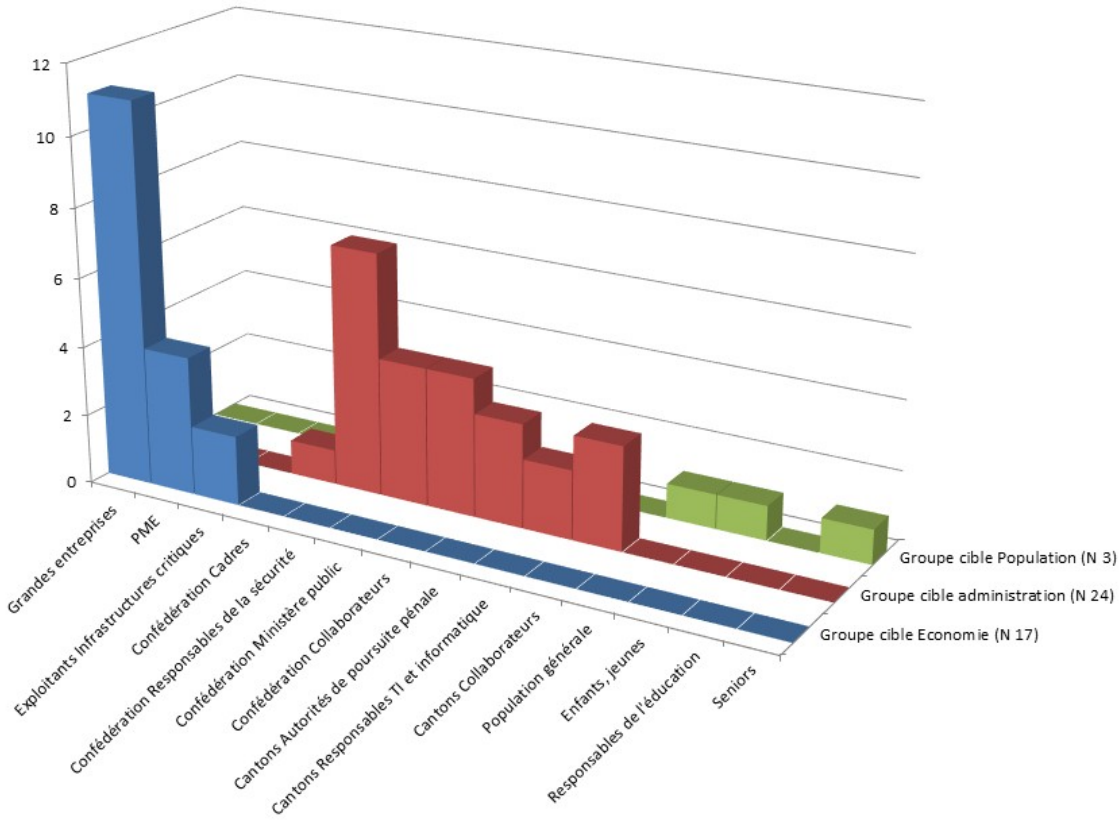


Illustration 2: Composition de l'échantillonnage

5.1.Groupe Economie

Pour tenir compte de l'échantillon hétérogène et complet du groupe cible Economie, trois sous-groupes ont été formés pour l'enquête: Grandes entreprises, PME et Exploitants d'infrastructures critiques[4]. Les menaces éventuelles ainsi que les besoins de protection qui en découlent sont variés, tout comme les moyens financiers et en personnel pour se prémunir contre les cyberrisques avec les compétences nécessaires. Une grande entreprise est probablement plus exposée aux attaques, mais dispose aussi de moyens de protection plus importants (ressources) qu'une PME.

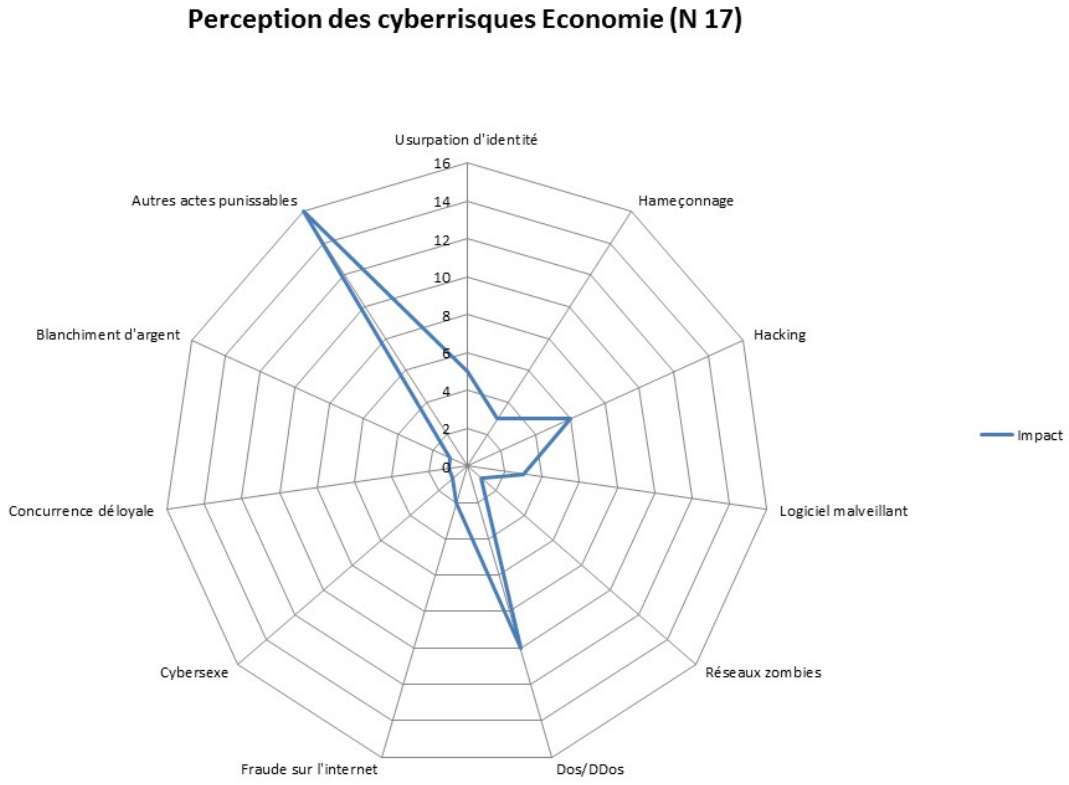


Illustration 3: Perception des cyberrisques par le groupe Economie

Illustration 3 décrit l'intégration des différentes formes de criminalité sur l'internet définies par le SCOCI en 2014[5]. Le tableau montre en particulier une prépondérance des *autres actes malveillants*. Cette caractéristique est décrite et analysée plus en détail ci-après.

Vu la diversité des mentions, il est recommandé de réfléchir à une reformulation des termes génériques et des formes. Une affectation claire entre les différentes formes de criminalité

[4] Les infrastructures critiques garantissent la disponibilité de biens et de services d'importance capitale, comme l'énergie, la communication ou les transports. Les défaillances de grande ampleur géographique ont des conséquences graves sur la population et l'économie. Elles compromettent également la sécurité et le bien-être national. (cf Stratégie nationale pour la protection des infrastructures critiques, Berne, 2012)

[5] M. Spasojevic, Formes de la criminalité sur internet, Département fédéral de justice et police, Berne, 2014

est difficile, car souvent une infraction peut en entraîner une autre. Par exemple, le *hacking* est un moyen pour accéder de manière illicite à un système de traitement de données.

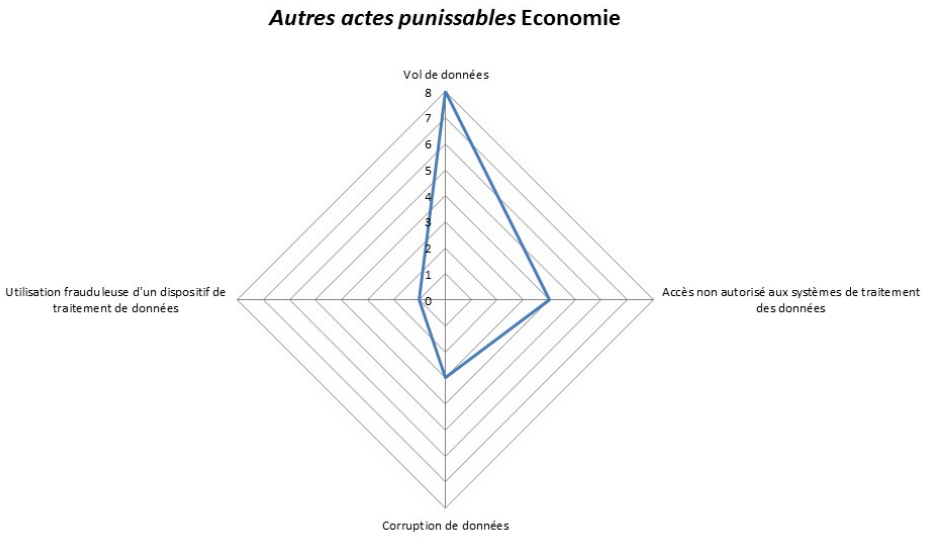


Illustration 4: Détail des actes illicites pour le groupe Economie

Illustration 4 présente les cyberrisques perçus. Un examen détaillé s'est avéré nécessaire, car 16 mentions ont été directement attribuées à ce domaine. Pour les experts du groupe Economie, la soustraction de données par des tiers (p. ex. espionnage)[6] constitue le risque potentiel le plus élevé. Il existe plusieurs moyens et méthodes pour accéder indûment aux données, par exemple par des actes de *hacking* ou de hameçonnage (*phishing*), voire par une perte de données en interne.

Les résultats des entretiens menés avec les experts sont présentés de manière résumée ci-après.

5.1.1. Grandes entreprises

Une entreprise comptant 250 emplois ou plus à temps plein est considérée comme une grande entreprise (Office fédéral de la statistique, OFS).

Type de risques perçus:

Suivant leur orientation économique, les grandes entreprises sont différemment exposées aux cyberrisques. Les risques majeurs sont la perte de données (de clients), la soustraction

[6] Autres infractions (Spasojevic, M., 2014). La pornographie n'a pas été retenue en raison de sa faible importance. Le cybersexe inclut par exemple des attaques potentielles par l'envoi de photos compromettantes ou l'utilisation du navigateur comme porte d'entrée pour l'implantation de virus, etc.

de données dans un but d'espionnage ou de revente, les manipulations (internes et externes), les cyberattaques de *hackers* (notamment hameçonnage, virus, DDos).

Capacités essentielles pour la perception, l'estimation et la gestion des cyberrisques:

- Connaissances techniques liées à une réflexion interdisciplinaire et opérationnelle, dans le but également d'aborder concrètement les questions de sécurité avec la direction.
- CEO: organiser l'entreprise de telle sorte que les questions de sécurité sont abordées intégralement et intégrées dans les processus commerciaux (p. ex. via le responsable de la sécurité).
- Fournisseurs externes de prestations: certification (ISACA et série ISO 2700x).

Lacunes en matière d'offres:

- Les offres s'adressent en premier lieu à des spécialistes TI. Il n'existe pas d'approche interdisciplinaire, par exemple une formation destinée aux collaborateurs chargés de la conformité et de la protection des données ou de la communication.
- Il n'existe pas de possibilités de formation pour le profil de médiateur entre la technique et les affaires (souvent au niveau C) permettant à la sécurité de soutenir le processus commercial.

5.1.2. PME

Une PME comprend jusqu'à 249 emplois à temps plein (Office fédéral de la statistique, OFS).

Type de risques perçus:

Suivant leur orientation économique, certaines PME sont fortement exposées aux cyberrisques, alors que d'autres ne le sont pratiquement pas. Il convient d'établir une distinction entre les risques externes et internes. Les risques majeurs sont l'espionnage économique, les cyberattaques sur les infrastructures (notamment DDos) et le vol de données qui, à l'exception des attaques DDos, relèvent essentiellement des *autres actes malveillants*.

Capacités essentielles pour la perception, l'estimation et la gestion des cyberrisques:

- Aversion élevée au risque, évaluation adéquate des risques et des incidents, activation de mesures de protection adaptées, sollicitation (au besoin) d'experts externes; expliquer les risques encourus par l'entreprise aux supérieurs peu au fait de la technique.
- Fournisseurs externes de prestations: certification (ISACA, série ISO 2700x, norme BSI).

Lacunes en matière d'offres:

- Il existe peu d'offres pour le traitement adéquat des données personnelles à l'interface entre vie privée et vie professionnelle. Des directives en ce sens seraient souhaitables.
- Des offres en matière de formation des compétences intégrées dans la concurrence font actuellement défaut et seraient souhaitables.

5.1.3. Exploitants d'infrastructures critiques

Ce groupe cible comprend les exploitants d'infrastructures dans des secteurs de l'économie privée hautement critiques.

Type de risques perçus:

Dans son fonctionnement quotidien, chaque organisation doit se protéger des probabilités de cyberrisques, tels que des perturbations et pannes suite à un accident ou à une catastrophe naturelle ou des attaques non ciblées. Pour les exploitants d'infrastructures critiques, il est primordial aussi de se protéger des attaques ciblées visant la disponibilité et l'intégrité des services TIC. Les risques primaires sont le chantage (attaques DDos, menaces de manipulations de systèmes ou de données, notamment pour les systèmes de commande), la soustraction de données (espionnage, recherche des points faibles par des organisations semblables à des organismes gouvernementaux, actes malveillants internes), les sabotages et les manipulations (de systèmes critiques, en particulier des systèmes de commande, mais aussi attaques contre des systèmes périphériques mal protégés).

Capacités essentielles pour la perception, l'estimation et la gestion des cyberrisques:

- Appréhension des risques et de la sécurité dans leur globalité, sans se restreindre à des mesures techniques sur les systèmes et les processus.
- Imposition des autorisations d'accès dans l'organisation par l'établissement de processus et de connaissances liées à la sécurité et à la protection des informations.
- Capacités analytiques pour l'identification des besoins en matière de protection.
- Protection contre les cyberattaques: détection (surveillance), réaction (gestion des incidents), plan d'urgence (notamment en ce qui concerne les flux des données) et prévention (y compris mise en place d'une culture de l'erreur et de l'échange, aussi dans le cadre de collaborations subsidiaires avec des organisations étatiques et privées).
- CERT: changement de perspective (point de vue de l'agresseur), concept et design des composants informatiques et leur implication sur la sécurité, des systèmes d'exploitation et des logiciels d'application, design et analyse des protocoles de réseaux, cryptologie, ingénierie inverse des appareils et des logiciels (y compris logiciels malveillants), développement d'outils de sécurité, forensique numérique, gestion des incidents, gestion et dépistage de la vulnérabilité.

Lacune en matière d'offres:

- En Suisse, il existe peu d'offres de formation permettant d'acquérir et de renforcer les capacités CERT.

5.2. Groupe Administration

Les autorités étatiques et les administrations publiques à tous les niveaux constituent des cibles potentielles pour des cyberattaques qui peuvent entraver leur activité en tant qu'or-

ganes législatifs, exécutifs ou judiciaires. Elles utilisent et exploitent aussi des infrastructures critiques et doivent les protéger. Ce groupe cible a été divisés en deux sous-groupes – Confédération et cantons –, puis en différents rôles et domaines d'activités.

Les résultats des entretiens menés avec les experts sont présentés de manière résumée dans l'illustration 5.

La perception des cyberrisques par l'administration présente un tableau similaire aux préoccupations exprimées par les experts du groupe cible Economie. Elle diffère par contre suivant la sphère de responsabilité et la position. Les avis des différents groupes sont résumés dans les descriptions. La forte proportion des *autres actes malveillants* est présentée plus en détail.

Illustration 6 indique la forte perception des sondés face à un certain nombre de cyberrisques potentiels, notamment l'acquisition non autorisée de données par des tiers ou l'accès non autorisé aux systèmes de traitement de données.

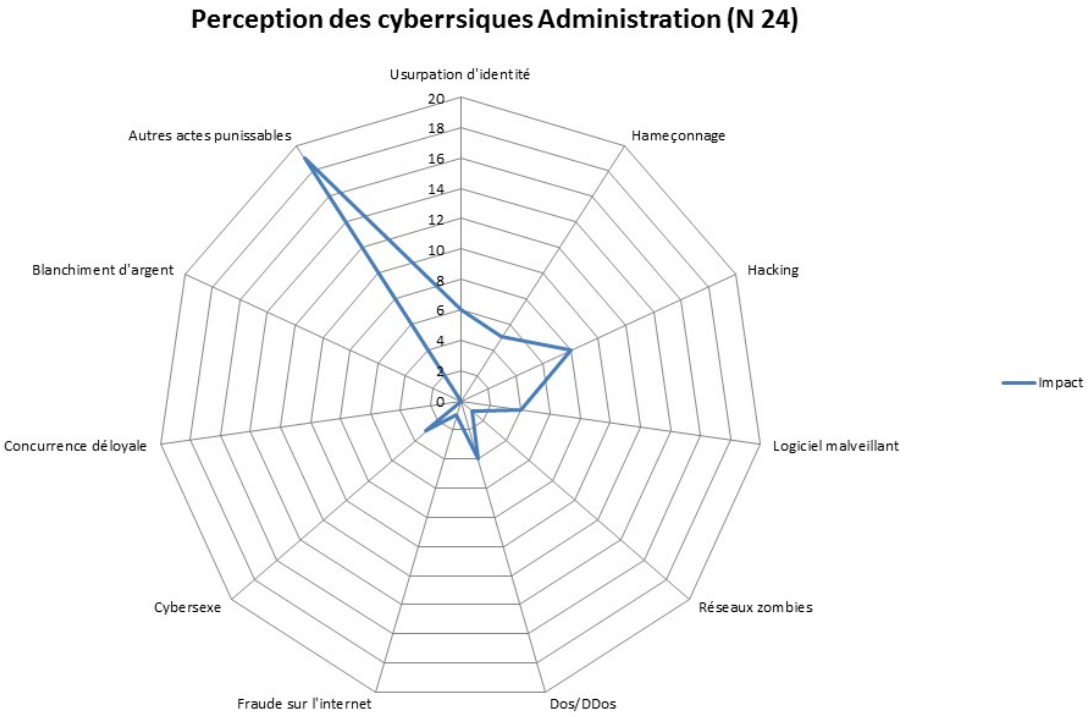


Illustration 5: Perception des cyberrisques par le groupe Administration

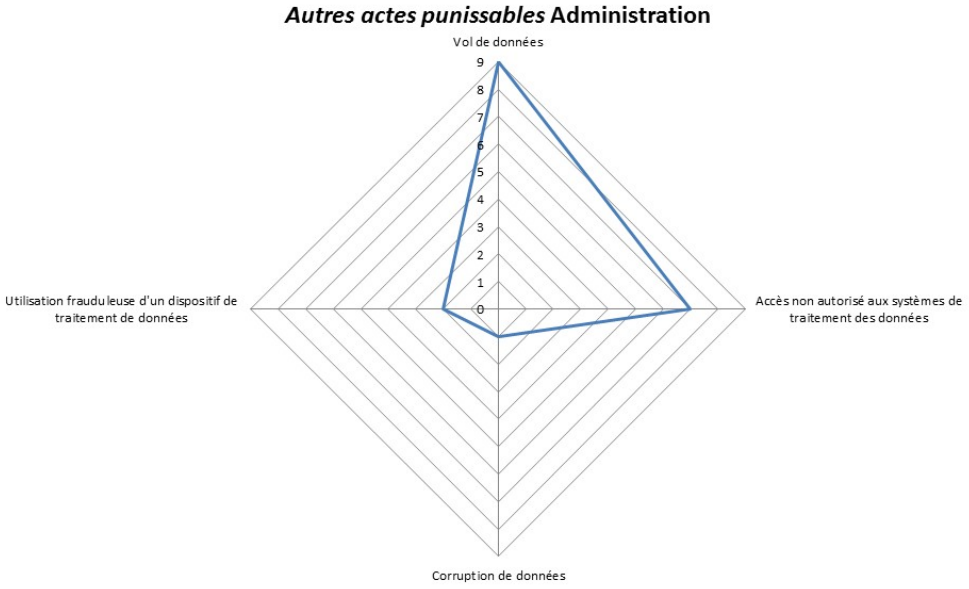


Illustration 6: Détail des actes illicites pour le groupe Administration

5.2.1. Confédération: Cadres

Type de risques perçus:

Les cadres sont responsables du bon fonctionnement de leur unité et supportent les risques (résiduels), qu'ils soient financiers ou opérationnels. Au vu de la forte interconnexion entre les processus, le cyberrisque fait aussi partie des risques opérationnels.

Capacités essentielles pour la perception, l'estimation et la gestion des cyberrisques:

- L'importance des risques pour l'organisation fait l'objet d'une évaluation; la sécurité est intégrée dans les processus afin d'élaborer ceux-ci de manière plus efficace; engagement d'instruments de gestion des risques (la gestion des risques relève du chef).

Lacune en matière d'offres:

- Formations systématiques pour les cadres moyens. Une offre d'e-apprentissage sur la sécurité des informations est prévue.

5.2.2. Confédération: Responsables de la sécurité

Les responsables de la sécurité à la Confédération comprennent les délégués à la sécurité informatique (ISBD/ISBO), les préposés à la protection des données, les préposés à la sécurité des objets, les analystes techniques et les ingénieurs en sécurité du CSIRTS ainsi que les personnes impliquées dans la sécurité des processus et les risques.

Type de risques perçus:

Attaques ciblées contre les infrastructures TIC, y compris attaques de grande envergure (organisations gouvernementales, criminels), dans le but d'accéder à des données à des fins d'espionnage; perte de données; actes malveillants internes tels que vol ou soustraction de données; intérêt commercial à la revente de données; attaques visant la disponibilité et l'intégrité des services TIC de l'administration fédérale; chantage de hackers; violation de la protection des données et atteinte à la personnalité.

Capacités essentielles pour la perception, l'estimation et la gestion des cyberrisques:

- Compréhension des déroulements et des processus commerciaux critiques au sein de la Confédération.
- Présentation des risques aux décideurs.
- Connaissances des systèmes de sécurité TI (techniques, organisationnelles et en matière de gestion) et protection des données.
- Elaboration d'une documentation relative à la protection des données personnelles dans les processus administratifs.
- Collaboration et échange d'informations avec d'autres acteurs importants comme MELANI, CSIRT OFIT, ISBO/ISBD.
- Compréhension conceptuelle et stratégique des dangers dans le cyberespace, et pas seulement au niveau technique.
- CSIRT: expérience pratique dans l'ingénierie des systèmes, l'exploitation et les réseaux, connaissances de l'analyse log, système de détection et de prévention d'intrusion, analyse des logiciels malveillants, forensique TI sur les plateformes usuelles, sécurité des applications, pare-feu, sécurité mobile, sécurité de l'informatique en nuage, etc.
- Fournisseurs externes de prestations: certification des produits et de l'exploitation.

Lacunes en matière d'offres:

- Offres comparables aux cours SANS en Suisse.
- Formations pour des fonctions de passerelle entre les spécialistes TIC et les décideurs, afin d'établir une meilleure compréhension des exigences de sécurité (y compris les risques résiduels).
- Elargissement du champ de vision des risques TI à la protection des infrastructures critiques en Suisse ("grande image").
- Rotations de postes sur plusieurs jours, afin de connaître le fonctionnement des autres offices en matière de sécurité (p. ex. rocade entre les ISBO).

5.2.3. Confédération: ministère public

Type de risques perçus:

Attaques ciblées en vue d'obtenir des informations sur des procédures en cours, actes malveillants internes tels que vol ou soustraction de données, appropriation de données sensibles, problématique du droit de la personnalité pour les personnes connues, non-respect ou respect insuffisant des directives et des lignes directrices.

Capacités essentielles pour la perception, l'estimation et la gestion des cyberrisques:

- *Dans le domaine de la poursuite pénale*:
  Expérience et disponibilité à se former, affinité technique et connaissances juridiques et forensiques.
- *Dans le domaine de la protection des informations*:
  Reconnaissance des risques et évaluations de la pertinence des incidents; établir des processus de gouvernance et les appliquer consciemment; connaissances des systèmes de sécurité TI (techniques, organisationnelles et en matière de gestion) et protection des données; collaboration et échange d'information (réseautage) avec des partenaires.

Lacune en matière d'offres:

- Formation combinée en droit et en forensique, p. ex. "juriste et cyberenquêteur", sensibilisation.

5.2.4. Confédération: collaborateurs de l'administration fédérale

Type de risques perçus:

Attaques non ciblées de l'extérieur, attaques ciblées via l'ingénierie sociale; surmenage dû à la complexité technique.

Capacités essentielles pour la perception, l'estimation et la gestion des cyberrisques:

- Exécution correcte des mesures de protection fondamentales.
- Respect des exigences en matière de protection des informations (également avec les informations électroniques).

Lacune en matière d'offres:

- Formations internes, répétées régulièrement, sur la protection des informations (éventuellement organisation de l'OFPER).

5.2.5. Cantons: autorités de poursuite pénale

Type de risques perçus:

Attaques ciblées en vue d'obtenir des données personnelles, notamment provenant de banques de données cantonales de recherche de personnes et d'objets. Acquisition d'informations et manipulation d'enquêtes en cours. Facteur d'incertitude lors de la transmission de données sécurisée.

Capacités essentielles pour la perception, l'estimation et la gestion des cyberrisques:

- Compétences techniques de base, disponibilité à se former, collaboration intercantonale, mise en réseau au niveau international.
- Perception fondamentale, c'est-à-dire conscience du problème.

Lacunes en matière d'offres:

- Formation combinée en droit et en forensique.
- Perfectionnement des services judiciaires en Suisse.

- Formation post-grade spécifique pour les forces de police.
- Sensibilisation.

5.2.6. Cantons: responsables des TI et de la sécurité informatique

Type de risques perçus:

Attaques ciblées via l'internet visant des applications spécifiques (p. ex. portail des impôts, guichet virtuel), vol de données, hameçonnage, maintenance des TIC, manipulations erronées par des personnes ainsi qu'attaques non dépistées et leurs conséquences.

Capacités essentielles pour la perception, l'estimation et la gestion des cyberrisques:

- Connaissances combinées dans la technique et la gestion, connaissances des dispositions juridiques, aptitudes à communiquer et force de conviction.
- Connaissances approfondies des processus de gestion de l'administration cantonale et de ses infrastructures, longue expérience dans l'exploitation de réseaux, surveillance du système, bonne estimation du degré d'importance des incidents, compétences forensiques.
- Collaboration étroite avec les responsables de la sécurité des TI des autres cantons et avec MELANI.
- Fournisseurs externes de prestations: certification (série ISO 2700x).

Lacune en matière d'offres:

- Pas de mention.

5.2.7. Cantons: collaborateurs des administrations cantonales

Type de risques perçus:

Accès non autorisé à des données confidentielles par des tiers (ingénierie sociale ou hameçonnage), manipulations de données, indisponibilité ou panne du réseau interne.

Capacités essentielles pour la perception, l'estimation et la gestion des cyberrisques:

- Capacités spécifiques des collaborateurs et aptitudes à effectuer les tâches déléguées. Plus le collaborateur dispose de compétences, plus les contacts par courriers électroniques avec l'extérieur sont fréquents et plus l'accès à des applications critiques est fréquent.
- Nécessité d'une prise de conscience à large échelle.

Lacunes en matière d'offres:

- Il n'existe pas d'offres adaptées à l'environnement et aux besoins des collaborateurs.
- Formation des présidents de tribunaux.
- Formation au niveau des ressources humaines (constituent souvent une porte d'entrée pour une attaque).

5.3.Groupe Population

Les cyberrisques concernent aussi la population, avec les utilisateurs individuels d'infrastructures critiques et de systèmes d'information et de communication privés et professionnels. Une stratégie efficace contre les cyberrisques doit également tenir compte du comportement des individus et des risques engendrés. Car le même principe s'applique à la population: la connaissance permet d'adopter une attitude sûre par rapport aux cyberrisques et protège des mauvaises surprises.

L'illustration 7 résume les résultats des entretiens avec les experts.

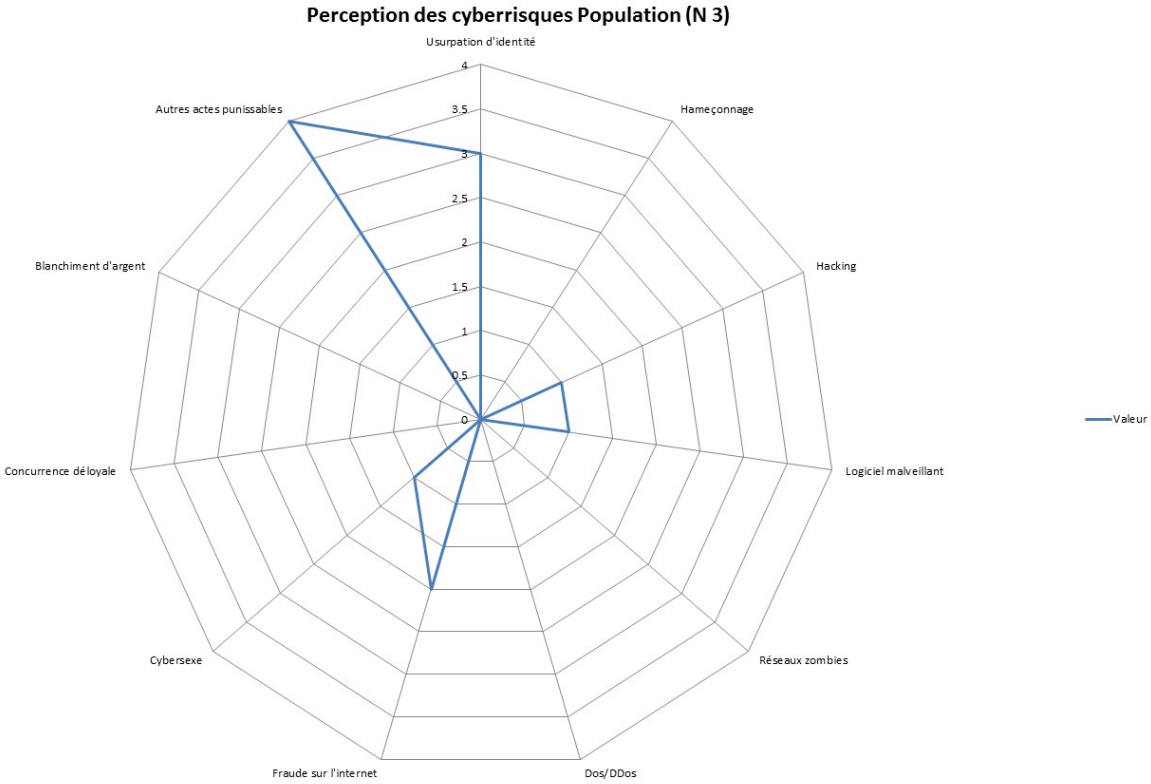


Illustration 7: Perception des risques par le groupe Population

5.3.1. Population générale

Le groupe cible constitué par la population générale comprend les personnes vivant en Suisse, quels que soient leur nationalité, leur âge et leur activité.

Type de risques perçus:

Fraude, arnaques, hameçonnage, usurpation d'identité, franchissement des limites de la pornographie légale à la pornographie illégale, escroquerie en ligne au mariage, cyberharcèlement obsessionnel, sextorsion (extorsion professionnelle avec des photos de nu sur l'internet).

Capacités essentielles pour la perception, l'estimation et la gestion des cyberrisques:

- Connaissances de base du fonctionnement de l'internet, du courrier électronique et du potentiel d'abus (p. ex. anonymat, possibilités de modifier des photos, sécurité des https://, etc.). Connaissances du hameçonnage, des cookies, des règles pour chatter en toute sécurité (p. ex. choix des pseudos) et lors de l'utilisation des données personnelles, mais aussi connaissances de l'empreinte numérique de l'ensemble des données, du caractère punissable du harcèlement sexuel et d'autres menaces sur l'internet.

Lacune en matière d'offres:

- Pas de mention.

5.3.2. Enfants et jeunes

Type de risques perçus:

Harcèlement sexuel (grooming), pornographie (protection de la jeunesse), sextos, cybermobbing, sextorsion par des personnes de l'entourage (extorsion avec des photos de nu sur l'internet). En outre, comme pour la population générale: fraude, arnaques, hameçonnage et usurpation d'identité.

Capacités essentielles pour la perception, l'estimation et la gestion des cyberrisques:

- Protection des données personnelles; connaissance des organisations et des personnes qui offrent une aide.

Lacunes en matière d'offres:

- Matériel de sensibilisation des jeunes enfants (3 à 9 ans) pour les premiers pas sur l'internet. Idéalement un matériel similaire à celui utilisé pour l'éducation routière.
- Matériel d'information pour les enfants et les jeunes qui se trouvent dans des institutions pédagogiques spécialisées et qui ne peuvent être atteints par le biais de l'école ordinaire.

5.3.3. Responsables de l'éducation et de la formation

Les parents, les enseignants, les maîtres d'apprentissage, les animateurs de jeunesse et autres sont aussi compétents, en tant que responsables de l'éducation et de la formation des enfants et des jeunes, pour transmettre des connaissances en matière de cyberrisques. Il est important de sensibiliser et de former ces responsables, au même titre que les enfants et les jeunes.

Vu les besoins en la matière, de nombreuses offres en matière de formation des compétences s'adressent aujourd'hui à ces groupes cibles (voir www.jeunesetmedias.ch). L'initiative de sensibiliser les parents est en général prise par les écoles, mais n'est pas systématique. La nécessité de former les enseignants va se renforcer, étant donné que les nouveaux plans d'études régionaux prévoient un ancrage de l'éducation aux médias (ou de la programmation informatique) dans l'enseignement scolaire.

Type de risques perçus:

(voir chapitre Enfants et jeunes)

Capacités essentielles pour la perception, l'estimation et la gestion des cyberrisques:

- Sensibilisation des enfants et des jeunes, information relative aux traces laissées sur l'internet et aux mesures spécifiques de protection contre les cyberrisques, assistance en cas de menaces et d'agressions. Réglementation de la consommation des médias par les enfants.

Lacunes en matière d'offres:

- Les offres publiques et privées pour les enseignants sont nombreuses (elles relèvent de la compétence des cantons), contrairement à celles proposées aux parents, où il manque notamment un matériel de formation rédigé dans les langues de migration et conçu pour les parents ayant un faible niveau de formation.
- Matériel d'information pour les jeunes vivant dans des institutions socio-pédagogiques et donc difficiles à atteindre par le biais des écoles et d'autres offres publiques.
- Au niveau des institutions spécialisées pour les enfants et les jeunes, on constate un manque de concepts et de lignes directrices avec des informations bien documentées, conçues en fonction du contexte (socio-pédagogique) spécifique donné. Des bases pour les responsables et les éducateurs travaillant dans le secteur de l'aide aux enfants et aux jeunes semi-ambulatoire ou en institution font également défaut.
- Informations relatives à la pornographie sur l'internet, destinées aux enfants et aux jeunes, mais aussi aux parents et aux responsables légaux. Les limites légales de la consommation de contenus pornographiques sont trop peu connues.

5.3.4. Personnes âgées

Le 4e âge (80 ans et plus) ne navigue encore guère sur l'internet; les données ci-dessous se rapportent aux "silver surfers" (50 ans et plus).

Type de risques perçus:

Fraude, arnaques, hameçonnage; usurpation d'identité, pornographie illégale, escroquerie en ligne au mariage, cyberharcèlement obsessionnel, sextorsion (extorsion professionnelle avec des photos de nu sur l'internet). De manière générale, les personnes âgées ne sont pas particulièrement ciblées par les cyberattaques. Elles sont néanmoins enclines, sur demande, à divulguer des données personnelles ou à s'engager par contrat.

Capacités essentielles pour la perception, l'estimation et la gestion des cyberrisques:

- Connaissances de base des cyberrisques et de leurs conséquences, compétences techniques sur les paramètres de sécurité des terminaux utilisés, attitude adéquate à adopter en cas de problème.

Lacune en matière d'offres:

- Mise à disposition d'informations relatives à la sécurité sur l'internet (p. ex. sous forme de brochures) conçues spécifiquement pour les personnes âgées.

6. Lacunes en matière d'offres

Les lacunes en matière d'offres identifiées avec les experts sont résumées dans l'illustration 8. Le déficit constaté dans le domaine "Conscience et culture" est particulièrement manifeste. Les lacunes relevées par les experts dans les secteurs "Sanctions techniques", "Compétences internes" et "Ressources" concernent avant tout l'entreprise elle-même; elles ne doivent pas être comblées spécifiquement par des offres du marché libre.

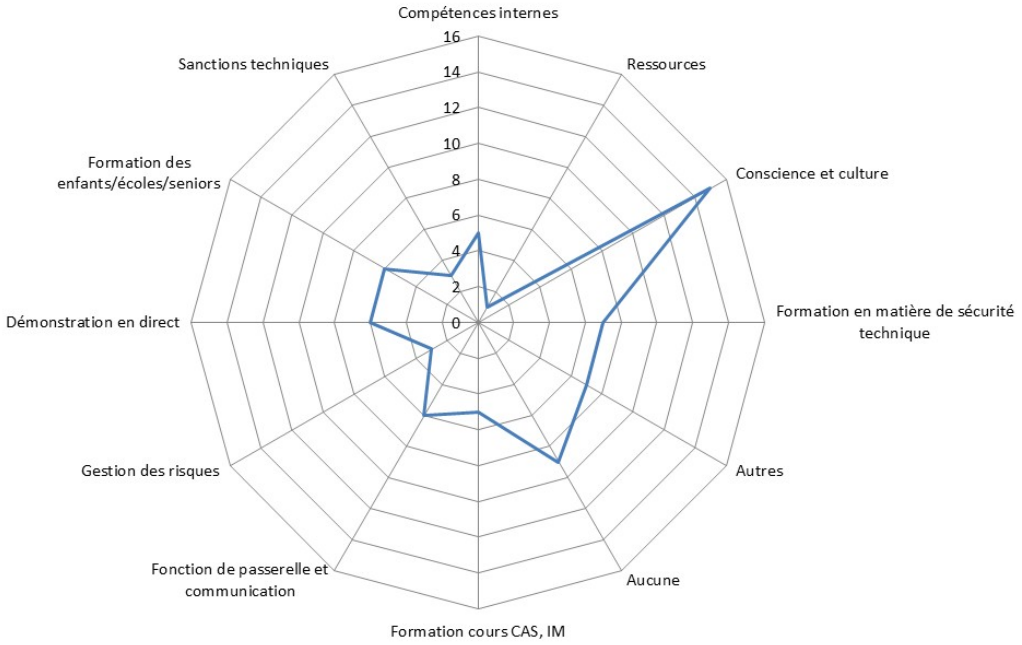


Illustration 8: Lacunes identifiées en matière d'offres

Un deuxième examen a permis d'identifier plus précisément les lacunes représentées à l'illustration 8 et de les classer dans les catégories suivantes (voir Illustration 9):

- Formation au sein de l'entreprise
- Formation en culture et communication
- Formation technique
- Formation générale
- Aucune lacune constatée
- Divers
- Aucune indication

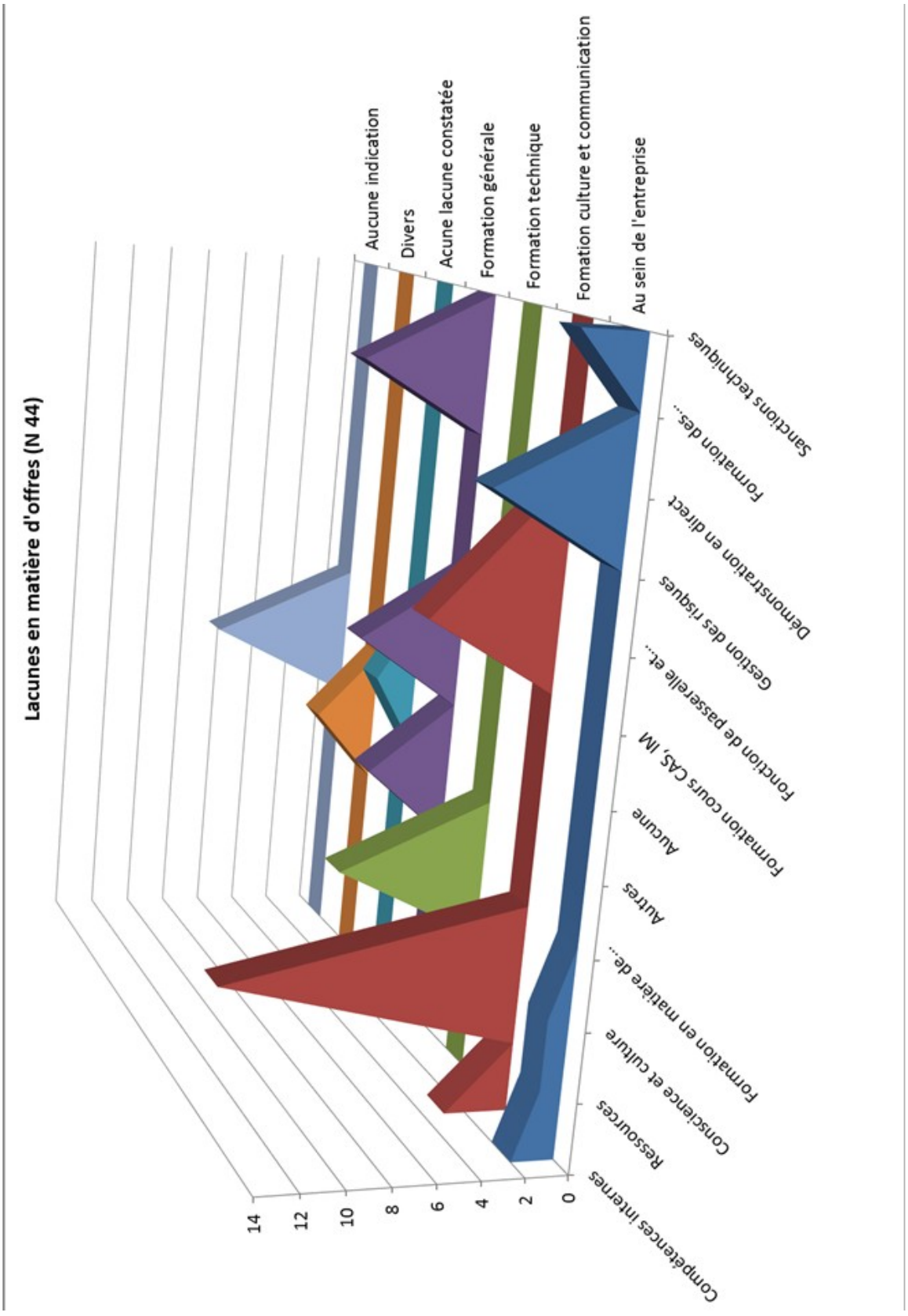


Illustration 9: Lacune identifiée par catégories

Cette approche met en exergue le fait que la formation, toutes spécificités confondues, affiche un déficit massif, avec 70% de mentions. On observe cependant que 18% des réponses entrent dans les catégories Divers ou Aucune indication.

L'illustration 9 résume les lacunes en matière d'offres identifiées par les experts. Les compétences et les déficits catégorisés sont décrits dans une représentation, les chiffres correspondent à l'attribution des réponses.

Les principaux manques relèvent du rapport entre le déficit d'offres "Formation en culture et communication" et les compétences "Conscience et culture", ainsi que de la "fonction de passerelle" et de la "gestion des risques". Les lacunes dans les domaines de la "Formation au sein de l'entreprise" et de la "Formation technique" reflètent les insuffisances mentionnées par les experts dans les certifications et le manque d'offres CAS, CERT et SAS.

Vu que des spécialistes hautement qualifiés ont pris part aux entretiens, il convient d'accorder une certaine importance aux déclarations relatives aux lacunes en matière d'offres. Il est par exemple intéressant de souligner que les experts soulèvent des questions liées non seulement aux aspects techniques, mais aussi à la culture de la sécurité dans les organisations. On peut en conclure que, cas échéant, la conscience des risques encourus ne va pas de soi et qu'elle doit être renforcée en implémentant et en contrôlant régulièrement une telle culture de la sécurité.

Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Département fédéral des finances DFF

Unité de pilotage informatique de la Confédération UPIC
Centrale d'enregistrement et d'analyse pour la sûreté de l'information

Ka Schuppisser, 9 avril 2014

Stratégie nationale de protection de la Suisse contre les cyberrisques (SNPC)

Mesure 7: Formation des compétences en gestion des cyberrisques – vue d'ensemble des bonnes pratiques

Mandat, approche et guide pour les interviews

Table des matières

1 Mandat et objectifs

La stratégie de protection de la Suisse contre les cyberrisques s'articule en seize mesures visant à accroître la cyberrésilience du pays.

La détection des cyberrisques et une protection ciblée de notre cadre de vie et des activités économiques exigent des connaissances spécifiques: d'où la nécessité d'une formation de base plus poussée, pour permettre aux spécialistes de la sécurité des TIC de surveiller efficacement les réseaux, d'analyser les menaces et de bien réagir en cas d'incident. La formation continue de tous les spécialistes en TIC sur les questions de sécurité s'avère également importante. Il s'agit par ailleurs de compléter les connaissances juridico-techniques qu'ont les autorités de poursuite pénale en matière de cyberdélits. De même, la population aurait besoin d'une solide compréhension des questions de sécurité, afin de se protéger des cyberrisques. Deux aspects sont ici prioritaires, soit la protection de la sphère privée et celle des systèmes TIC privés, susceptibles d'être piratés en vue du lancement d'attaques contre des infrastructures critiques. Conscient de l'importance de créer ou renforcer les aptitudes susmentionnées, le Conseil fédéral y a consacré la mesure 7 de sa stratégie: «Formation des compétences en gestion des cyberrisques».[1]

Il existe déjà de nombreuses possibilités de perfectionnement dans le domaine de la protection contre les cyberrisques: campagnes, filières de formation, manuels, sites Web, etc. Or non seulement l'offre reste trop peu connue, mais il est difficile d'en mesurer la qualité et l'adéquation à son propre groupe-cible.

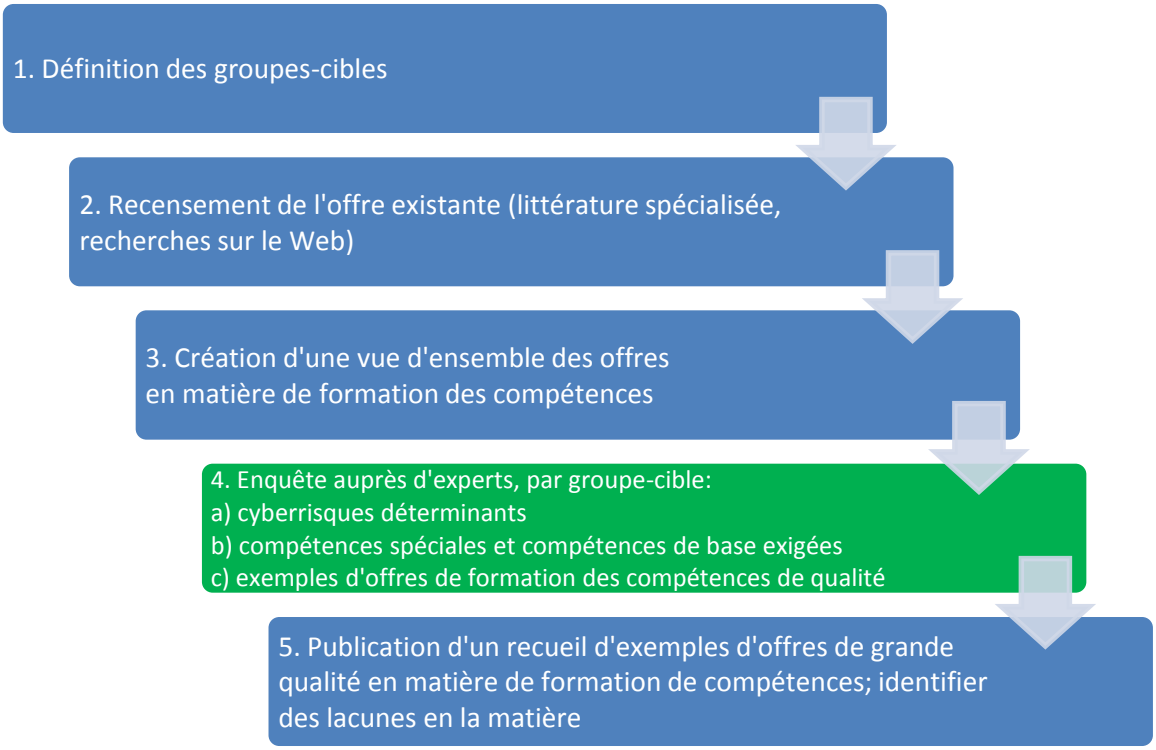
La mesure 7 a donc pour but d'informer en fonction de leurs besoins les milieux économiques, l'administration et la population sur les offres de qualité existantes pour la formation des compétences en gestion des cyberrisques. Il s'agit en outre d'identifier les éventuelles lacunes en la matière.

2 Méthode et approche

Pour faire face aux cyberrisques, il faut des compétences variées et qui diffèrent beaucoup, en fonction des objectifs de protection ou des tâches et responsabilités assumées dans l'économie, dans l'administration ou la société civile. Le choix s'est donc porté, pour le volet d'enquête du présent travail, sur un modèle différencié par groupe-cible, avec une approche qualitative sous forme de questionnement d'experts, et une recherche approfondie dans la littérature spécialisée et sur Internet.
Le choix d'une approche qualitative offre une grande liberté pour la collecte d'informations – ce qui paraissait judicieux, compte tenu du caractère encore peu exploré du thème. D'un autre côté, une démarche qualitative ne permet pas de constatations représentatives. Même les offres de formation des compétences signalées par les experts comme étant de grande qualité pour leur groupe-cible n'ont qu'une valeur d'exemple et ne peuvent être considérées comme exhaustives.

[1] Pour plus de détails sur le mandat concernant la mesure 7, voir la stratégie SNPC (pp. 38/39) et son plan de mise en œuvre (p. 23): www.isb.admin.ch/themen/01709/index.html?lang=fr

Les étapes suivantes ont été définies:



Graphique 1: Etapes de mise en œuvre de la mesure 7 de la SNPC

3 Mise en œuvre

3.1 Groupes-cibles

La stratégie donne des groupes-cibles une définition large et sommaire: les acteurs issus de l'économie, de l'administration et de la société civile doivent être en mesure de minimiser sur le plan suisse les cyberrisques. Les groupes-cibles ont été affinés et définis comme suit:

Groupe-cible: société civile
Grand public
Responsables de l'éducation et de la formation, en tant qu'intermédiaires auprès des enfants et des adolescents (p. ex. parents, corps enseignant, maîtres d'apprentissage, etc.)
Les enfants et les jeunes
Personnes âgées

Groupe-cible: administration
Confédération: cadres
Confédération: responsables de la sécurité (ambassades, Corps des gardes-frontières, préposés à la sécurité informatique, conseillers/délégués à la protection des données, responsables de la protection des objets, etc.)
Confédération: Ministère public de la Confédération
Confédération: collaborateurs
Cantons: autorités de poursuite pénale (police cantonale, ministères publics, tribunaux, etc.)
Cantons/grandes villes: responsables informatiques et de la sécurité informatique
Cantons/grandes villes: collaborateurs

Groupe-cible: économie
Grandes entreprises
PME: choix de branches où la communication/les interactions sont essentielles
Exploitants d'infrastructures critiques[2]

3.2 Enquête auprès d'experts

Des experts ont été identifiés pour tous les groupes-cibles et interrogés sur les cyberrisques pertinents dans leur cas.

L'enquête auprès d'experts portait sur les thèmes suivants:

a) cyberrisques : la stratégie ne précise pas pour quels cyberrisques actuels il faut former les compétences et donc recenser l'offre existante. Selon le groupe-cible, l'accent est mis ici sur des compétences différentes dans les domaines technique, juridique, organisationnel, pédagogique, en économie d'entreprise, etc.

b) compétences-clés et compétences de base requises: chaque groupe-cible a besoin de certaines compétences élémentaires (de base) et d'autres plus spécifiques (compétences-clés). L'enquête auprès des experts doit permettre de recueillir 4 ou 5 compétences-clés par groupe-cible. Elles serviront à réduire l'éventail des offres existantes de formation des compétences, à répertorier dans une prochaine étape.

c) exemples de bonnes pratiques: il s'agit ici de connaître l'avis personnel des experts interrogés, soit lesquelles des offres existantes ils recommanderaient à leur groupe-cible, comme exemples de bonnes pratiques.

d) lacunes de l'offre: tout indique qu'il n'existe pas d'offre adaptée et facile d'accès pour chaque compétence qu'un groupe-cible juge nécessaire. Les experts sont interrogés ici sur les lacunes de l'offre.

L'enquête a principalement consisté en interviews téléphoniques, mais aussi en entretiens personnels. Elle avait pour canevas un questionnaire spécialement conçu par l'iimt (international institute of management in technology) de l'Université de Fribourg, complété et adapté en fonction des groupes-cibles.

-> Le questionnaire figure en annexe du présent document.
(annexe 1 : questionnaire destiné aux organisations exposées aux cyberrisques ;
annexe 2 : questionnaire destiné aux intermédiaires auprès des groupes-cibles)

[2] Exploitants d'IC des sous-secteurs présentant une criticité très importante et hôpitaux, ainsi que leurs fournisseurs: approvisionnement en électricité, approvisionnement en pétrole, banques, technologies de l'information, télécommunications, approvisionnement en eau, trafic ferroviaire et trafic routier. Voir la stratégie nationale pour la protection des infrastructures du 27 juin 2012, FF **2012** 7177, www.admin.ch/opc/fr/federal-gazette/2012/7173.pdf.

Annexe 1:
Questionnaire destiné aux organisations exposées aux cyberrisques

1. Cyberrisques présents dans votre domaine

1 a. Quels sont, selon vous, les cyberrisques à craindre dans votre organisation?

1 b. Dans quelle mesure vos activités opérationnelles y sont-elles exposées?

1 c. Disposez-vous de documents internes / guides / normes sur la gestion des cyberrisques ou cyberattaques?
-> Si oui, continuer avec 1d; sinon, passer à 1e

1 d. Avez-vous obtenu une certification de sécurité? Si oui, laquelle?

1.1 Cybersécurité

1 e. Qui est responsable, dans votre organisation, de la protection contre les cyberrisques?

1 f. Relations avec les partenaires commerciaux / les fournisseurs. Un travail de sensibilisation aux cyberrisques est-il effectué? Donnez-vous ou recevez-vous des directives?

2. Compétences nécessaires

2 a. Connaissez-vous des offres de cours / de formation portant sur les cyberrisques?
-> Nouvelle question portant sur les associations professionnelles, les hautes écoles (spécialisées), etc.

2 b. Avez-vous participé personnellement à une telle offre de perfectionnement?

2 c. Proposez-vous à vos collaborateurs des cours/formations continues sur ce thème? Si oui, lesquels (offre interne/externe)?

2 d. Avez-vous instauré dans votre organisation une culture de la sécurité informatique, ou existe-t-il dans votre entreprise une politique de sécurité des TIC?

2 e. A votre avis, quelles compétences faut-il avoir pour maîtriser les cyberrisques?
-> Nouvelle question sur les compétences de base / les compétences spéciales.

3. Exemples de bonnes pratiques

3 a. Connaissez-vous dans ce contexte des exemples de bonnes pratiques?

3 b. Avez-vous constaté des lacunes dans l'offre actuelle?

Annexe 2:
Questionnaire destiné aux intermédiaires auprès des groupes-cibles

1. Cyberrisques présents dans votre domaine

1 a. Quels sont, selon vous, les cyberrisques à craindre pour votre groupe-cible?

1 b. Dans quelle mesure votre groupe-cible y est-il exposé au niveau opérationnel / dans la vie de tous les jours?

1 c. Disposez-vous, pour votre groupe-cible, de documents / guides / normes sur la gestion des cyberrisques ou cyberattaques?

1 d. Relations avec les intermédiaires/experts (p. ex. responsables de la formation servant de relais auprès des jeunes). Les intermédiaires sont-ils dûment sensibilisés aux cyberrisques et se conforment-ils aux directives à ce sujet?

2. Compétences nécessaires

2 a. Connaissez-vous des offres de cours / de formation portant sur les cyberrisques?
-> Nouvelle question portant sur les associations professionnelles, les hautes écoles (spécialisées), etc.

2 b. Avez-vous participé personnellement à une telle offre de perfectionnement?

2 c. Proposez-vous à votre groupe-cible des cours/formations continues sur ce thème? Si oui, lesquels (offre interne/externe)?

2 d. Avez-vous établi dans votre groupe-cible des règles visant à instaurer une culture de la sécurité informatique?

2 e. A votre avis, de quelles compétences votre groupe-cible a-t-il besoin pour maîtriser les cyberrisques?
-> Nouvelle question sur les compétences de base / les compétences spéciales

3. Exemples de bonnes pratiques

3 a. Connaissez-vous dans ce contexte des exemples de bonnes pratiques?

3 b. Avez-vous constaté des lacunes dans l'offre actuelle?

Annexe 2 – Experts consultés

Les experts consultés provenaient notamment des entreprises, administrations et associations suivantes:

- Etat-major de l'armée PIO, Protection des informations et sécurité industrielle SIS (DDPS)
- Baloise Group
- Office fédéral de l'informatique et de la télécommunication OFIT (DFF), CSIRT
- Office fédéral des assurances sociales OFAS (DFI)
- Ministère public de la Confédération, Informatique et services centraux
- Ministère public de la Confédération, Protection de l'État et délits spéciaux
- Comlab SA
- Société Coopérative Coop
- Service informatique, canton de Lucerne
- Direction des ressources DFAE, domaines de la sécurité
- Division criminalité économique et entraide judiciaire
- educa.ch – Institut suisse des médias pour la formation et la culture
- Préposé fédéral à la protection des données et à la transparence (PFPDT) (ChF)
- Office fédéral du personnel OFPER (DFF)
- FKB BCF – Banque Cantonale de Fribourg
- Base d'Aide au Commandement BAC (DDPS), Computer Network Operations CNO
- Hostpoint SA
- Service informatique, canton d'Argovie
- Unité de pilotage informatique de la Confédération UPIC-MELANI (DFF)
- Unité de pilotage informatique de la Confédération UPIC-SEC (DFF)
- ISSS – Information Security Society Switzerland
- Police cantonale de Saint-Gall
- Ministère public central
- Service de renseignement de la Confédération SRC-OIC ME-LANI (DDPS)
- Pro Juventute
- Pro Senectute canton de Saint-Gall
- République et Canton de Genève, Direction générale des systèmes d'information
- République et Canton du Jura, Service Informatique
- CFF SA
- Association suisse des banquiers
- Prévention Suisse de la Criminalité PSC
- Science Industries Switzerland, Association des industries Chimie Pharma Biotech
- SRG SSR – Société suisse de radiodiffusion et télévision
- Ministère public du canton de Zurich

Annexe 2- Experts

- Swisscom SA, Team Corporate Responsibility
- Swissmedic – Institut suisse des produits thérapeutiques (DFI)
- Swissmem
- SWITCH
- Unité de sécurité des systèmes d'informations VD

Annexe 3 – Ouvrages de référence

Voici une liste des principaux ouvrages de référence consultés (état avril 2014). Ils mettent davantage l'accent sur une gestion prometteuse des cyberrisques que sur l'introduction d'une application technique.

[CARD2011] A. Cárdenas, S. Amin, Z. Lin, Y. Huang, C. Huang, S. Sastry: Attacks Against Process Control Systems: Risk Assessment, Detection, and Response. Proceedings of the 6th ACM Symposium on Information, Computer and Communications Security (ASIACCS '11), Hong Kong, 2011. http://dl.acm.org/citation.cfm?id=1966959

[ENISA2012a] European Network and Information Security Agency: National Cyber Security Strategies - Practical Guide on Development and Execution. ENISA, Heraklion, 2012. http://www.enisa.europa.eu/activities/Resilience-and-CIIP/national-cyber-security-strategies-ncsss/national-cyber-security-strategies-an-implementation-guide

[ENISA2012b] European Network and Information Security Agency: National Cyber Security Strategies - Setting the course for national efforts to strengthen security in cyberspace. ENISA, Heraklion, 2012. http://www.enisa.europa.eu/activities/Resilience-and-CIIP/national-cyber-security-strategies-ncsss/national-cyber-security-strategies-an-implementation-guide

[GOOD2013] C. Goodwin, J. Nicholas: Developing a National Strategy for Cybersecurity. Microsoft Corp., Redmond, 2013. http://www.google.ch/url?sa=t&rct=j&q=&esrc=s&source=web&cd=2&ved=0CD4QFjAB&url=http%3A%2F%2Fdownload.microsoft.com%2Fdownload%2FB%2FF%2F0%2FBF05DA49-7127-4C05-BFE8-0063DAB88F72%2FDeveloping_a_National_Strategy_for_Cybersecurity.pdf&ei=lRsPU477F6aNywOt2oHYBA&usg=AFQjCNHXi7y5Mp25n9vcjl0asq4exuVLAg&bvm=bv.61965928,d.bGQ

[ITU2012] International Telecommunications Unit: The ITU National Cybersecurity Strategy Guide. ITU, Geneva, 2012. http://www.itu.int/ITU-D/cyb/cybersecurity/docs/ITUNationalCybersecurityStrategyGuide.pdf

[JULI2012] K. Julisch: Understanding and overcoming cyber security anti-patterns. Journal on Computer Networks, Vol. 57, 2013, pp. 2206 – 2211. http://www.sciencedirect.com/science/article/pii/S1389128613000388

[KOUN2010] J. Kouns, D. Minoli: Information Technology Risk Management in Enterprise Environments – A Review of Industry Practices. John Wiley & Sons, Hoboken, 2010. http://eu.wiley.com/WileyCDA/WileyTitle/productCd-0471762547.html

[KRIT2010] E. Kritzinger, S. von Solms: Cyber security for home users: A new way of protection through awareness enforcement. Journal of Computers & Security, Volume 29, Issue 8, 2010, pp. 840–847 http://www.sciencedirect.com/science/article/pii/S0167404810000775

[LECL2013] J. LeClair, S. Abraham, L.Shih: An Interdisciplinary Approach to Educating an Effective Cyber Security Workforce. Proceedings of the InfoSecCD '13: Information Security Curriculum Development Conference, Kennesaw, 2013. http://dl.acm.org/citation.cfm?id=2528923

[LUII2013] E. Luiijf, K. Besseling, P. De Graaf: Nineteen national cyber security strategies. International Journal of Critical Infrastructures, Volume 9, Issue 1, pp. 3-31, 2013. http://www.inderscience.com/info/inarticle.php?artid=51608

[NICH2011] A. Nicholson, S. Webber, S. Dyer, T. Patel, H. Janicke: SCADA security in the light of Cyber-Warfare. Journal of Computers and Security, Volume 31, 2012, pp. 418 – 436. http://www.sciencedirect.com/science/article/pii/S0167404812000429

[NCSC2013] National Cyber Security Centre: Cyber Security Assessment Netherlands. National Cyber Security Centre, The Hague, 2013. https://www.google.ch/search?q=National+Cyber+Security+Centre:+Cyber+Security+Assessment+Nether-lands&ie=utf-8&oe=utf-8&rls=org.mozilla:en-US:official&client=firefox-a&gfe_rd=ctrl&ei=gxcPU9ncMabD8gf0yYHgCA&gws_rd=cr#q=National+Cyber+Security+Centre:+Cyber+Security+Assessment+Nether-lands&rls=org.mozilla:en-US:official&spell=1

[NRECA2011] National Rural Electric Cooperative Association: Guide to Developing a Cyber Security and Risk Mitigation Plan. Dulles, 2011. https://www.smartgrid.gov/sites/default/files/doc/files/CyberSecurity-GuideforanElectricCooperativeV11-2%5B1%5D.pdf

[PFLE2012] S. Pfleeger, D. Caputo: Leveraging Behavioral Science to Mitigate Cyber Security Risk. Journal of Computers and Security, Volume 31, 2012, pp. 597–611. http://www.sciencedirect.com/science/article/pii/S0167404811001659

[SOLM2013] R. von Solms, J. van Niekerk: From information security to cyber security. Journal of Computers and Security, Vol. 38, 2013, pp. 97 – 102. http://ac.els-cdn.com/S0167404813000801/1-s2.0-S0167404813000801-main.pdf?_tid=35497348-9fa0-11e3-b1c7-00000aacb362&acdnat=1393499798_b90774ced2f9d1c1df8bed2ceba725f4

[WANG2013] W. Wang, Z. Lu: Cyber security in the Smart Grid: Survey and challenges. Journal of Computer Networks, Vol. 57, 2013, pp. 1344 – 1371. http://www.sciencedirect.com/science/article/pii/S1389128613000042