Les risques cyber et la cyber assurance

Fédération Française de l'Assurance

CHIFFRES CLÉS DE LA FFA

99 % des sociétés d'assurances en France

1er marché de l'Union européenne post Brexit et **5ème** mondial

37 millions de bénéficiaires d'une assurance vie

2,1 millions d'entreprises assurées

146 200 salariés du secteur

280 entreprises membres

40 millions de contrats habitation

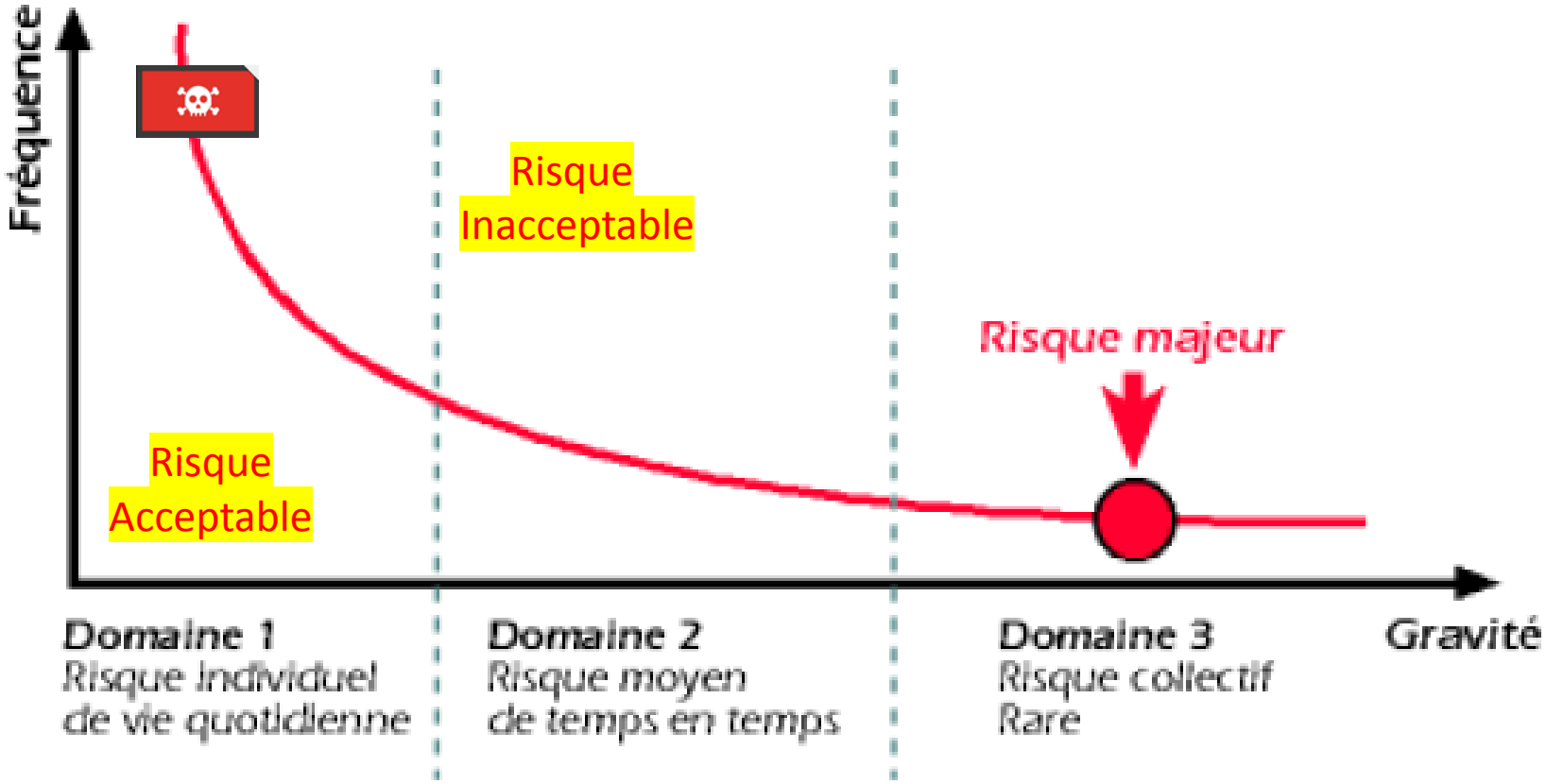
42 millions de véhicules assurés

13,4 millions de sinistres gérés par an

170 collaborateurs

Fédération Française de l'Assurance

Courbe de Farmer



Fédération Française de l'Assurance

2003: California's Database Breach Notification Security Act

2013: Loi relative à la programmation militaire pour les années 2014 à 2019

Fédération Française de l'Assurance

UNDER ARMOUR

Mars 2018

ACCOR FASTBOOKING THINK DIRECT

Juin 2018

intel inside

Janvier 2018

Hillary for President HillaryClinton.com

Juillet 2016

EQUIFAX

Septembre 2017

Janvier 2018

LA RÉPUBLIQUE En Marche !

Avril 2017

Deloitte.

Novembre 2016 à avril 2017

OVH.com

Septembre 2016

SONY

Novembre 2014

Commission européenne

Novembre 2016

BANGLADESH BANK

Avril 2016

TV5MONDE

Avril 2015

TARGET

Décembre 2013

NETFLIX

Spotify

PayPal

Octobre 2016

elysee.fr

Mai 2012

STUXnet

Dès 2007

YAHOO!

Aout 2013

Dec 2014

Les attaques cyber concernent également les administrations, les TPE et PME …

WIKIPEDIA The Free Encyclopedia

Mai 2018

Fédération Française de l'Assurance

BRITISH AIRWAYS

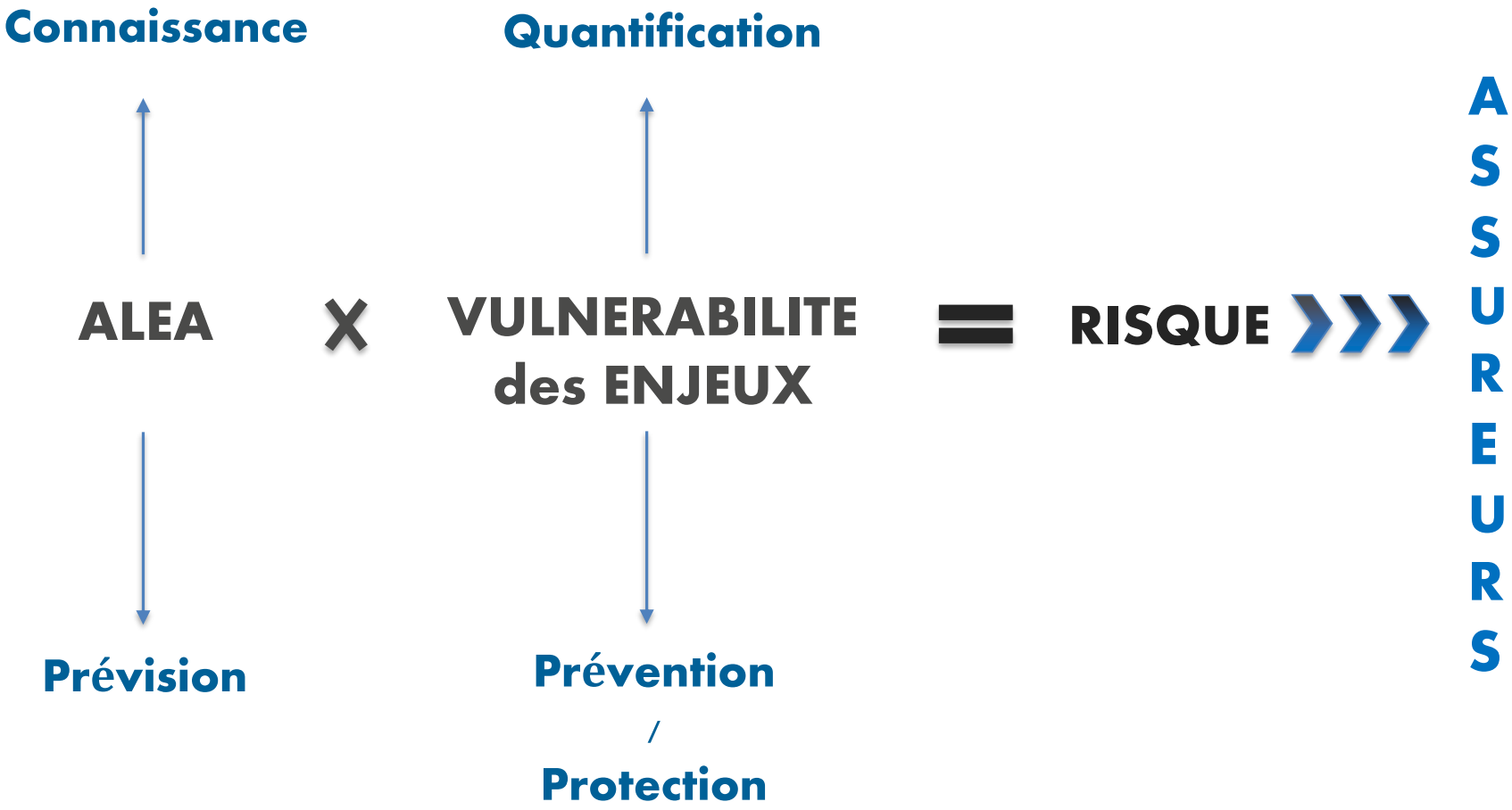
Septembre 2018

Risque = Alea * Enjeux

Risque = Alea * Vulnérabilité des enjeux

Risque = Probabilité * Gravité

Fédération Française de l'Assurance



Fédération Française de l'Assurance

Mettre en place un écosystème favorable au développement de l’assurance cyber

Fédération Française de l’Assurance

I. Les problématiques rencontrées par les assureurs

4 axes de travail :

1. Mieux connaître le risque

2. Maîtriser le cumul des engagements

3. Maîtriser l'environnement juridique

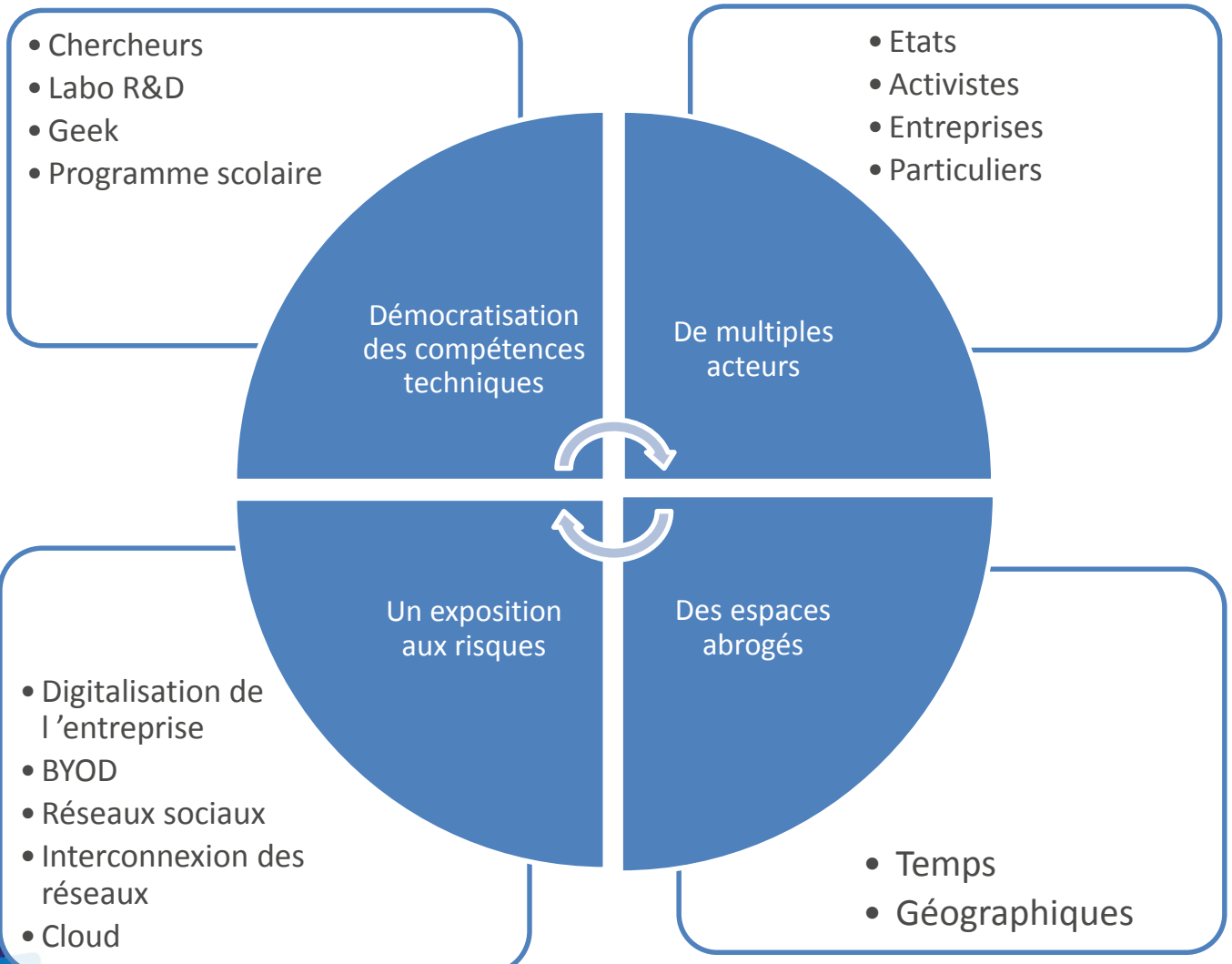
4. Développer la culture du risque

Fédération Française de l'Assurance

4 axes de travail :

1. Mieux connaître le risque

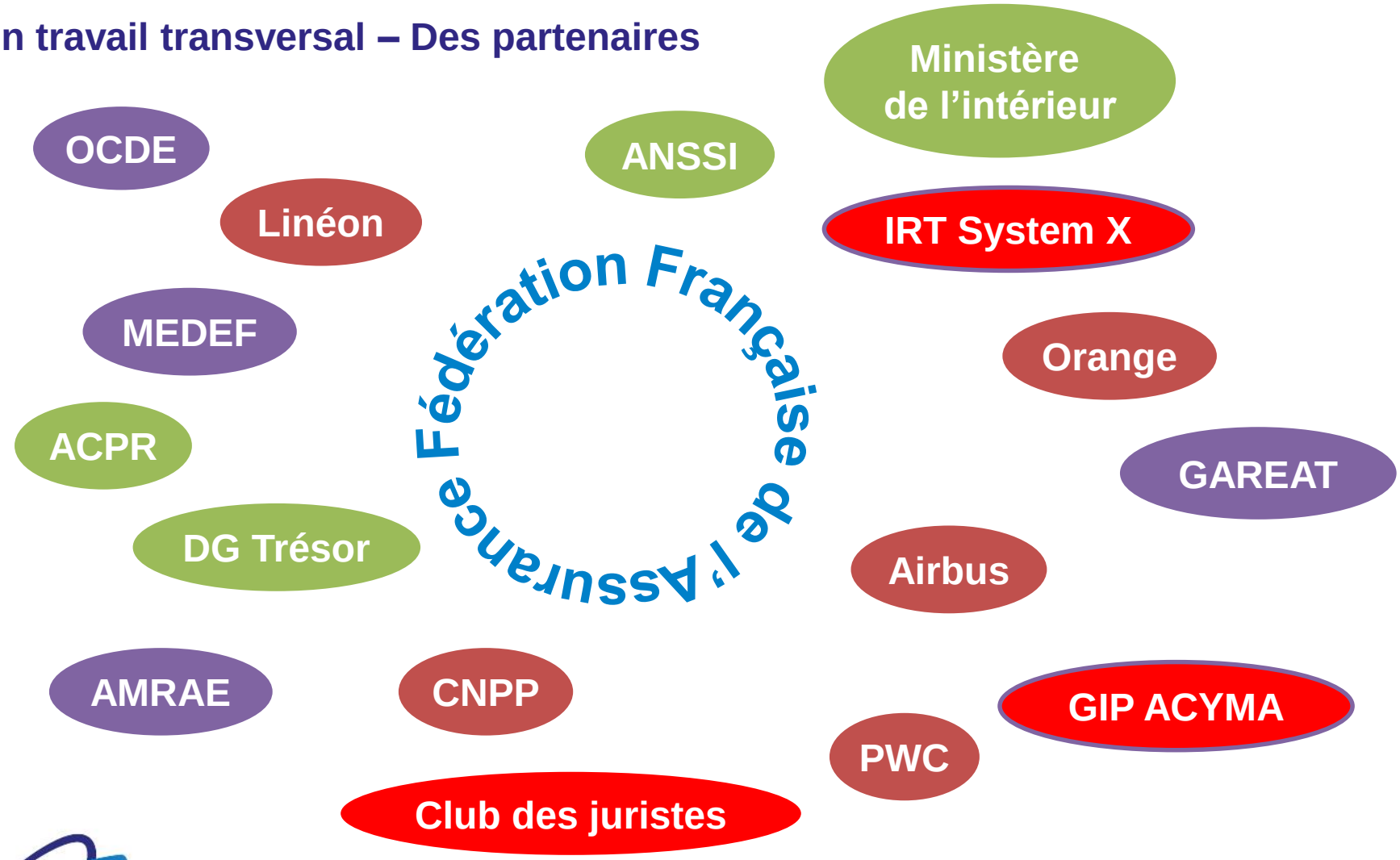
1. Mieux connaitre le risque: Des risques protéiformes



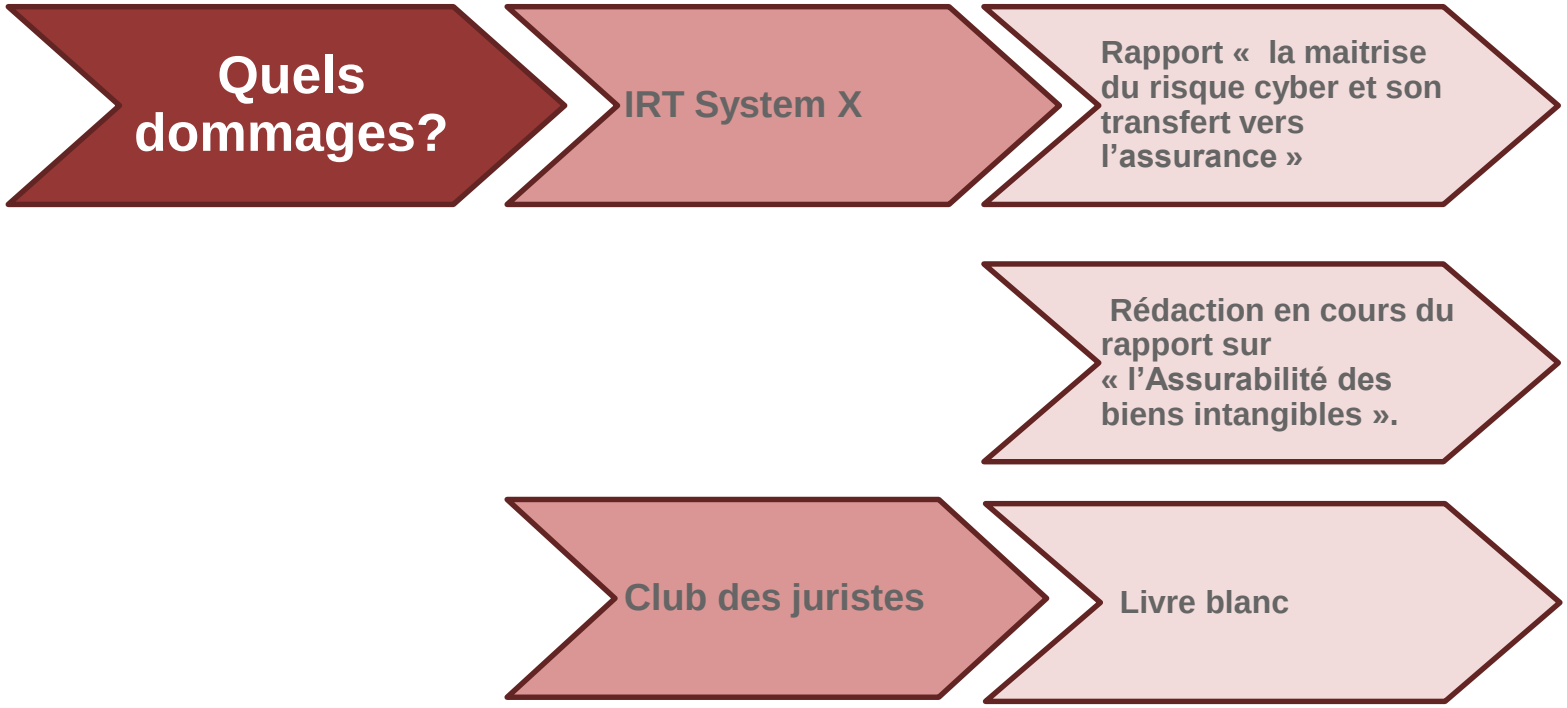
Fédération Française de l'Assurance

1. Mieux connaitre le risque:

Un travail transversal – Des partenaires

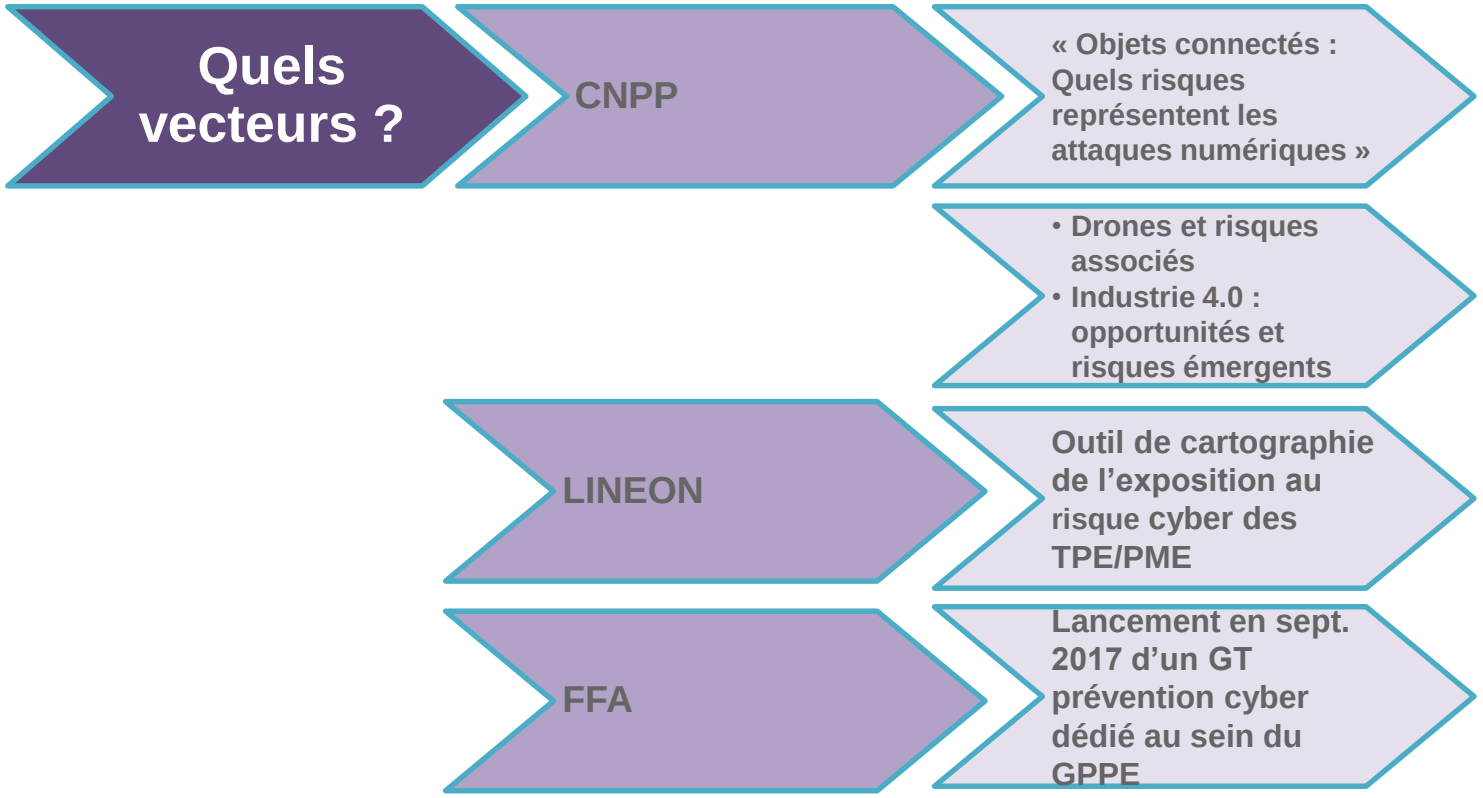


1. Mieux connaître le risque



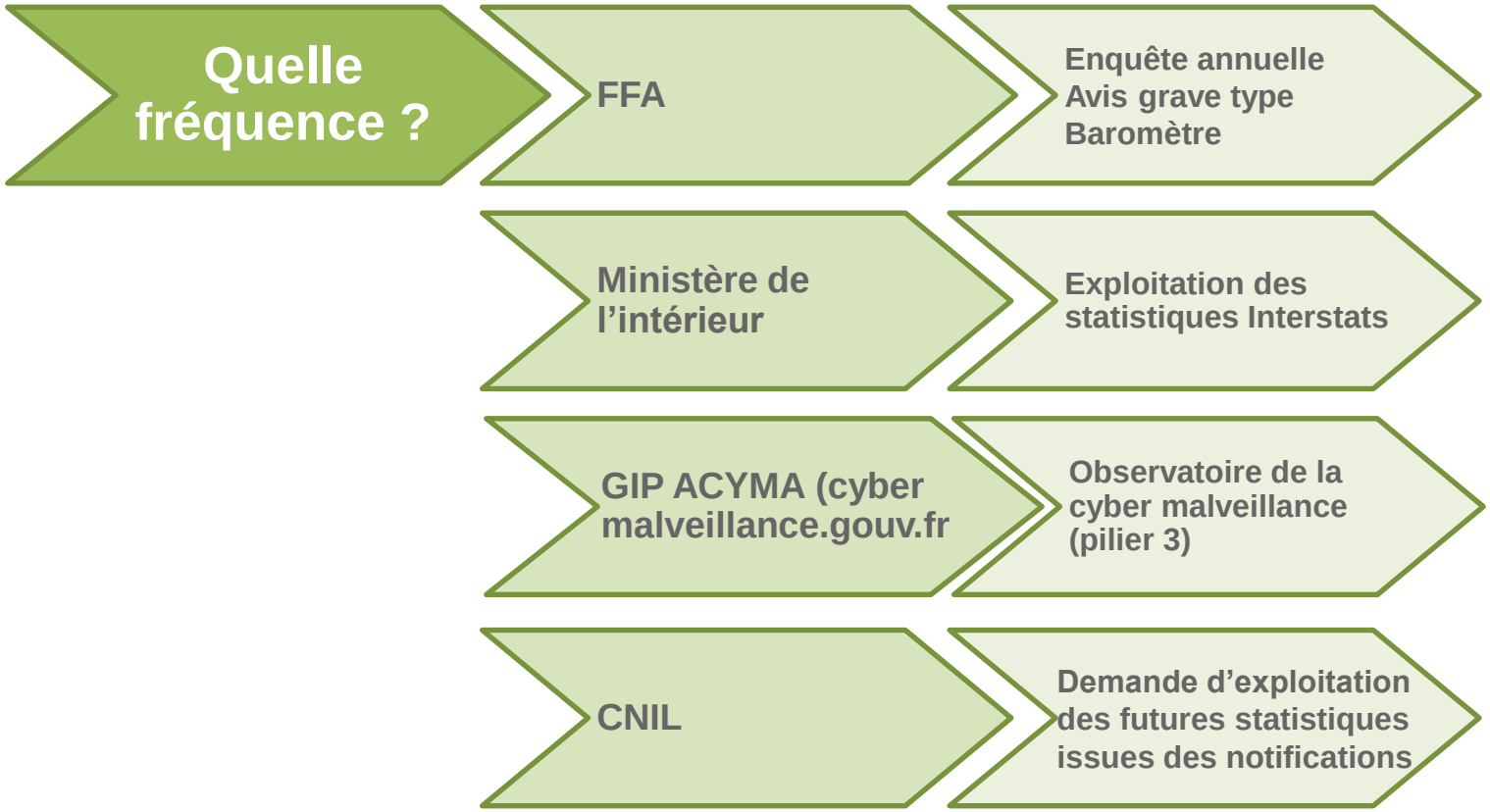
Fédération Française de l'Assurance

1. Mieux connaître le risque



Fédération Française de l'Assurance

1. Mieux connaître le risque



Fédération Française de l'Assurance

4 axes de travail :

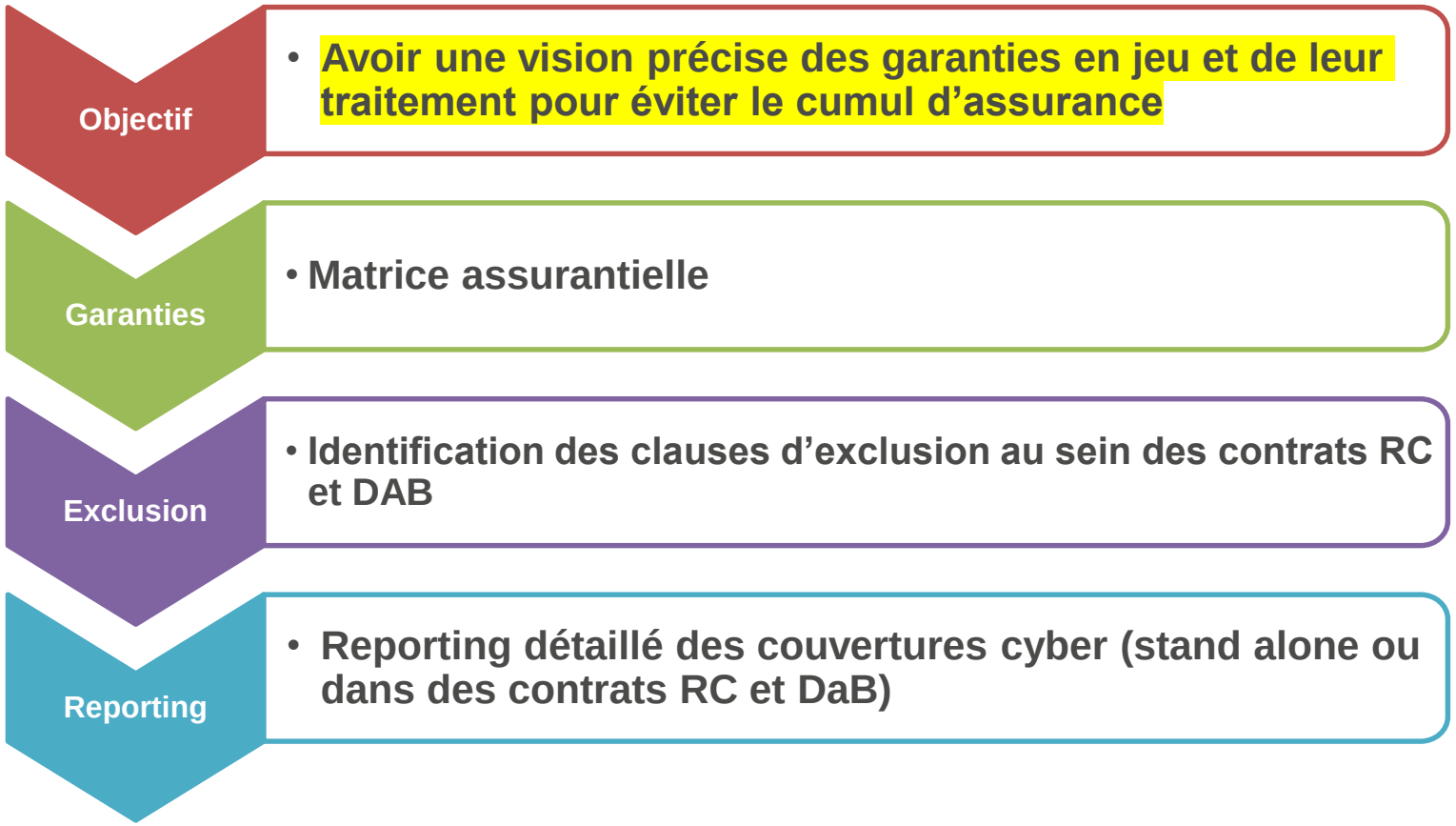
2. Maîtriser le cumul des engagements

Fédération Française de l'Assurance

2. Maîtriser le cumul des engagements

Fédération Française de l'Assurance

2. Maîtriser le cumul des engagements



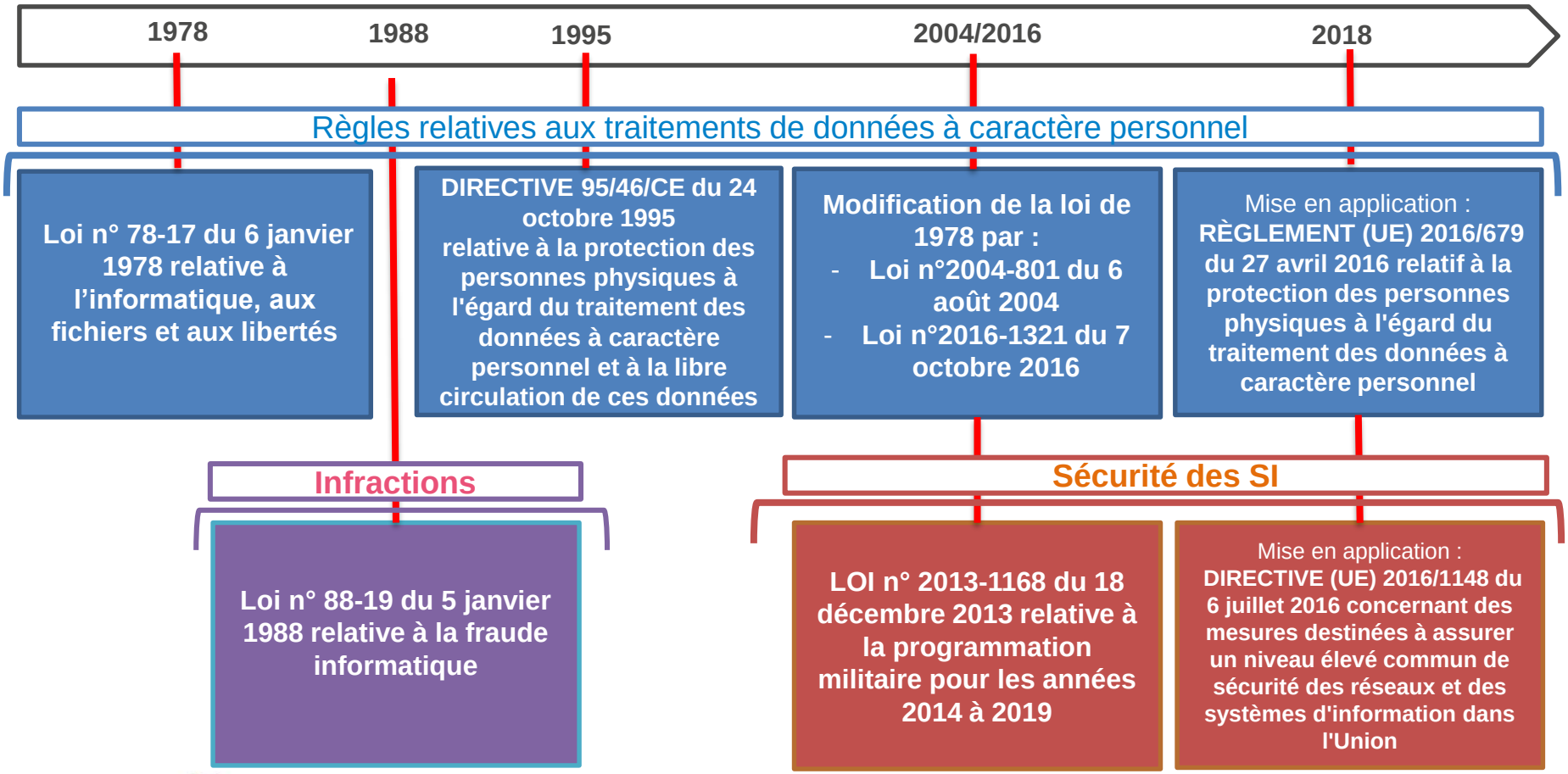
Fédération Française de l'Assurance

4 axes de travail :

3. Maîtriser l’environnement juridique

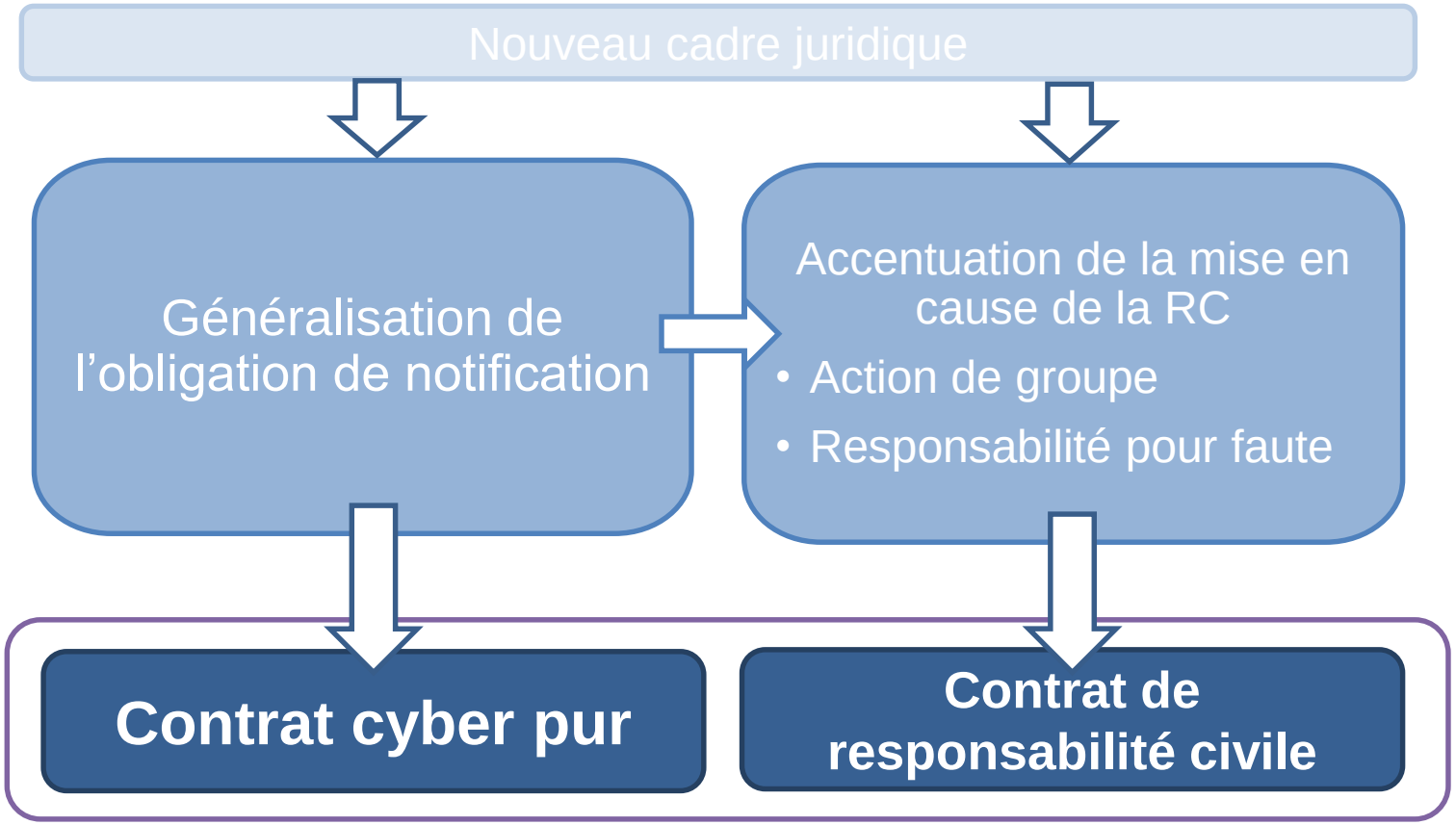
Fédération Française de l’Assurance

3. L'environnement juridique



Fédération Française de l'Assurance

3. L'échéance mai 2018 : un possible booster pour la demande d'assurance



Fédération Française de l'Assurance

3. Maîtriser l'environnement juridique : Des insuffisances du cadre législatif

Amendes administratives

Leur assurance est-elle contraire à l'ordre public (articles 6 du Code Civil, arrêt du 14/02/2012 de la Cour d'Appel de Paris) ?

Rançons

Leur prise en charge est-elle assimilée à du financement du terrorisme (article 421-2-2 du Code pénal) ?

Fédération Française de l'Assurance

4 axes de travail :

4. Développer la culture du risque

Fédération Française de l'Assurance

4. Culture du risque cyber : plaquette de sensibilisation à destination des TPE/PME

- En quoi suis-je concerné par les cyber risques ?
- Protéger mon entreprise
- Assurer mon entreprise
  - Assurer ce qui m'appartient
  - Assurer ma responsabilité vis-à-vis des tiers
  - Assurer mon risque de fraude
- Que faire en cas d'incident informatique ?
- Questions fréquentes

https://www.ffa-assurance.fr/content/anticiper-et-minimiser-impact-un-cyber-risque-sur-votre-entreprise-tpe-pme-vous-etes

Fédération Française de l'Assurance

4. Culture du risque cyber : En partenariat avec le club des juristes – Document de référence sur l'état de l'art en 2018

- Dans un contexte où les entreprises françaises restent encore insuffisamment couvertes contre ce nouveau risque, la Commission Cyber Risk du Club des Juristes, présidée par Bernard Spitz, Président de la FFA, publie un rapport « Assurer le risque cyber » présentant un ensemble de recommandations
- Ce tome 1 présente un éventail de solutions qui permettraient de favoriser l'émergence d'une véritable assurance cyber, suivies de dix préconisations pour une approche globale et efficace du problème

https://www.ffa-assurance.fr/content/assurer-le-risque-cyber-quels-enjeux

Fédération Française de l'Assurance

4. Culture du risque cyber : GIP ACYMA

https://www.cybermalveillance.gouv.fr/

La FFA membre fondateur du GIP ACYMA - 3 missions

1° **Assistance aux particuliers, aux entreprises et aux administrations victimes d'actes de cyber malveillance** par la mise en place d'un « guichet unique ».

2° **Sensibilisation du public sur les enjeux de la sécurité et de la protection de la vie privée numérique** en lien avec les autorités compétentes et le développement de campagnes de prévention en la matière ;

3° Ffourniture d'éléments statistiques offrant une vue réelle et consolidée de la menace cyber afin de mieux l'anticiper à travers la création d'un observatoire dédié.

Fédération Française de l'Assurance

4. Culture du risque cyber : plaquette de sensibilisation à destination des TPE/PME

- Une plaquette réalisée par la FFA pour comprendre les enjeux du RGPD pour les TPE/PME et les collectivités territoriales (juin 2018)

https://www.ffa-assurance.fr/content/protection-des-donnees-personnelles-risques-encourus-et-assurance?parent=79&lastChecked=152

Fédération Française de l'Assurance

4. Culture du risque cyber : plaquette de sensibilisation à destination des TPE/PME

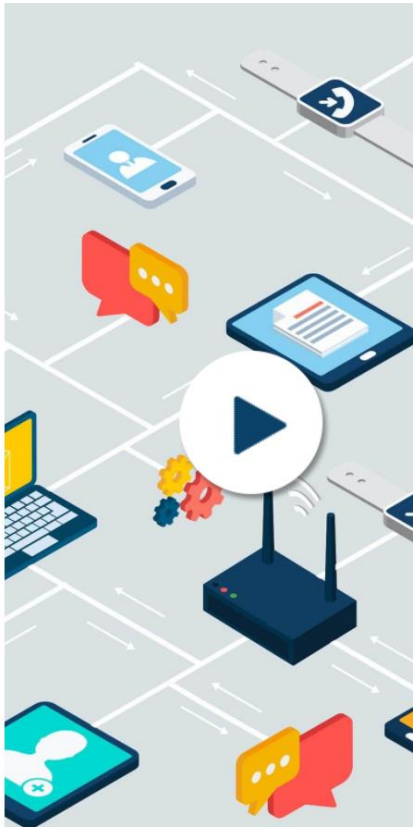
SecNumacadémie.gouv.fr
Formez-vous à la sécurité du numérique

Bienvenue sur le MOOC de l'ANSSI.

Vous y trouverez l'ensemble des informations pour vous initier à la cybersécurité, approfondir vos connaissances, et ainsi **agir efficacement sur la protection de vos outils numériques**. Ce dispositif est accessible gratuitement jusqu'au mois d'avril 2019. Le suivi intégral de ce dispositif vous fera bénéficier d'une attestation de réussite.

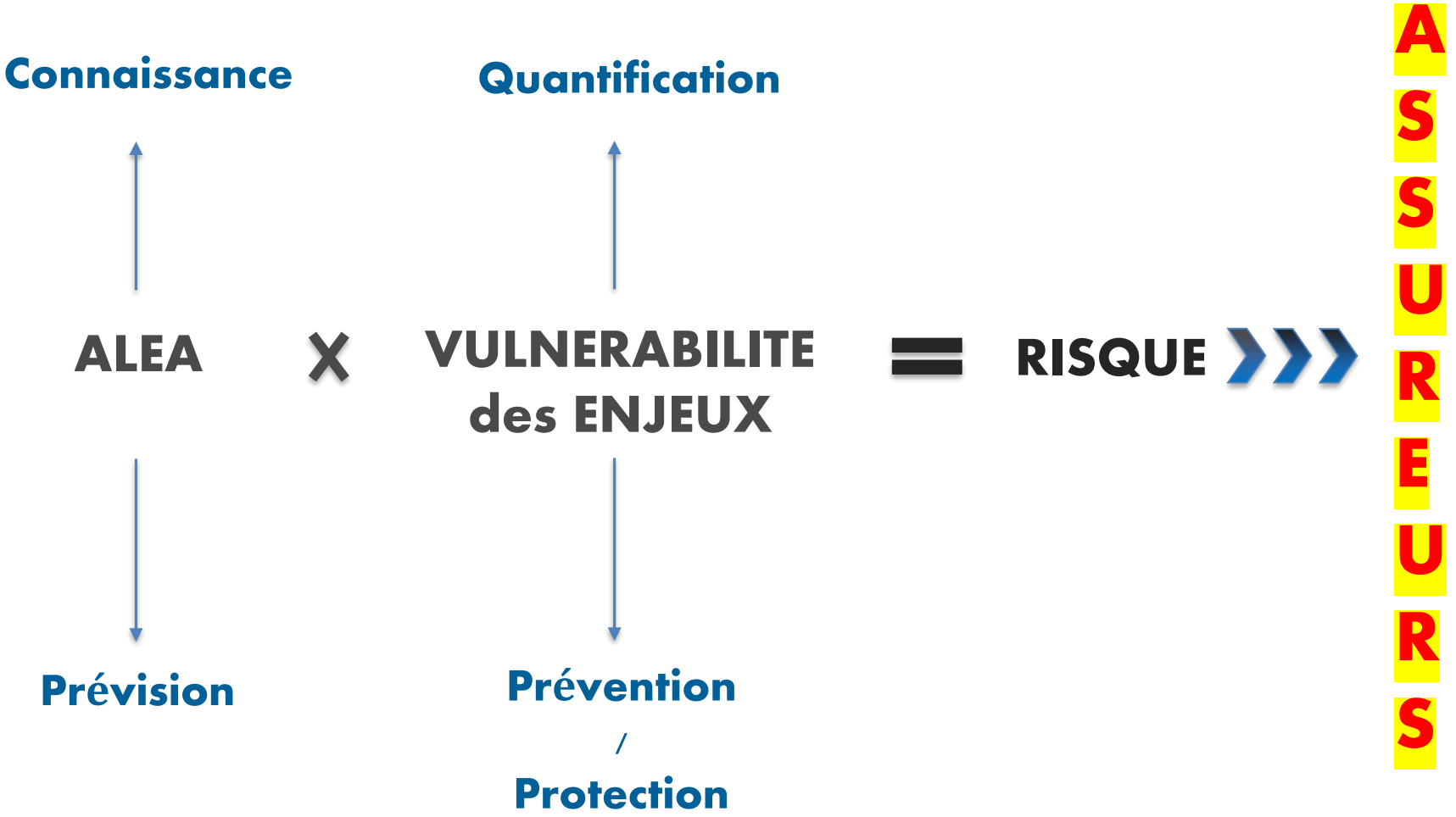
Accéder au MOOC de l'ANSSI

MENTIONS LÉGALES | F.A.Q.



https://www.secnumacademie.gouv.fr/

Fédération Française de l'Assurance

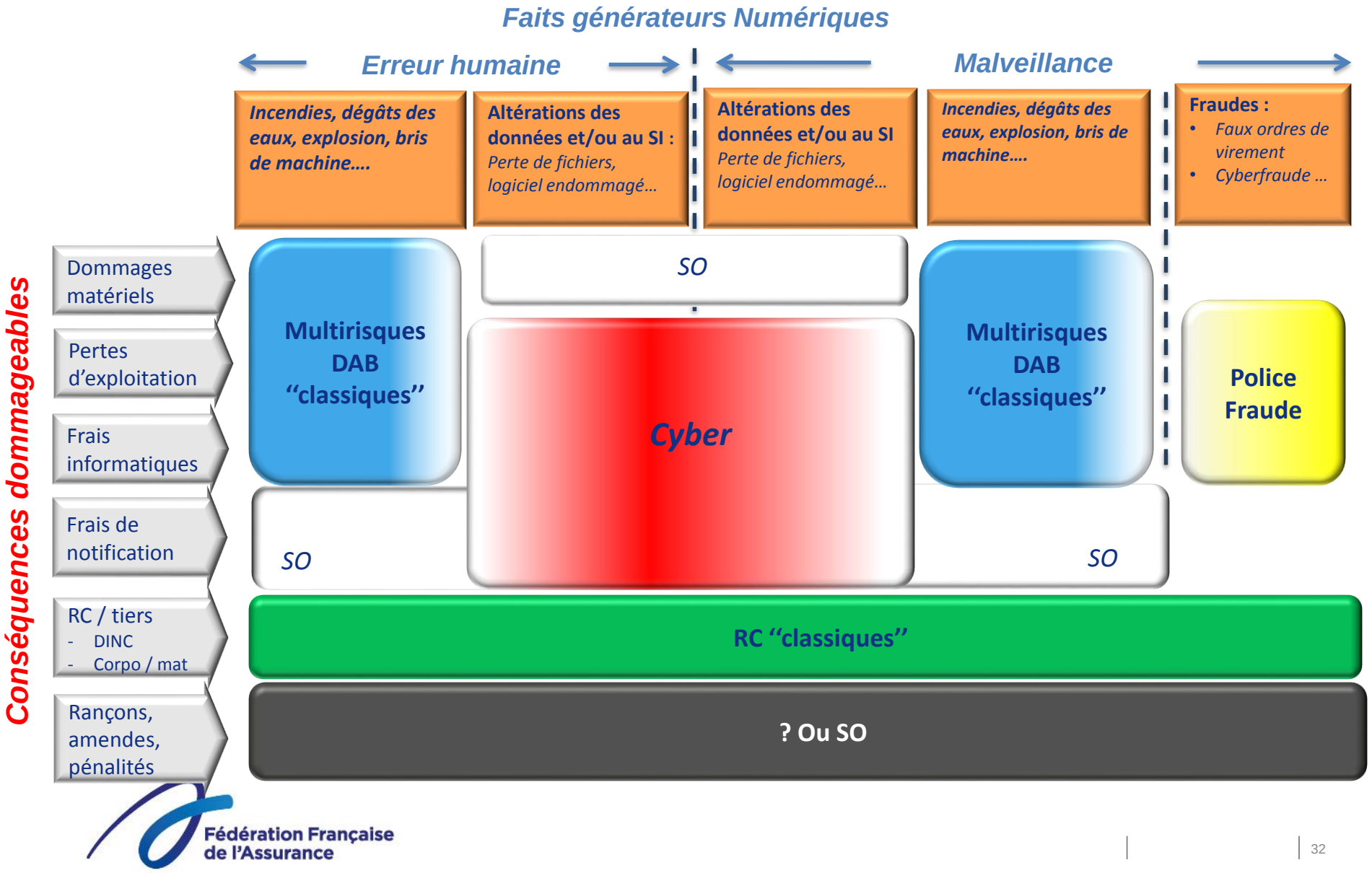


Fédération Française de l'Assurance

II. Le transfert du risque cyber à l'assurance

Les garanties proposées par l'assurance pour faire face aux cyber risques

Les garanties existantes



Fédération Française de l'Assurance

Les garanties existantes

1. Dans les contrats cyber

a. Définition

Le contrat cyber couvre les dommages immatériels et matériels résultant d'un fait générateur cyber accidentel ou non qui peut être :

- Une **erreur humaine** (accidentelle, non intentionnelle) : transmission involontaire de données, téléchargement involontaire d'un logiciel contenant un virus informatique.
- Une **malveillance informatique** (volontaire) : envoi par un hacker d'un virus informatique ou d'un rançongiciel, attaque par déni de service..

Les garanties existantes

1. Dans les contrats cyber

b. Prises en charge

Le contrat cyber peut notamment prendre en charge :

- les frais liés à la **gestion immédiate de l'incident**,

Frais de communication de crise, redirection vers un centre d'appel, recherche de cause « forensic », frais de préservation de la réputation et de l'image de la société ou éventuels frais d'avocat,

- les **conséquences financières directes subies par l'assuré**,

Frais de notification d'une violation de données personnelles, frais de monitoring bancaire, frais nécessités par les enquêtes administratives, frais résultant des éventuelles amendes administratives ou frais résultant d'un piratage téléphonique,

Les garanties existantes

1. Dans les contrats cyber

b. Prises en charge

Le contrat cyber peut notamment prendre en charge :

- les **dommages directs subis par l'assuré**

exemples : reconstitution des données altérées ou perte d'exploitation,

- les frais liés à une **cyber-extorsion**

principalement les frais de consultant spécialisé,

- la **responsabilité civile**

exemples : conséquences financières d'un dommages subis par un tiers, des frais de défense. → Le risque juridique contentieux

Les garanties existantes

1. Dans les contrats cyber

b. Exclusions et interrogations :

Les contrats cyber ne couvrent pas :

- Risque juridique pénal (sanctions pénales)

Des interrogations existent quant à l'assurabilité du :

- Risque juridique financier (sanctions administratives)
- Le paiement des rançons dans le cadre de la cyber-extorsion

La connaissance du risque

INGERENCE ECONOMIQUE

Flash n° 26 - Septembre 2016

Si le recours aux assurances est indispensable pour la pérennité de l'entreprise, notamment face à la montée de risques émergents, il convient de s'assurer du respect de la confidentialité des échanges et des données transmises.

Fédération Française de l'Assurance

Les garanties existantes

2. Dans les contrats de Responsabilité Civile

a. Définition

Les contrats d'assurance de responsabilité civile couvrent **les conséquences financières de la mise en cause de la RC de l'assuré en cas de dommages corporels, matériels et immatériels causés à un tiers**. !

Il s'agit **du risque juridique contentieux.**

Sauf exclusion spécifique, le contrat de RC indemnisera les dommages matériels, immatériels et corporels résultant d'un incident cyber.

Les garanties existantes

3. Dans les contrats de Dommages aux Biens

a. Définition

Les contrats d'assurance de Dommages aux Biens couvrent **les conséquences dommageables (frais de réparation, frais supplémentaires, perte d'exploitation) liés à la survenance d'un risque (incendies, vol, évènements naturels..) aux biens de l'entreprise**.

Sauf exclusion spécifique, ce contrat indemnisera les dommages matériels résultant d'un incident cyber.

III. Cartographie de son exposition aux risques cyber

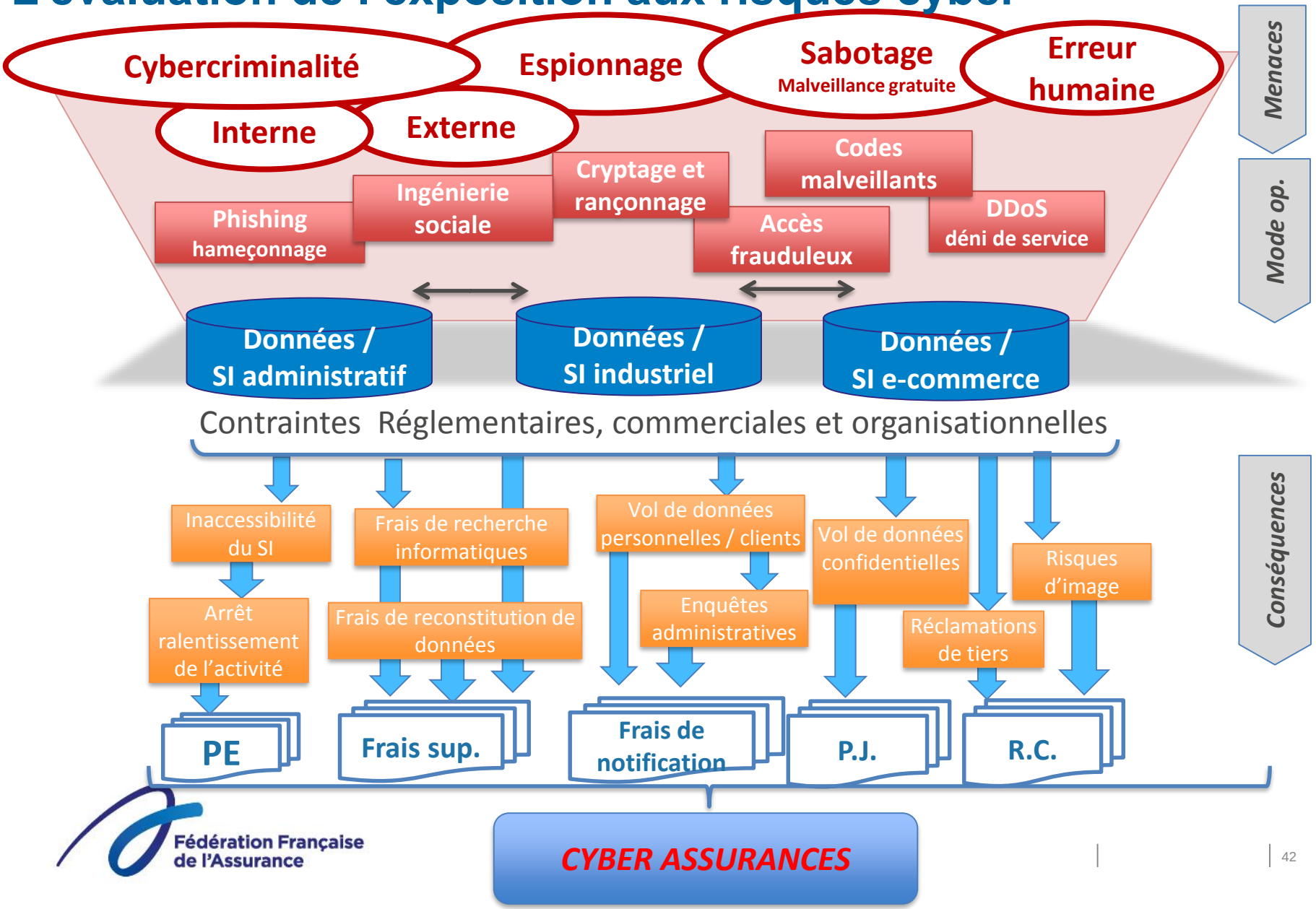
Cartographie de son exposition aux risques cyber

A. L’évaluation de l’exposition aux risques cyber

B. La quantification de l’exposition aux risques cyber

C. Transfert du risque à l’assureur

L'évaluation de l'exposition aux risques cyber



Fédération Française de l'Assurance

L'évaluation de l'exposition aux risques et de la quantification financière

Il est impératif :

- d'identifier les facteurs de risque (surface d'attaque & attractivité)
- de faire une évaluation relative

Suivant les réglementations ou les exigences contractuelles :

- RGPD
- NIS

En fonction de l'activité :

- Secteur Industriel
- Vente et Commerce
- Logistique
- Opérateur de réseau
- Fournisseur de service tangible
- Fournisseur de service intangible

Selon comment l'entreprise utilise les outils informatiques:

- Pour les activités support (compta, achats, RH, gestion clients, …)
- Pour les activités opérationnelles métiers (fabrication, R&D, gestion des stocks, logistique, …)
- Pour les produits et/ou services fournis

Fédération Française de l'Assurance

Une obligation légale

Le droit national ainsi que les textes communautaires créent des obligations légales en matière de prévention des risques cyber.

1. Prévention du risque de corruption des données à caractère personnel

   a) La loi Informatique et Liberté du 6 janvier 1978
   b) Le Règlement Général pour la Protection des Données personnelles (RGPD) du 27 avril 2016 – 25 Mai 2018

2. Prévention du risque d'altération des Systèmes d'Information

   a) La loi de programmation militaire de 2013
   b) La Directive sur la Sécurité des Systèmes d'Information - NIS du 6 juillet 2016 – 9 Mai 2018

L'évaluation de l'exposition au risque cyber

Risque juridique – Données à caractère personnel

Règlement (UE) 2016/679 (RGPD)

Risques financier et pénal

Risque juridique financier	Risque juridique pénal	Risque juridique contentieux
Article 83 jusqu'à 20 millions d'euros ou 4% du CA mondial.	**Article 84** Droit des états membres	**Articles 79 et 82** Droit à un recours juridictionnel effectif Droit à réparation et responsabilité

Fédération Française de l'Assurance

Une obligation légale

Prévention – Données à caractère personnel

Règlement (UE) 2016/679 (RGPD) du 27 avril 2016

Introduire une culture du risque au sein de toutes les entreprises

Article 25 : Dès la conception et par défaut

1. Assurer un maximum de sécurité dès la conception des moyens de traitements
2. Certification

Article 28 : Choix des sous-traitants

1. Garanties suffisantes des mesures employées par le sous-traitant
2. Certification ou suivi d'un code de conduite

Article 32 : Sécurité du traitement

1. Niveau de sécurité adapté au risque
2. Cartographie des risques

Fédération Française de l'Assurance

Une obligation légale

Prévention – Données à caractère personnel

Règlement (UE) 2016/679 (RGPD)

Instaurer un dialogue avec l'autorité de contrôle (CNIL en FR)

Article 35 : Analyse d'impact sur demande de la CNIL

1. Analyse d'impact des opérations de traitements
2. Analyses obligatoires ou non établies par une liste de l'autorité de contrôle (CNIL)

Article 36 : Consultation préalable de la CNIL

1. Consultation de la CNIL en cas de constatation risque élevé suite à une étude d'impact
2. CNIL rend un avis

Articles 37 à 39 : Désignation d'un délégué

1. Désignation d'un délégué à la protection des données personnelles
2. Délivre informations, conseils, surveille le respect du règlement…

Fédération Française de l'Assurance

Une obligation légale

Prévention – Systèmes d'information

Loi de programmation militaire 2013 pour 2014-2019

Pour les opérateurs d'importance vitale

Article 22 : Fixation de règles de sécurité nécessaire à la protection des systèmes d'information des opérateurs par le Premier ministre

1. **Systèmes de détection d'évènements susceptibles d'affecter la sécurité des SI**
2. **Contrôle des SI pour vérifier le niveau de sécurité**
3. **Politique de sécurité des systèmes d'information**
4. **Procédure d'homologation des systèmes d'information d'importance vitale**

- Arrêté du 10 juin 2016 Secteur « produits de santé »
- Arrêté du 17 juin 2016 Secteur « alimentation »
- Arrêté du 17 juin 2016 Secteur « Gestion de l'eau »
- Arrêté du 11 aout 2016 Secteur « énergie »
- Arrêté du 11 aout 2016 Secteur « transport »

Fédération Française de l'Assurance

Une obligation légale

Prévention – Systèmes d'information

Directive (UE) 2016/1148 du 6 juillet 2016

Mesures destinées à assurer un niveau élevé commun de sécurité des réseaux et des systèmes d'information pour les Opérateurs de services essentiels et fournisseurs de services numériques

Article 14 : Exigences de sécurité pour les OSE

1. Gestion des risques
2. Niveau de sécurité adapté aux risques
3. Mesures de prévention des risques

Article 16 : Exigences de sécurité pour les FSN

1. Identification des risques
2. Niveau de sécurité adapté au risque existants
3. Mesures pour éviter les incidents
4. Mesures pour réduire l'impact des incidents

Fédération Française de l'Assurance

IV. Que faire en cas d'attaque cyber ?

A. Gérer la crise au sein de l’entreprise

B. Porter plainte

C. Se rendre sur la plateforme cybermalveillance.gouv.fr

D. Contacter l’assureur

E. Notifier

Gérer la crise au sein de l'entreprise

En cas de survenance d'une cyber attaque, la gestion de crise doit être pluridisciplinaire, au croisement de la gestion du risque et de la sécurité informatique.

Les experts techniques seront au service de l'entreprise dans cette gestion.
Plus les choses auront été préparées en amont *(notamment la cartographie des risques ou l'analyse des vulnérabilités, des vecteurs et des modes d'attaque),* **plus la gestion de crise sera efficace.**

La conception d'outils de résilience tel que le Plan de Reprise d'Activité est précieuse dans cette situation.

Contacter l'assureur

Contacter sans délai l'assureur qui conseillera et accompagnera l'entreprise dans la gestion de cette crise.

L'assureur vérifiera le domaine et l'étendue des contrats souscrits en cours afin de s'assurer que l'entreprise est correctement couverte.

En tout état de cause, l'assureur doit être informé de l'attaque cyber avant toute prise de décision qui pourrait avoir un impact :

- sur les conséquences de l'incident,
- sur la gestion du dossier de déclaration de sinistre.

Porter plainte

Dans le Code Pénal :
- Les articles 323-1 à 323-7
- L'article 434-15-2
- et les articles 226-1 à 226-4

Dans le Code Monétaire et Financier :
- les articles L163-3 à L163-12

➢ **Ces articles définissent les cyber attaques constitutives d'infractions aux technologies de l'information et de la communication pour lesquelles il est possible de porter plainte.**

Se rendre sur cybermalveillance.gouv.fr

C’est la solution vers laquelle peuvent désormais se tourner les victimes de cybermalveillance : une plateforme unique qui met en relation ces victimes avec des prestataires de proximité, compétents et présents sur l’ensemble du territoire national.

Il s’adresse aux particuliers, aux entreprises (PME/TPE) et collectivités territoriales.

Notifier

	OBLIGATION DE NOTIFICATION		AUJOURD'HUI	DEMAIN (mai 2018)
En cas de violation des donnees à caractère personnel		Pour qui ?	**Pour les fournisseurs de services de communications électroniques au public** (Loi Informatique et libertés 1978)	**Pour toutes les entreprises ayant des activités de traitement de données** (Règlement européen « RGPD » 2016/679)
		À qui ?	À la CNIL et à l'intéressé	À l'autorité compétente et à l'intéressé
En cas d'atteinte au système d'information		Pour qui ?	**Pour les opérateurs d'Importance vitale (OIV)** (Loi de programmation militaire 2014 -2019)	**Pour les opérateurs de services essentiels et fournisseurs de services numériques** (Directive européenne « NIS »2016/1148)
		À qui ?	Au Premier ministre et à l'ANSSI	À l'autorité compétente

Conclusion