Atelier C8

Cyber attaque sur un site industriel ou sur de grandes infrastructures

Atelier C8

Intervenants

Eric Freyssinet	**Ministère de l'Intérieur** **Conseiller auprès du Délégué ministériel chargé de la lutte contre les cybermeances**
Mehdi AÏT HAMMOU	**RATP** **Responsable Sécurité des Systèmes d'Information**
Philippe COTELLE	**AIRBUS DEFENSE AND SPACE** **Risk Manager**
Jimaan SANE	**Beazley Solutions Limited** **Souscripteur Technologies-Media-Sociétés de service**

Modérateur

Philippe VAPPEREAU	**RATP** **Précédent Risk Manager**

AMRAE LES RENCONTRES

Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
MINISTÈRE DE L'INTÉRIEUR

Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
MINISTÈRE DE L'INTÉRIEUR

DMISC
Lutte contre les
cybermenaces

La lutte contre les cybermenaces

Col. Eric Freyssinet - @ericfreyss

Synthèse cybercriminalité

- Sur la base des trois piliers traités par Europol:
  - Atteintes aux mineurs facilitées par Internet
    - Toujours un sujet très fort
    - Croissance des situations d'abus « sur commande »
  - Cartes bancaires, moyens de paiement
    - Stable, avec une adaptation des modes opératoires
    - En réalité ce sont toutes les formes d'escroquerie, quels que soient les moyens de paiement qui tiennent le haut du pavé
  - Atteintes aux STAD
    - Développement fort des menaces liées à des virus informatiques et les atteintes directes contre les systèmes d'information

Ecosystème du cybercrime financier

Est européen et local

Poseurs

Mules

International

Copie de cartes bancaires *skimming*

Électroniciens

Copie de données bancaires ou autres identifiants / données sensibles

Escroquerie au commerce électronique

Attaquants isolés

Parfois très « local »

Accès frauduleux

Crime organisé

Escroqueries à l'avance de frais

Botnets

Déni de service

Scareware, ransomware...

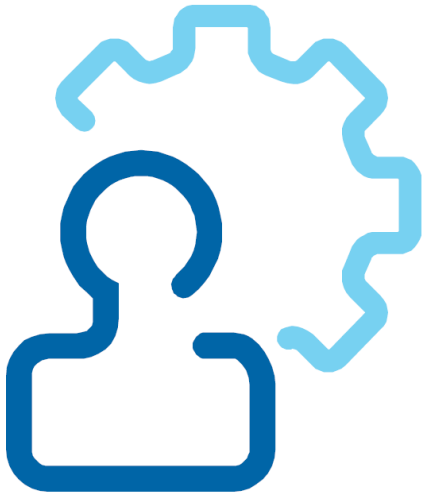
Escrocs isolés

Script-kiddies

Logiciels malveillants

Développeurs

Evolution des formes de criminalité organisée



- Intermédiaires:
  - Blanchiment
  - Mules

- Gestionnaires:
  - D'infrastructures (bulletproof)
  - De services criminels divers
  - De plateformes de discussion / marchés

- Développeurs de:
  - Virus
  - Plateformes de diffusion
  - Vulnérabilités/ exploits

Perception du risque

- Tous les acteurs sont concernés
  - Autant les petites entreprises que les plus grandes
    - Directement ou indirectement (sous-traitants)
  - Les risques sont multiples, mais tournent avant tout autour:
    - Finances (escroquerie au président, extorsion / DDoS ou rançongiciel)
    - Détournement de données
    - Atteintes à l'outil de production (comme conséquence des atteintes précédentes, ou parfois comme objectif principal)
    - Espionnage industriel

Actions de prévention

- Réseau des référents sûreté et référents intelligence économique dans les régions (police et gendarmerie)
  - Inclure dans le dialogue avec entreprises (notamment PME) la dimension cybersécurité
  - Cybercriminalité au 3e rang des risques remontés
  - Faciliter le contact avec les enquêteurs spécialisés
- Sensibilisation par les antennes régionales de la DGSI, 1450 conférences au cours de l'année 2016

Actions de prévention

- S’inscrire dans un contexte interministériel
  - En partenariat avec ANSSI, DGE, …
- Apporter une aide mieux adaptée aux entreprises, collectivités locales et particuliers
- Rendre plus visible et accessible l’information de sensibilisation et sur les dispositifs existants, notamment en réponse à une cybermalveillance
  - Développer les bonnes pratiques de préservation de la preuve
- Rapprocher des prestataires mieux sensibilisés des victimes
  - Faire circuler de l’information
- Première phase du dispositif dans les Hauts de France

Contact

- Ministère de l'intérieur
- - Lutte contre les cybermenaces
- eric.freyssinet@interieur.gouv.fr
- @ericfreyss

- Membre associé du LORIA, Nancy (CNRS UMR 7503, INRIA, Université de Lorraine)

- CECyF – https://www.cecyf.fr/ @Cyber_FR

CYBERSÉCURITÉ DES SI INDUSTRIELS
RETOUR D'EXPÉRIENCE DU GROUPE RATP

Mehdi Aït Hammou – RATP

La cybermalveillance s'accentue, la loi encadre précisément les TIC, les frontières d'un SI devenu essentiel s'atténuent *(…)*, la cybersécurité est désormais un enjeu majeur.

Le SI est un levier de performance essentiel mais constitue également un point de fragilité évident.

- L'information est un actif parfois stratégique,
- Les SI soutiennent toujours davantage nos processus métiers et notre offre de transport,
- Les SI et notre environnement digital sont à la fois plus ouverts, complexes et exposés.

Assurer la confidentialité, l'intégrité, la disponibilité et la traçabilité de nos informations et systèmes est désormais un enjeu majeur.

+

La menace est désormais concrète et protéiforme

- Vol de données : Sony, Target, Areva, Thales, Safran, Yahoo…
- Compromission des SI industriels : Stuxnet, BlackEnergy…

La loi encadre précisément les TIC

- Informatique & Libertés, RGPD.
- LPM, Directive NIS.
- PCI-DSS…

Le Groupe RATP n'est pas épargné

=

En sa qualité d'opérateur de transport de l'un des premiers réseaux multimodaux au monde, la RATP porte, y compris en matière de cybersécurité, une responsabilité de premier plan.

Notre stratégie de maîtrise du risque cyber s'appuie sur une vision partagée des enjeux métiers et un système de défense en profondeur ajusté en permanence.

Un cadre défini de gouvernance cyber

- Une politique et une organisation dédiée à la cyber
- Des liens étroits avec l'ANSSI et le MEEM

RATP ⇄ Liberté • Égalité • Fraternité RÉPUBLIQUE FRANÇAISE

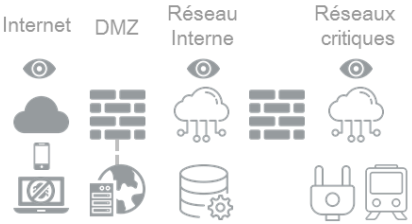
Un management continu du risque cyber

- Des menaces et des vulnérabilités hiérarchisées au regard des enjeux métier

+1200 appli classifiées
+300 scénarios évalués
+20 carto. revues/an.

Un système de défense ajusté en permanence

- Un système technique visant l'état de l'art



- SOC: des capacités cyber renforcées d'analyse et de réponse

sopra steria / RATP

+4Milliards d'événements
17030 alertes
1080 incidents
25 escalades
0 attaque réussie détectée

Un effort essentiel de sensibilisation

- Des campagnes ponctuelles de formation cyber
- Un vif succès des opérations lancées de sensibilisation

Un contrôle continu de nos pratiques cyber

- Une stratégie d'autocontrôles
- Un plan annuel d'audits renforcé

+15 audits DG / an

Entreprise | Transport | Energie

Traditionnellement engagée sur la sécurité ferroviaire, la RATP a pris conscience de la nécessité de protéger ses SI industriels face à un risque cyber désormais démontré.

Au service de la production de l'offre de transport, du pilotage de l'énergie ou encore de la commande des équipements techniques installés dans nos espaces (ventilation, systèmes incendie, puisards), les SI industriels du Groupe RATP sont également exposés à une menace tangible de compromission.

 	**2015**	Différentes cyberattaques à l'encontre de **centrales électriques** ukrainiennes entraînent des coupures générales d'énergie dans plusieurs zones géographiques du pays.
 	**2014**	La compromission des systèmes industriels pilotant les **installations d'une aciérie** allemande provoque d'importants dégâts sur les hauts fourneaux du site.
 	**2010**	Le vers Stuxnet sabote les **centrifugeuses** (systèmes siemens) du site de Natanz et perturbe durablement le développement du programme nucléaire iranien.
 	**2007**	Différentes attaques effectuées par communication infrarouge entraînent le déraillement d'un **tramway** en Pologne (12 blessés),
 	**2003**	Le vers Sobig paralyse les **systèmes d'aiguillage** d'une vingtaine d'états américains.

Sur la base des compétences cyber acquises et empreinte de sa culture "sécurité ferroviaire & SdF", la RATP accélère le renforcement de son système de défense en profondeur sur le périmètre industriel.

De récentes nouvelles obligations légales et les publications/référentiels de l'ANSSI ont constitué un catalyseur puissant de mobilisation au sein de l'entreprise.

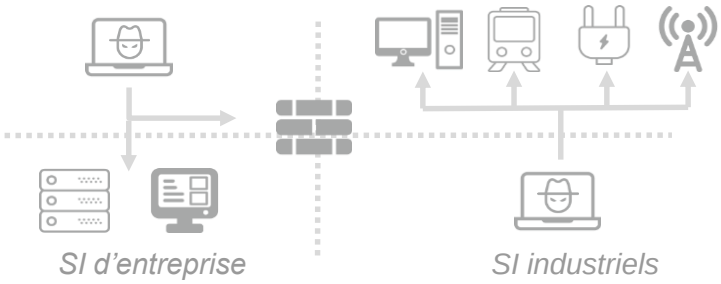
Fin 2013, quatre chantiers ont été engagés afin d'identifier et lancer les actions nécessaires au renforcement du système de défense des SI industriels du groupe.

1 Formalisation de l'inventaire des SI industriels critiques de la RATP

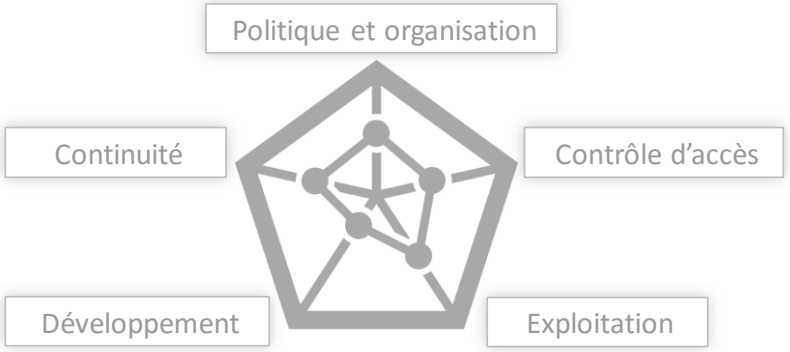
- Liste à identifier parmi une quinzaine de catégories de SI définies.

Typologie des systèmes critiques	
Nom et description	CONFIDENTIEL
Cartographie	

2 Analyse de risque et audits techniques afin de compléter notre vision du niveau de sécurité



3 Conduite d'un audit afin d'évaluer notre maturité en termes d'organisation & processus



4 Analyse d'écart et programmation des actions de sécurisation prioritaires.

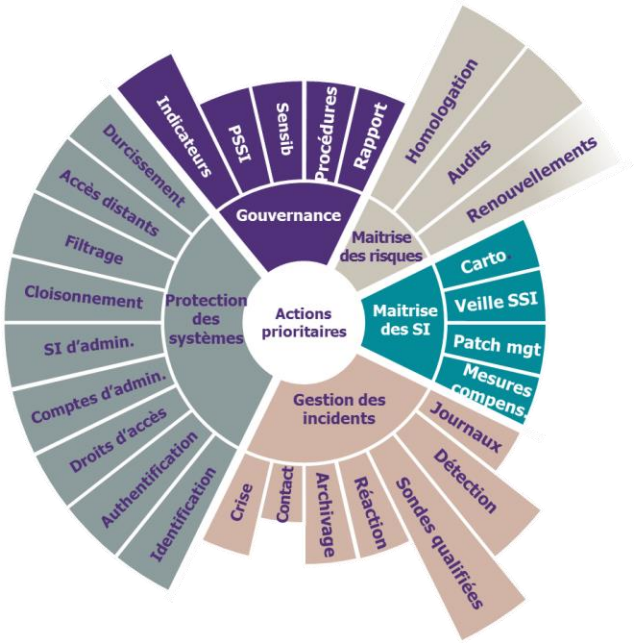
- Analyse des écarts aux règles et bonnes pratiques de l'ANSSI
- Estimations des coûts de mise en œuvre
- Programmation des actions de sécurisation prioritaires

La démarche engagée a permis la mise en œuvre d'un programme d'actions ambitieux; Cette action s'appuie sur un renforcement des équipes et une mobilisation en mode projet de l'entreprise.

4

Un programme d'actions partagées, évaluées et planifiées au sein de la RATP

Obligations légales & Référentiels ANSSI



Ce programme d'actions s'articule autour des trois axes de travail prioritaires suivants :

- Concevoir immédiatement nos futurs systèmes conformes à ces nouvelles règles
- Renforcer la fonction de gestion op^{elle} de la sécurité et lancer les chantiers techniques
- Initier le travail d'homologation des systèmes industriels critiques existants

Coût initial	> X M€
Coût récurrent	> Y M€

t_0 — t_{0+5ans}

Afin de répondre à une démarche ambitieuse et exigeante (délais, écart à l'existant…), deux facteurs clés ont semblé indispensables :

Une mobilisation en mode projet des organisations concernés

L'installation d'un comité directeur SI industriel sous le pilotage de la DG

Cyber attaque sur un site industriel ou sur de grandes infrastructures

Philippe Cotelle – AIRBUS Defense & Space
Head of Insurance Risk Management

2 février 2017

Le risque Cyber : un risque d'Entreprise

Besoin Clé d'une Stratégie efficace de Gestion du risque Cyber

Cybersécurité et valorisation de l'Entreprise

Forte Sensibilisation des Boards

- **Valorisation Business**
- **Confiance et réputation**

Les risques Cyber affectent l'entreprise et sa réputation

- **Evolution rapide** peut impacter les fonctions clés de l'entreprise
- L'attaque, une fois rendue publique, **grande sensibilité** des investisseurs et de l'opinion publique
- **Pression des Régulateurs** en Europe pour communiquer de façon plus transparente sur les incidents: directive NIS, GDPR

Le Risque Cyber devient une préoccupation forte des **Boards**

Le risque Cyber: multiples impacts pour une même occurrence

- Impact Cours Bourse
- Réputation
- Fraudes extortions ransonnage
- DDoS
- Poursuites légales Amendes
- Altération des Produits menant à des dommages aux biens ou aux personnes

- Pertes d'opportunité
- Pertes de données
- Dommages immatériels
- Vol de données / Pertes de données personnelles
- Vol de Propriété intellectuelle

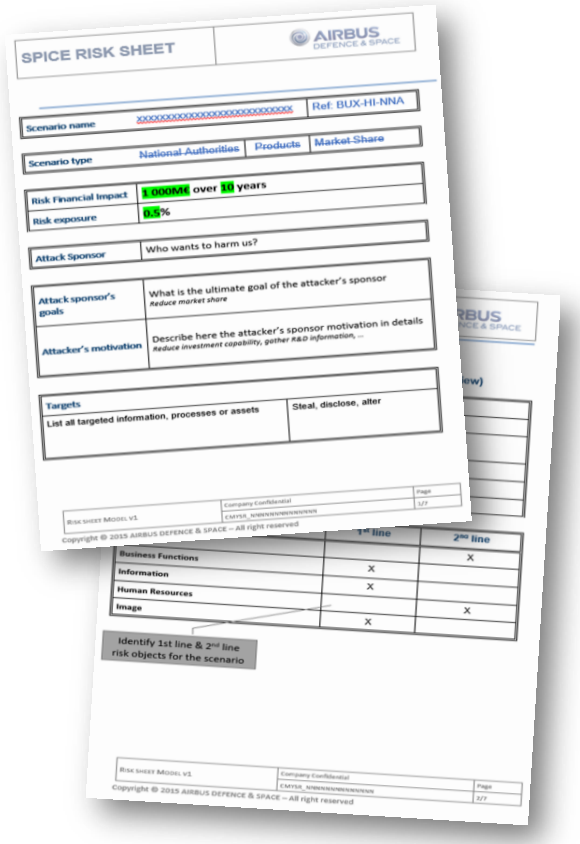
- Perte de données personnelles
- Relais d'attaque / Transmission de virus
- Alteration des Produits menant à des dommages aux biens ou aux personnes

- Contenu publié sur le web
- Diffamation
- Reponsabilité Produit ou Services

Identification de Scénarios

Identification des Scénario clés

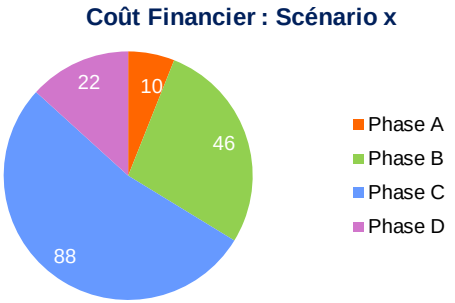
- Focus sur les scenarios catastrophe
- Hypothèses clairement identifiées



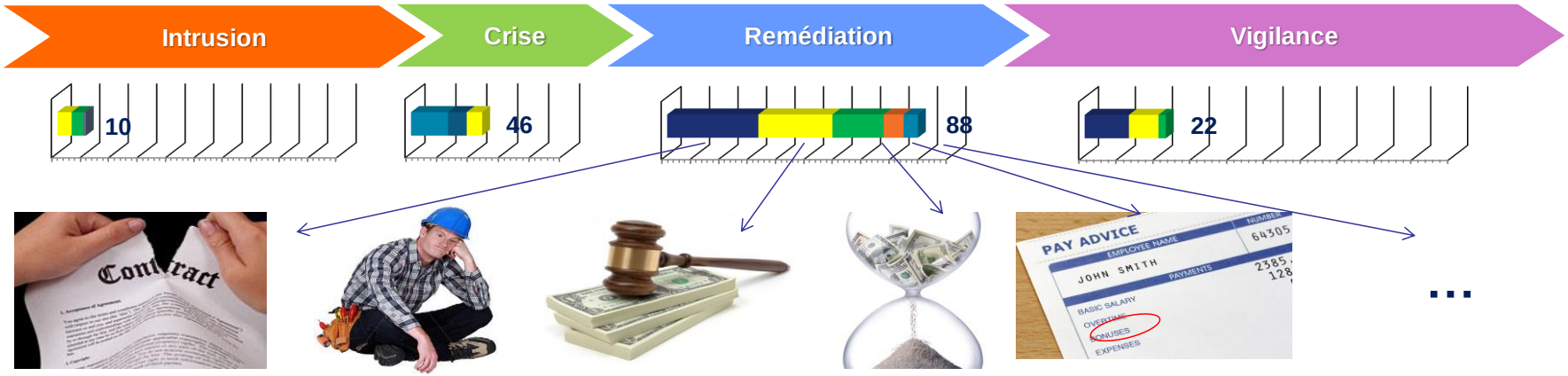
Quantification Financière

Assessment du coût financier de chaque scénario

- Scenarios décomposés en 4 différentes phases
- Contribution de chacune des fonctions impactées
- Consolidation par phase pour chaque scenario



Détection
Défaut de Sécurité



Programme de Recherche IRT-SystemX

Lawyers

Concept d'Analyse de Risque

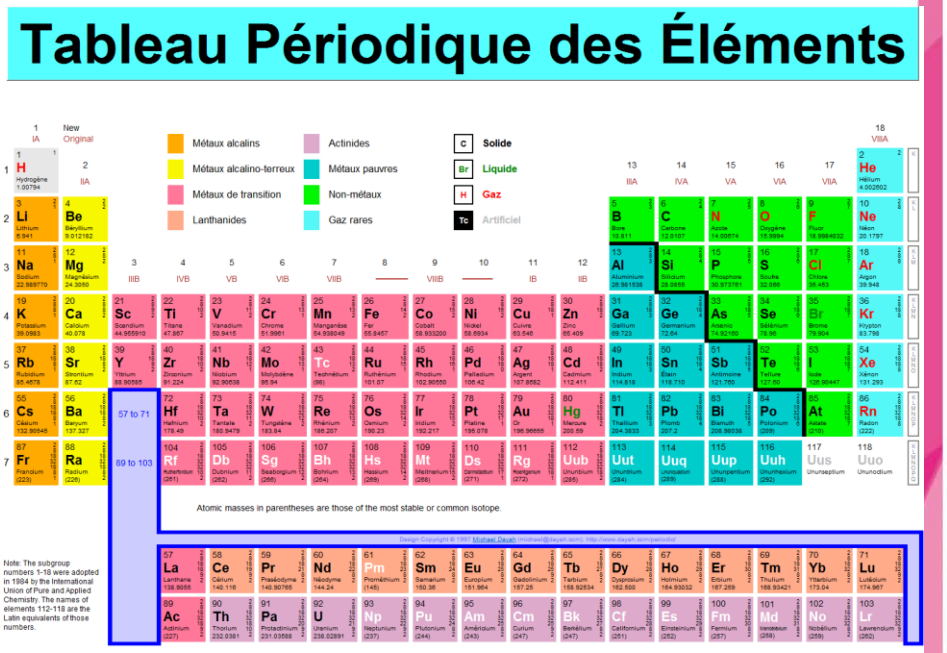
Les scenarios d'exposition pour être pertinent doivent être spécifiques à la situation de chaque société:

- Attractivité et sensitivité
- Taille et structure
- Localisation

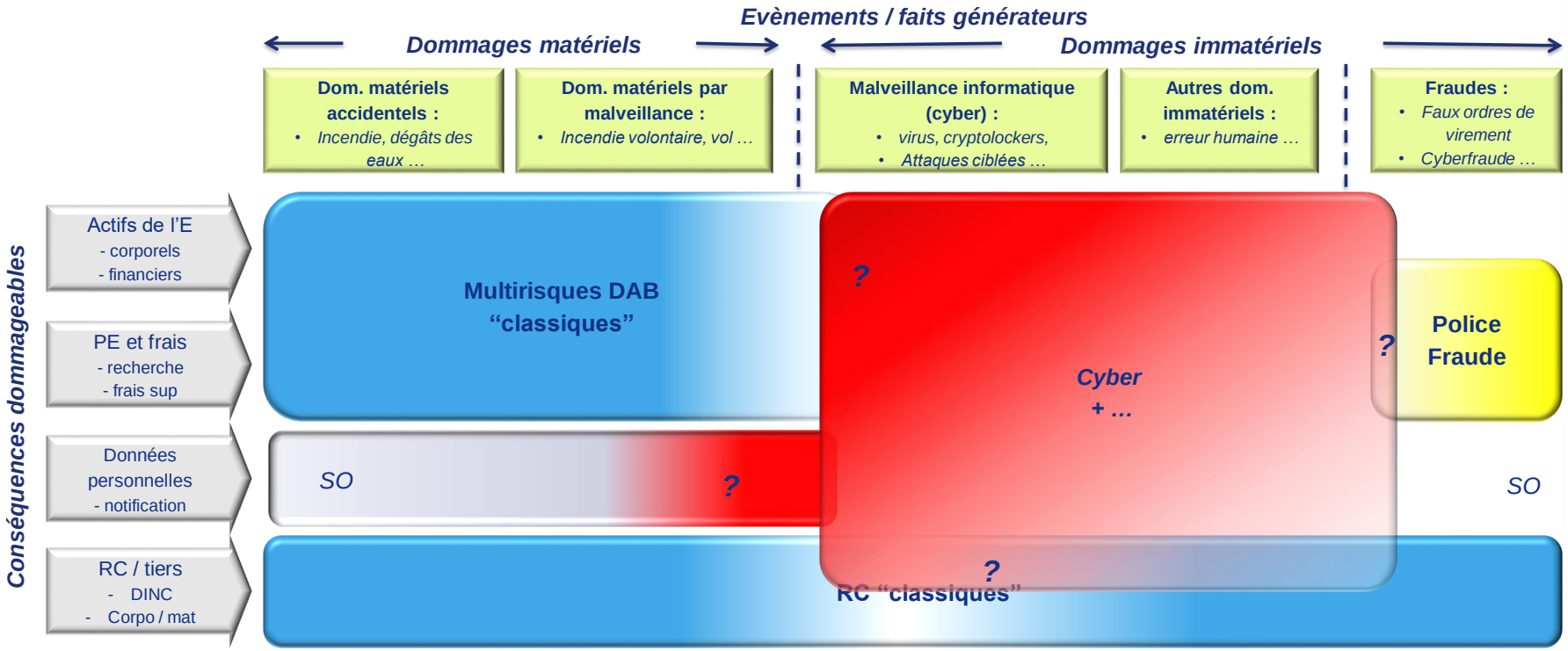
Méthode:

- Définir des catégories de risk élémentaires
- Associer des métriques à ces catégories

Chaque scénario envisagé est décomposable en une combinaison de ces risques élémentaires



Mapping des couvertures d'assurance



AMRAE LES RENCONTRES

Périmètre Cyber sur le marché français

Faits générateurs dommeageables / Garanties

Dommages Materiels

Evénements causant des Dommages physiques accidentels

Garanties	Incendie	Explosion / foudre	DDE, TDC, événements naturels	Bris de machines
Bâtiments	DAB	DAB	DAB	DAB
Marchandises	DAB	DAB	DAB	DAB
Matériels industriels	DAB	DAB	DAB	DAB
Matériels informatiques	DAB	DAB	DAB	DAB
Transport Maritime	Corps et faculté ?			
Transport Aérien	Dommage aux aéronefs, etc. ?			
Perte pécuniaire : remboursement des fonds détournés	so	so	so	so
Remboursement des rançons / sommes extorquées sous la	so	so	so	so
Frais de recours et de poursuites	so	so	so	so
Perte d'opportunité				
Perte de marge brute / de recette	DAB	DAB	DAB	DAB
Frais supplémentaires d'exploitation (pour minimiser la perte	DAB	DAB	DAB	DAB
Aggravation de PE à la suite d'une décision administrative légalement prise	DAB	DAB	DAB	DAB
Frais de recherche de cause: - IT : Forensic, frais d expertise, d assistance... - Mat : frais d'expertise, de recherche de cause...	DAB	DAB	DAB	DAB
Frais de reconstitution de données	DAB	DAB	DAB	DAB
Frais supplémentaires (travaux activité sup., gestion de crise	DAB	DAB	DAB	DAB
Conseils/ préconisations après attaque/ sinistre (remédiation	DAB	DAB	DAB	DAB
Frais d'amélioration de la sécurité informatique du SI				
Frais de notification aux instances administratives	so	so	so	so
Frais de comparution (enquêtes administratives)	so	so	so	so
Frais de notification aux personnes concernées par une violation de données personnelles	so	so	so	so
Conseil en communication / Relations Publiques / Gestion de	DAB	DAB	DAB	DAB
Nettoyage- noyage	so	so	so	so
Frais de référencement	so	so	so	so
Plateforme téléphonique (n° vert)	DAB	DAB	DAB	DAB
Conseil juridique (hot line, gestion de crise)	so	so	so	so
Assistances juridiques : mise en œuvre de l'action juridique	so	so	so	so
Honoraires d'avocats, d'huissiers, d'experts judiciaires	so	so	so	so
Dommages matériels aux tiers	DAB	DAB	RC	RC
Dommages immatériels (aux tiers) consécutifs	DAB	DAB	RC	RC
Dommages immatériels non consécutifs	DAB	DAB	RC	RC
Dommages corporels (aux tiers)	RC	RC	RC	RC
Frais de retraits / dépose / repose	so	so	so	so
Défense recours	RC	RC	RC	RC
RC des mandataires sociaux	RC	RC	RC	RC
Amendes civiles (procédures abusives)	so	so	so	so
Amendes administratives				
Amendes pénales				
Pénalités de retard (consécutifs au fait dommageable)	DAB	DAB	DAB	DAB
Pénalités PCI -DSS (UNIQUEMENT pour les banques)	so	so	so	so
Pénalités PCI -DSS (hors banques si applicable)	so	so	so	so

Evénements causant des Dommages physiques par malveillance (actes crapuleux, activisme ou terrorisme si conditions légales réunies)

Garanties	Incendie volontaire	Sabotage	Vol physique (avec ou sans effraction)	Vol physique ou dégradation faisant suite à une cyber attaque
Bâtiments	DAB	DAB	DAB	DAB
Marchandises	DAB	DAB	DAB	DAB
Matériels industriels	DAB	DAB	DAB	DAB
Matériels informatiques	DAB	DAB	DAB	DAB
Transport Maritime				
Transport Aérien				
Perte pécuniaire : remboursement des fonds détournés	so	so	Fraude si pas effr	Fraude si pas effr
Remboursement des rançons / sommes extorquées sous la	so	so	so	so
Frais de recours et de poursuites	so	so	Fraude si pas effr	Fraude si pas effr
Perte d'opportunité				
Perte de marge brute / de recette	DAB	DAB	DAB	DAB
Frais supplémentaires d'exploitation (pour minimiser la perte	DAB	DAB	DAB	DAB
Aggravation de PE à la suite d'une décision administrative légalement prise	DAB	DAB	so	so
Frais de recherche de cause: - IT : Forensic, frais d expertise, d assistance... - Mat : frais d'expertise, de recherche de cause...	DAB	DAB	DAB	DAB
Frais de reconstitution de données	DAB	DAB	DAB	DAB
Frais supplémentaires (travaux activité sup., gestion de crise	DAB	DAB	DAB	DAB
Conseils/ préconisations après attaque/ sinistre (remédiation	DAB	DAB	DAB	DAB
Frais d'amélioration de la sécurité informatique du SI				
Frais de notification aux instances administratives	so	so	Cyber ?	Cyber ?
Frais de comparution (enquêtes administratives)	so	so	Cyber ?	Cyber ?
Frais de notification aux personnes concernées par une violation de données personnelles	so	so	Cyber ?	Cyber ?
Conseil en communication / Relations Publiques / Gestion de	DAB	DAB	DAB	DAB
Nettoyage- noyage	so	so	so	so
Frais de référencement	so	so	so	so
Plateforme téléphonique (n° vert)	DAB	DAB	DAB	DAB
Conseil juridique (hot line, gestion de crise)	so	so	so	so
Assistances juridiques : mise en œuvre de l'action juridique	so	so	so	so
Honoraires d'avocats, d'huissiers, d'experts judiciaires	so	so	so	so
Dommages matériels aux tiers	RC	RC	RC	RC
Dommages immatériels (aux tiers) consécutifs	RC	RC	RC	RC
Dommages immatériels non consécutifs	RC	RC	RC	RC
Dommages corporels (aux tiers)	RC	RC	RC	RC
Frais de retraits / dépose / repose	so	so	so	so
Défense recours	RC	RC	RC	RC
RC des mandataires sociaux	RC	RC	RC	RC
Amendes civiles (procédures abusives)	so	so	so	so
Amendes administratives				
Amendes pénales				
Pénalités de retard (consécutifs au fait dommageable)	DAB / RC	DAB / RC		
Pénalités PCI -DSS (UNIQUEMENT pour les banques)	so	so	so	so
Pénalités PCI -DSS (hors banques si applicable)	so	so	so	so

Dommages Immateriels

Malveillance informatique (actes crapuleux, activisme ou terrorisme si conditions légales réunies)

Cyber attaques diffuses

Garanties	Livraison d'un logiciel vicié	Virus, vers... (codes malveillants) => entrave au fonctionnement	Rançongage par cryptolocker	Rançongage sur vol de données personnelles
Bâtiments	so	so	so	so
Marchandises	so	so	so	so
Matériels industriels	so	DAB	so	so
Matériels informatiques	so	DAB / Cyber	so	so
Transport Maritime				
Transport Aérien				
Perte pécuniaire : remboursement des fonds détournés	so	so	so	so
Remboursement des rançons / sommes extorquées sous la	so	so	?	?
Frais de recours et de poursuites	so	so	Cyber	Cyber
Perte d'opportunité				
Perte de marge brute / de recette	so	Cyber	Cyber	Cyber
Frais supplémentaires d'exploitation (pour minimiser la perte	so	Cyber	Cyber	Cyber
Aggravation de PE à la suite d'une décision administrative légalement prise	so	Cyber	Cyber	Cyber
Frais de recherche de cause: - IT : Forensic, frais d expertise, d assistance... - Mat : frais d'expertise, de recherche de cause...	Cyber	Cyber	Cyber	Cyber
Frais de reconstitution de données	Cyber	Cyber	Cyber	Cyber
Frais supplémentaires (travaux activité sup., gestion de crise	Cyber	Cyber	Cyber	Cyber
Conseils/ préconisations après attaque/ sinistre (remédiation	Cyber	Cyber	Cyber	Cyber
Frais d'amélioration de la sécurité informatique du SI				
Frais de notification aux instances administratives	Cyber ?	Cyber ?	Cyber ?	Cyber
Frais de comparution (enquêtes administratives)	Cyber ?	Cyber ?	Cyber ?	Cyber
Frais de notification aux personnes concernées par une violation de données personnelles	Cyber ?	Cyber ?	Cyber ?	Cyber
Conseil en communication / Relations Publiques / Gestion de	Cyber	Cyber	Cyber	Cyber
Nettoyage- noyage	Cyber ?	Cyber ?	Cyber ?	Cyber ?
Frais de référencement	Cyber ?	Cyber ?	Cyber ?	Cyber ?
Plateforme téléphonique (n° vert)	Cyber ?	Cyber ?	Cyber ?	Cyber ?
Conseil juridique (hot line, gestion de crise)	Cyber ?	Cyber ?	Cyber ?	Cyber ?
Assistances juridiques : mise en œuvre de l'action juridique	Cyber ?	Cyber ?	Cyber ?	Cyber ?
Honoraires d'avocats, d'huissiers, d'experts judiciaires	Cyber ?	Cyber ?	Cyber ?	Cyber ?
Dommages matériels aux tiers	RC	RC	RC	RC
Dommages immatériels (aux tiers) consécutifs	RC	RC	RC	RC
Dommages immatériels non consécutifs	RC	RC	RC	RC
Dommages corporels (aux tiers)	RC / Cyber	RC / Cyber	RC / Cyber	RC / Cyber
Frais de retraits / dépose / repose	so	so	so	so
Défense recours	RC	RC	RC	RC
RC des mandataires sociaux	RC	RC	RC	RC
Amendes civiles (procédures abusives)	so	so	so	so
Amendes administratives				
Amendes pénales				
Pénalités de retard (consécutifs au fait dommageable)	so	Cyber / RC ?	Cyber / RC ?	Cyber / RC ?
Pénalités PCI -DSS (UNIQUEMENT pour les banques)	so	so	so	Cyber / RC ?
Pénalités PCI -DSS (hors banques si applicable)	so	so	so	so

Cyber attaques ciblées

Garanties	Rançongage sur vol de données personnelles	Vol de données personnelles	Vol de données confidentielles / espionnage économique	Sabotage externe
Bâtiments	so	so	so	DAB
Marchandises	so	so	so	DAB
Matériels industriels	so	so	so	DAB
Matériels informatiques	so	so	so	DAB
Transport Maritime				
Transport Aérien				
Perte pécuniaire : remboursement des fonds détournés	so	so	so	so
Remboursement des rançons / sommes extorquées sous la	so	so	so	so
Frais de recours et de poursuites	so	so	so	so
Perte d'opportunité				
Perte de marge brute / de recette	Cyber	Cyber	Cyber	Cyber
Frais supplémentaires d'exploitation (pour minimiser la perte	Cyber	Cyber	Cyber	Cyber
Aggravation de PE à la suite d'une décision administrative légalement prise	Cyber	Cyber	Cyber	Cyber
Frais de recherche de cause: - IT : Forensic, frais d expertise, d assistance... - Mat : frais d'expertise, de recherche de cause...	Cyber	Cyber	Cyber	Cyber
Frais de reconstitution de données	Cyber	Cyber	Cyber	Cyber
Frais supplémentaires (travaux activité sup., gestion de crise	Cyber	Cyber	Cyber	Cyber
Conseils/ préconisations après attaque/ sinistre (remédiation	Cyber	Cyber	Cyber	Cyber
Frais d'amélioration de la sécurité informatique du SI				
Frais de notification aux instances administratives	Cyber ?	Cyber ?	Cyber ?	Cyber ?
Frais de comparution (enquêtes administratives)	Cyber ?	Cyber ?	Cyber ?	Cyber ?
Frais de notification aux personnes concernées par une violation de données personnelles	Cyber ?	Cyber ?	Cyber ?	Cyber ?
Conseil en communication / Relations Publiques / Gestion de	Cyber	Cyber	Cyber	Cyber
Nettoyage- noyage	Cyber ?	Cyber ?	Cyber ?	Cyber ?
Frais de référencement	Cyber ?	Cyber ?	Cyber ?	Cyber ?
Plateforme téléphonique (n° vert)	Cyber ?	Cyber ?	Cyber ?	Cyber ?
Conseil juridique (hot line, gestion de crise)	Cyber ?	Cyber ?	Cyber ?	Cyber ?
Assistances juridiques : mise en œuvre de l'action juridique	Cyber ?	Cyber ?	Cyber ?	Cyber ?
Honoraires d'avocats, d'huissiers, d'experts judiciaires	Cyber ?	Cyber ?	Cyber ?	Cyber ?
Dommages matériels aux tiers	RC	RC	RC	RC
Dommages immatériels (aux tiers) consécutifs	RC	RC	RC	RC
Dommages immatériels non consécutifs	RC	RC	RC	RC
Dommages corporels (aux tiers)	RC / Cyber	RC / Cyber	RC / Cyber	RC / Cyber
Frais de retraits / dépose / repose	so	so	so	so
Défense recours	RC	RC	RC	RC
RC des mandataires sociaux	RC	RC	RC	RC
Amendes civiles (procédures abusives)	so	so	so	so
Amendes administratives				
Amendes pénales				
Pénalités de retard (consécutifs au fait dommageable)	Cyber / RC ?	Cyber / RC ?	Cyber / RC ?	Cyber / RC ?
Pénalités PCI -DSS (UNIQUEMENT pour les banques)	so	so	so	so
Pénalités PCI -DSS (hors banques si applicable)	so	so	so	so

Erreur humaine

Garanties	Perte de fichiers	Livraison d'un logiciel endommagé	Transmission involontaire de données	Autres actions immatérielles involontaires (sans dommage matériel
Bâtiments	so	so	so	so
Marchandises	so	so	so	so
Matériels industriels	so	so	so	so
Matériels informatiques	so	so	so	so
Transport Maritime				
Transport Aérien				
Perte pécuniaire : remboursement des fonds détournés	so	so	so	so
Remboursement des rançons / sommes extorquées sous la	so	so	so	so
Frais de recours et de poursuites	so	so	so	so
Perte d'opportunité				
Perte de marge brute / de recette	Cyber ?	so	Cyber ?	Cyber ?
Frais supplémentaires d'exploitation (pour minimiser la perte	Cyber ?	so	Cyber ?	Cyber ?
Aggravation de PE à la suite d'une décision administrative légalement prise	Cyber ?	so	Cyber ?	Cyber ?
Frais de recherche de cause: - IT : Forensic, frais d expertise, d assistance... - Mat : frais d'expertise, de recherche de cause...	Cyber ?	so	Cyber ?	Cyber ?
Frais de reconstitution de données	Cyber ?	so	Cyber ?	Cyber ?
Frais supplémentaires (travaux activité sup., gestion de crise	Cyber ?	so	Cyber ?	Cyber ?
Conseils/ préconisations après attaque/ sinistre (remédiation	Cyber ?	so	Cyber ?	Cyber ?
Frais d'amélioration de la sécurité informatique du SI				
Frais de notification aux instances administratives	Cyber ?	so	Cyber ?	Cyber ?
Frais de comparution (enquêtes administratives)	Cyber ?	so	Cyber ?	Cyber ?
Frais de notification aux personnes concernées par une violation de données personnelles	Cyber ?	so	Cyber ?	Cyber ?
Conseil en communication / Relations Publiques / Gestion de	Cyber ?	so	Cyber ?	Cyber ?
Nettoyage- noyage	Cyber ?	so	Cyber ?	Cyber ?
Frais de référencement	Cyber ?	so	Cyber ?	Cyber ?
Plateforme téléphonique (n° vert)	Cyber ?	so	Cyber ?	Cyber ?
Conseil juridique (hot line, gestion de crise)	Cyber ?	so	Cyber ?	Cyber ?
Assistances juridiques : mise en œuvre de l'action juridique	Cyber ?	so	Cyber ?	Cyber ?
Honoraires d'avocats, d'huissiers, d'experts judiciaires	Cyber ?	so	Cyber ?	Cyber ?
Dommages matériels aux tiers	RC	RC	RC	RC
Dommages immatériels (aux tiers) consécutifs	RC	RC	RC	RC
Dommages immatériels non consécutifs	RC	RC	RC	RC
Dommages corporels (aux tiers)	RC	RC	RC	RC
Frais de retraits / dépose / repose	so	RC	so	so
Défense recours	RC	RC	RC	RC
RC des mandataires sociaux	RC	RC	RC	RC
Amendes civiles (procédures abusives)	so	so	so	so
Amendes administratives				
Amendes pénales				
Pénalités de retard (consécutifs au fait dommageable)				
Pénalités PCI -DSS (UNIQUEMENT pour les banques)	so	so	so	so
Pénalités PCI -DSS (hors banques si applicable)	so	so	so	so

Fraude

Fraude

Garanties	Cyber détournement de fonds	Fraude téléphonique	Vol (saisie effs.), escroquerie, abus de confiance, fauxsavoir de faux, falsification de chèque	Faits criminels / terroristes internationaux - Fraude au président
Bâtiments	so	so	so	so
Marchandises	so	so	Fraude	so
Matériels industriels	so	so	Fraude	so
Matériels informatiques	so	Fraude	Fraude	so
Transport Maritime	Corps et faculté ?	so	so	so
Transport Aérien	Dommages aéronefs	so	so	so
Perte pécuniaire : remboursement des fonds détournés	Cyber-Fraude	Fraude	Fraude	Fraude
Remboursement des rançons / sommes extorquées sous la	so	so	so	so
Frais de recours et de poursuites	Cyber-Fraude	Fraude	Fraude	Fraude
Perte d'opportunité				
Perte de marge brute / de recette	Cyber-Fraude	Fraude	Fraude	Fraude
Frais supplémentaires d'exploitation (pour minimiser la perte	Cyber-Fraude	Fraude	Fraude	Fraude
Aggravation de PE à la suite d'une décision administrative légalement prise	Cyber-Fraude	Fraude	Fraude	Fraude
Frais de recherche de cause: - IT : Forensic, frais d expertise, d assistance... - Mat : frais d'expertise, de recherche de cause...	Cyber-Fraude	Fraude	Fraude	Fraude
Frais de reconstitution de données	Cyber-Fraude	Fraude	Fraude	Fraude
Frais supplémentaires (travaux activité sup., gestion de crise	Cyber-Fraude	Fraude	Fraude	Fraude
Conseils/ préconisations après attaque/ sinistre (remédiation	Cyber-Fraude	Fraude	Fraude	Fraude
Frais d'amélioration de la sécurité informatique du SI				
Frais de notification aux instances administratives	so	so	so	so
Frais de comparution (enquêtes administratives)	so	so	so	so
Frais de notification aux personnes concernées par une violation de données personnelles	so	so	so	so
Conseil en communication / Relations Publiques / Gestion de	so	so	so	so
Nettoyage- noyage	Cyber-Fraude	Fraude	Fraude	so
Frais de référencement	so	so	so	so
Plateforme téléphonique (n° vert)	so	so	so	so
Conseil juridique (hot line, gestion de crise)	so	so	so	so
Assistances juridiques : mise en œuvre de l'action juridique	so	so	so	so
Honoraires d'avocats, d'huissiers, d'experts judiciaires	so	so	so	so
Dommages matériels aux tiers	RC	RC	RC	RC
Dommages immatériels (aux tiers) consécutifs	RC	RC	RC	RC
Dommages immatériels non consécutifs	RC	RC	RC	RC
Dommages corporels (aux tiers)	RC	RC	RC	RC
Frais de retraits / dépose / repose	so	so	so	so
Défense recours	RC	RC	RC	RC
RC des mandataires sociaux	RC	RC	RC	RC
Amendes civiles (procédures abusives)	so	so	so	so
Amendes administratives				
Amendes pénales				
Pénalités de retard (consécutifs au fait dommageable)	Cyber / RC ?	Fraude	Fraude	Fraude
Pénalités PCI -DSS (UNIQUEMENT pour les banques)	so	so	so	so
Pénalités PCI -DSS (hors banques si applicable)	so	so	so	so

Commentaires
Exclusion du cyber (Clause 380 ou équivalents)
A l'étude
Assurabilité des rançons en cours d'analyse
Risque d'entreprise
non assurable
non assurable
Pénalités contractuelles que les assureurs ne veulent pas couvrir
Point de discussion !!!

Dommages subis par l'assuré (first party)

Actifs de l'entreprise : -actifs corporels -actifs financiers

Frais et pertes : -pertes d'exploitation -frais de recherche -frais supplémentaires

Responsabilités de l'assuré

Protection juridique

Dommages causés par l'assuré à un tiers (third party)

Sanctions infligées à l'assuré

AIRBUS DEFENCE & SPACE

Recommandations issues des travaux de recherche

1- Promouvoir des analyses de risques quantifiées et coordonnées par les Risk Manager

2- Promouvoir un référentiel commun sur les risques cyber avec les assureurs

3- Améliorer la Communication et la Clarté des couvertures d'assurance du risque cyber

4- Bâtir les conditions d'un dialogue de confiance entre assurés et assureurs

5- Clarifier les incertitudes juridiques sur le risque cyber:

- De quoi parle-t-on ? Qualification juridique
- Sécuriser le continuum droit des contrats assurance, droit positif cyber et vocabulaire technique cyber

Conclusion

- La digitalisation vecteur de croissance économique
- La cyber sécurité environnement nécessaire pour permettre cette création de valeur
- Une transparence accrue demandée par les régulateurs et acteurs économiques (investisseurs, agences de notation)
- Une plus grande responsabilité directe des mandataires sociaux et des managers

Le management du risque cyber contribue à la valorisation et à la compétitivité de l'entreprise

Merci !

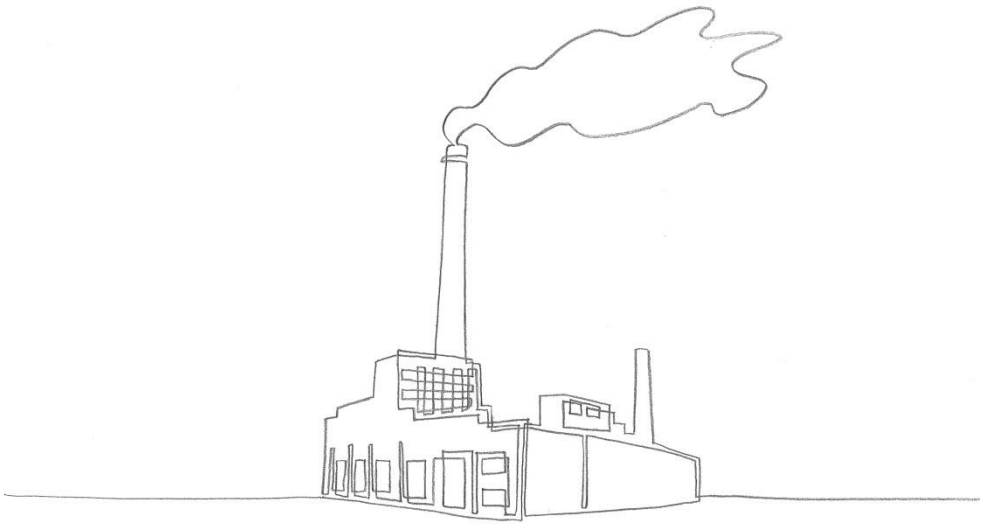
philippe.cotelle@airbus.com

Risques cyber et systèmes industriels

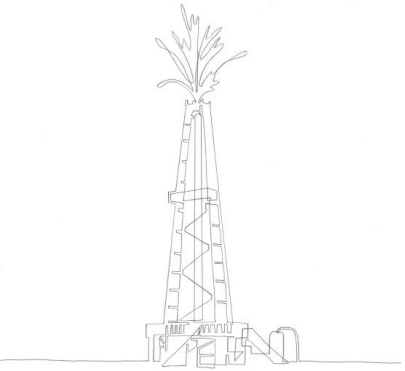
Jiman SANE - Beazley

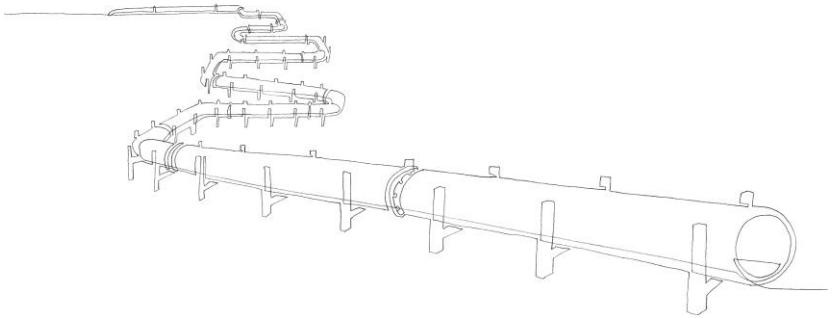
Risques Cyber et Systèmes Industriels

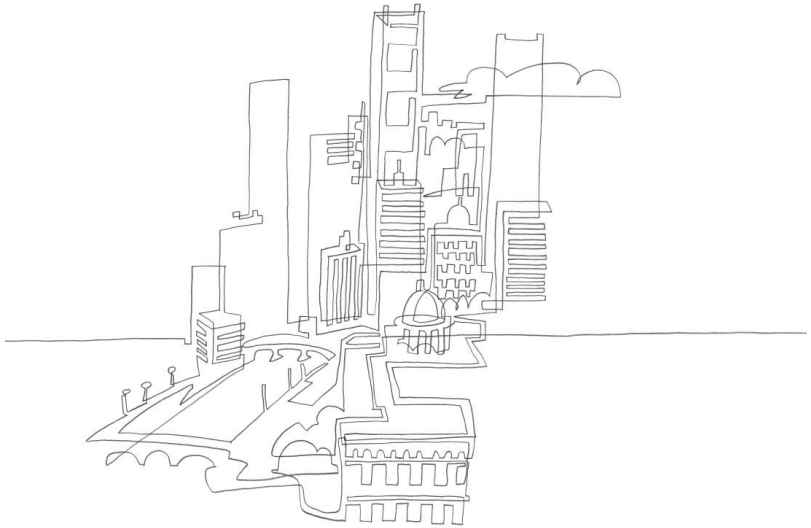
- **Particularités des Systèmes Industriels**
  - Systèmes SCADA
  - Robotique
  - Propriété Industrielle
- **Typologie des Attaques**
- **Auteurs présumés**
- **Assurances**

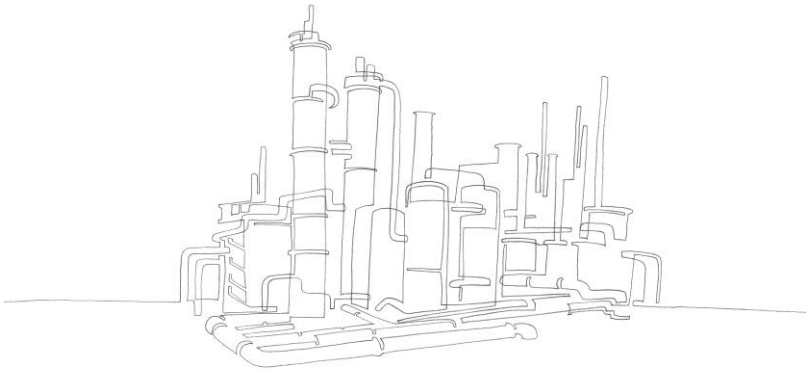


Cas pratiques









MERCI DE VOTRE ATTENTION !

AVANT DE PARTIR , N'OUBLIEZ PAS DE REMPLIR L'EVALUATION !

- Soit sur la feuille , à remettre à l'hotesse à la sortie
- Soit directement sur la **WEB APPLI**

Merci : vous participez à l'objectif ZERO PAPIER !

Les slides seront en ligne dès la semaine prochaine sur www.amrae.fr