OPRISKO.ch

Observatoire des Risques Opérationnels

# OBSERVATOIRE DES RISQUES OPERATIONNELS

UNE ASSOCIATION À BUT NON LUCRATIF

Ateliers

# Cybercriminalité

## Restitution des travaux du 15 septembre 2017

Cyrille Reynard

Operational Risk Observatory
OpRiskO

*10 novembre 2017 SwissMadeSecurity*

Oprisko.ch – c.reynard@oprisko.ch

OPRISKO.ch

Observatoire des Risques Opérationnels

# Normes étatiques de cyber sécurité imposées par l'Etat

***Imaginez que l'Etat impose aux entreprises privées ou publiques de nouvelles normes règlementaires liées à la cyber sécurité (exemple normes de sécurité de base, détection et réaction, prévention).***

*Dans ce cas, quels seraient les défis/problèmes pour ces entreprises?*

- Animateurs : **Dan Bihi-Zenou et Pablo Faus Perez**

OPRISKO.ch

Observatoire des Risques Opérationnels

# Normes étatiques de cyber sécurité imposées par l'Etat

***Dans ce cas, quels seraient les défis/problèmes pour ces entreprises?***

**Défi**

***Définir*** *et* ***contrôler*** *de l'application des normes ?*

**Solutions retenues :**

**Créer un « label » / certification « auditable » de manière standard**

**Commentaires :**

Présenter la norme comme un avantage compétitif.

OPRISKO.ch

Observatoire des Risques Opérationnels

# Normes étatiques de cyber sécurité imposées par l'Etat

***Dans ce cas, quels seraient les défis/problèmes pour ces entreprises?***

**Défi**

***Définir*** *et* ***contrôler*** *de l'application des normes ?*

**Solutions retenues :**

**Adopter de manière structurée et progressive ces normes**

**Commentaires :**

Les normes doivent être crées en cascade (i.e. : directives, normes, procédures.). Elles doivent être définies par consensus et leur implémentation échelonnée dans le temps.

**Ne pas se baser sur des normes ISO, trop compliqué peu adapté aux PMEs.**

OPRISKO.ch

Observatoire des Risques Opérationnels

# Normes étatiques de cyber sécurité imposées par l'Etat

***Dans ce cas, quels seraient les défis/problèmes pour ces entreprises?***

**Défi**

***Définir*** *et* ***contrôler*** *de l'application des normes ?*

Autre solution :

**Adopter un standard / référentiel flexible**

**Commentaires :**

Le référentiel doit pouvoir évoluer, être adaptable au type d'entreprise et être résilient.

**Evoqué la nécessité de créer un standard propre à la Suisse.**

OPRISKO.ch

Observatoire des Risques Opérationnels

# Normes étatiques de cyber sécurité imposées par l'Etat

***Dans ce cas, quels seraient les défis/problèmes pour ces entreprises?***

**Défi**

***Définir** et **contrôler** de l'application des normes ?*

Autre solution

**Adopter des normes sectorielles**

**Commentaires :**

Les normes pourront varier par secteur afin de répondre aux spécificités

**P.ex. : FINMA pour les banques.**

OPRISKO.ch

Observatoire des Risques Opérationnels

# Normes étatiques de cyber sécurité imposées par l'Etat

***Dans ce cas, quels seraient les défis/problèmes pour ces entreprises?***

**Défi**

***Définir*** *et* ***contrôler*** *de l'application des normes ?*

**Autres solutions :**

**Edicter des principes et non pas de règles détaillées.**

**Commentaires :**
Les normes doivent être « principle based » et « risk-based » pour laisser aux entreprises la flexibilité d'adapter les règles à leur business, risques.

**Contrôler de ces normes par des « peers ».**

**Commentaires :**
Créer au sein de chaque secteur d'activité des organes de contrôle composés par des professionnels du secteur. Orchestrer les contrôles de l'application des principes par sondage au niveau de l'état.

OPRISKO.ch

Observatoire des Risques Opérationnels

- Intervention de Yves Le-Thiec :

# *Comment créer un label standard sous forme de norme en matière de sécurité des systèmes d'information pour les industries critiques et les autres entreprises ?*

- Sous-directeur adjoint de l'Agence nationale de la sécurité des systèmes d'informations en France (ANSSI) de 2013 à 2016.
- **Responsable du pilotage des systèmes d'informations à l'Etat-major des armées depuis 2016.**
- Actuellement consultant en cyber sécurité et PDG de HurbanIT, entreprise spécialisée dans la protection et la sauvegarde du patrimoine informationnel.

https://youtu.be/zC506spuoGQ?t=3m15s

OPRISKO.ch

Observatoire des Risques Opérationnels

# Obligation d'annonce des incidents auprès d'un organisme (cantonal/fédéral).

***Imaginez que l'Etat impose aux entreprises privées ou publiques victimes d'une attaque de communiquer les cas auprès d'un organisme central (cantonal, fédéral). Dans ce cas, quels seraient les défis/problèmes pour ces entreprises ?***

*Dans ce cas, quels seraient les défis/problèmes pour ces entreprises?*

- Animateur : **Jean-Jaques Kohler et Bénédict Mugnier**

OPRISKO.ch

Observatoire des Risques Opérationnels

# Obligation d'annonce des incidents auprès d'un organisme (cantonal/fédéral).

***Dans ce cas, quels seraient les défis/problèmes pour ces entreprises?***

**1er défi**

*Garantir la confidentialité*

**Solution retenue :**

**Référentiel d'incidents commun des entreprises**

**Commentaires :**

Mettre en place d'une clause de confidentialité. L'anonymisation des rapports est indispensable et la possibilité de revenir sur sa déclaration.

**Autres solutions :**

**Utilisation d'une technologie blockchain.**

**Commentaires :**

Permet de garantir la confidentialité
Permet la centralisation
Empêche la corruption de l'information

OPRISKO.ch

Observatoire des Risques Opérationnels

# Obligation d'annonce des incidents auprès d'un organisme (cantonal/fédéral).

***Dans ce cas, quels seraient les défis/problèmes pour ces entreprises?***

**1er défi**

*Garantir la confidentialité*

**Autres solutions :**

**Gestion et communication des incidents**

**Commentaires :**

Annonces anonymes avec délai d'annonce contraignant (pas à la carte). Produire un reporting et fournir des éléments pour contrer l'attaque une fois le reporting fait.

*Hors atelier, dans l'étude Oprisko 2017 les entreprises souhaitent que l'état coordonne la réponse face à des incidents globaux.*

OPRISKO.ch

Observatoire des Risques Opérationnels

# Obligation d'annonce des incidents auprès d'un organisme (cantonal/fédéral).

***Dans ce cas, quels seraient les défis/problèmes pour ces entreprises?***

**2ème défi**

*Définir / Normer le référentiel incident*

**Solution retenue :**

**-Adopter un référentiel mondial et l'adapter à la situation locale mais surtout informer et délivrer l'information.**

**-Formulaire d'annonce avec catégories prédéfinies**

**-e-learning à disposition pour l'annonceur et pour tous les collaborateurs.**

OPRISKO.ch

Observatoire des Risques Opérationnels

# Obligation d'annonce des incidents auprès d'un organisme (cantonal/fédéral).

***Dans ce cas, quels seraient les défis/problèmes pour ces entreprises?***

**3ème défi**

*Avoir les bons outils*

**Solution retenue : (outils)**

**-Mettre en place des procédures / scénarios.**

**-Les entrainements et des exercices avec des scenarios cyber.**

**-plan d'action commun avec partage d'expérience.**

**-implémenter selon typologie de l'entreprise.**

OPRISKO.ch

Observatoire des Risques Opérationnels

# Obligation d'annonce des incidents auprès d'un organisme (cantonal/fédéral).

***Dans ce cas, quels seraient les défis/problèmes pour ces entreprises?***

**4 ème défi**

*Avoir les bonnes compétences*

**Solution retenue : (compétence)**

**- Information et formation de l'ensemble du personnel avec l'aide de l'Etat et des fédérations professionnelles.**

**- programme de sensibilisation face aux risques cyber.**

OPRISKO.ch

Observatoire des Risques Opérationnels

- Intervention de Yves Le-Thiec :

## *Si vous deviez guider l'état de Genève dans mise en place de règles de gestion centralisée des incidents, et communication de ces incidents à l'industrie quelles missions (ou mandat) donneriez-vous à l'administration publique ?*

- Sous-directeur adjoint de l'Agence nationale de la sécurité des systèmes d'informations en France (ANSSI) de 2013 à 2016.
- **Responsable du pilotage des systèmes d'informations à l'Etat-major des armées depuis 2016.**
- Actuellement consultant en cyber sécurité et PDG de HurbanIT, entreprise spécialisée dans la protection et la sauvegarde du patrimoine informationnel.

https://youtu.be/zC506spuoGQ?t=9m

OPRISKO.ch

Observatoire des Risques Opérationnels

# Etendre la compétence et la prise de conscience des employés et le management sur le risque cyber.

*Etendre la compétence et la prise de conscience des employés et le management sur le risque cyber.*

*Imaginez que l'Etat impose aux entreprises privées ou publiques une licence «cyber» pour pouvoir exercer leurs activités.*

***Dans ce cas, quels seraient les défis/problèmes pour ces entreprises?***

- Animateurs : **Erwin Kessler et Maria Tootell**

OPRISKO.ch

Observatoire des Risques Opérationnels

# Licence Cyber : Etendre la compétence et la prise de conscience des employés et le management sur le risque cyber.

***Dans ce cas, quels seraient les défis/problèmes pour ces entreprises?***

**1er défi**

*Inciter les entreprises à mettre en place de nouveaux standards.*

**Solutions retenues :**

**Promouvoir la mesure (mise en place de licence cyber) auprès de l'industrie et population.**
**Story telling -> sensibilisation -> processus**

**Commentaires :**

Faire de la « cyber résilience » un enjeu de sécurité nationale.

Lobby/influence des secteurs économiques/industriels sur la position nécessaire / démarches.

Semaine Cyber dans les écoles.

OPRISKO.ch

Observatoire des Risques Opérationnels

# Licence Cyber : Etendre la compétence et la prise de conscience des employés et le management sur le risque cyber.

***Dans ce cas, quels seraient les défis/problèmes pour ces entreprises?***

**2ème défi**

*PME : manque de ressources financières et humaines.*

**Solutions retenues :**

- **Mise en place de procédures, de recommandations adaptées à l'activité. Rapport, analyse sécurité x fois par année en fonction de l'activité et des moyens.**
- **Mise en place d'un organisme de formation dédié aux différentes tailles et secteurs des PME.**
- **Mutualiser les moyens via l'association de PME, réunir les compétences / ressources. Créer des supports et aides à la conformité. Formation.**
- **Mise en place d'un fonds national suisse réslience d'accompagnement des PME (financer par impôts et taxe dons. )**

OPRISKO.ch

Observatoire des Risques Opérationnels

# Mise en place d'une licence cyber pour les entreprises

***Dans ce cas, quels seraient les défis/problèmes pour ces entreprises?***

**2ème défi**

*PME : manque de ressources financières et humaines. (suite)*

**Solutions retenues : (suites)**

**- Définir un processus d'acquisition et de renouvellement de la licence qui mobilise peu de ressources humaines.**

OPRISKO.ch

Observatoire des Risques Opérationnels

- Intervention de Yves Le-Thiec :

***La France dispose de l'agence nationale de la sécurité des systèmes d'information.***

***Pourriez-vous s'il vous plait décrire le mandat de cet organisme ANSSI, son rôle auprès de l'industrie, et, son mode de financement.***

- Sous-directeur adjoint de l'Agence nationale de la sécurité des systèmes d'informations en France (ANSSI) de 2013 à 2016.
- **Responsable du pilotage des systèmes d'informations à l'Etat-major des armées depuis 2016.**
- Actuellement consultant en cyber sécurité et PDG de HurbanIT, entreprise spécialisée dans la protection et la sauvegarde du patrimoine informationnel.

https://youtu.be/zC506spuoGQ

# Conclusion Cybercriminalité

OPRISKO.ch

Observatoire des Risques Opérationnels

- L'Etat et la majorité des entreprises ne disposent pas d'un dispositif de sécurité des systèmes adéquat.

- Les entrepreneurs proposent des solutions pour améliorer le dispositif étatique aux travers de normes, labels de sécurité et gestion des incidents à grande échelle.

- Nos voisins français ont pris cette problématique très au sérieux avec un organisme étatique de coordination des menaces cyber, doté d'un service de 600 experts 24h/ 7 jours sur 7 et de gestion des incidents.

OPRISKO.ch

Observatoire des Risques Opérationnels

# Merci pour votre attention et

- **Aux sponsors.**

- Enrico Vigano et Raoul Diez.

- **Les responsables d'atelier d'Oprisko :**
  Pablo Faus Perez, Dan Bihi-Zenou,
  Jean-Jaques Kohler, Bénédict Mugnier,
  Maria Tootell et Erwin Kessler

- **Les entrepreneurs qui ont participé aux ateliers.**

*Oprisko.ch accueille avec plaisir de nouveaux membres (actifs, passifs, étudiants)*