
# Cybersécurité et Résilience

## *AMRAE – Commission ERM 360°*

*21 mai 2021*

# L'ANSSI en bref

## ANSSI – Agence nationale de la sécurité des systèmes d'information

- *Autorité nationale de défense et de sécurité*
- *Mission de conseil et soutien auprès des administrations et opérateurs d'importance vitale*
- *Mission de défense : veille, détection, alerte et réaction aux attaques informatiques*

## Bureau appui au Management des crises cyber

- *Définir les doctrines et référentiels opérationnels au niveau National et International en matière de Résilience et gestion de crise*
- *Accompagner la montée en maturité gestion de crise cyber des organisations*
- *Accompagner l'Agence, l'Etat et les bénéficiaires de l'Agence dans leur gestion de crise (volet stratégique)*

## Intervenant

- *Mathieu COUTURIER – Chef du bureau*

- Comprendre la menace cyber
- Anticiper et gérer le risque cyber
- Réagir face au risque cyber : la crise d'origine cyber
- Conclusion : rôle du risk manager ?

# 1. Comprendre la menace cyber

*2. Anticiper et gérer le risque cyber*

*3. Réagir face au risque cyber : la crise d'origine cyber*

# Une évolution croissante de la menace cyber

**+250%** *de cyberattaque en 2020*

*54 > 192*

*Existence d'acteurs systémiques*

*Interdépendance des systèmes*

*Interconnexion des systèmes*

*Facilité d'automatisation des attaques*

# Menaces cyber : quelles motivations ?

**LUCRATIVE**
*Cyber-mercenaires*
*Officines*

**IDÉOLOGIQUE**
*Hacktivistes*
*Cyber-terroristes*
*Cyber-patriotes*

**ÉTATIQUE**
*Unités spécialisées*

**TECHNIQUE**
*Hackers*
*chevronnés*
*Développeurs*
*Chercheurs*

# Menaces cyber : quelles finalités ?

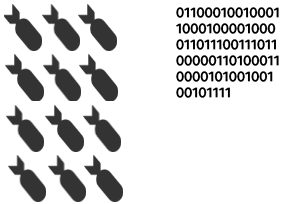
ESPIONNAGE

PRÉ-POSITIONNEMENT (INVASION)

AGITATION - PROPAGANDE

DESTRUCTION

FRAUDE




NEUTRALISATION

# Deux menaces principales à prendre en considération

## *Ranconlogiciel*

- *Attaque visant à déployer un logiciel malveillant permettant de chiffrer les données de la victime et de demander une rançon*
- *Conséquences dévastatrices, sur la continuité d'activité, voir la survie de l'organisation victime.*
- *Attaque opportuniste.*
- *Depuis 2018 : émergence du « Big Game Hunting »*
- *Comment s'en prémunir,* **un guide : « attaques par rançongiciels – tous concernés »**


## *Espionnage économique*

- *Captation par des moyens discrets, clandestins ou illégaux d'informations sensibles.*
- *Objectif de l'attaquant : maintenir discrètement son accès le plus longtemps possible afin de capter l'information stratégique en temps voulu.*
- *Il faut parfois des années pour s'apercevoir de l'intrusion.*
- *Coexistence d'attaquantes très sophistiquées et des attaques qui le sont moins.*

# Quels sont les impacts d'une menace cyber ?

## Impact Direct : financier et organisationnel

*Perturbations de l'organisation interne*

*Manques à gagner / Perte d'exploitation*

*Frais de reconstruction*

*Notification (GDPR)*

## Impact Indirect : l'image

*Un sujet au cœur de l'actualité*

*Un sujet fondamentalement technique mais aussi politique et sensible*

*Une communauté virale et exigeante*

*Une temporalité longue*

**En cas de crise, attention au dilemme :**

**Rétablir vite versus rétablir « bien »**

**Menace cyber : attention à l'impact d'image !**

**Un objectif : Maintenir la confiance pendant et après la crise**

# Pourquoi les attaques réussissent-elles trop souvent ?

## La sécurité du numérique n'est pas un état stable

*Des nouvelles vulnérabilités apparaissent quotidiennement et les modes opératoires des attaquants évoluent perpétuellement*

## La transformation numérique augmente les risques

*Vecteur d'innovation et de croissance, la transformation numérique présente aussi des risques en augmentant la surface d'attaque (ex. convergence IT/OT) ou concept de SI étendu (cloudisation))*

## Les systèmes d'information sont vulnérables

*La sécurité des systèmes d'information est souvent mal prise en compte dans le cycle de vie des systèmes*

## L'environnement technologique est en perpétuelle évolution

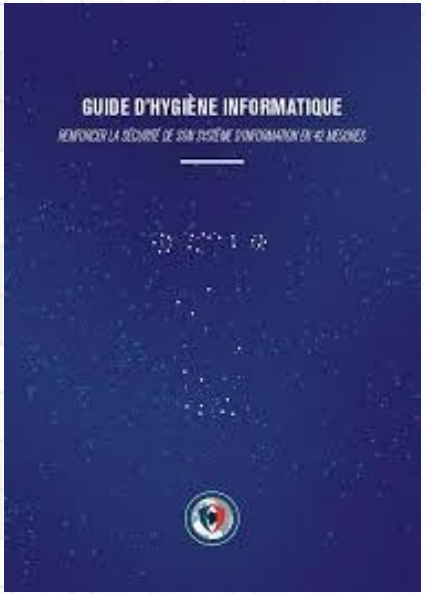
*La transformation rapide des technologies, des équipements et des usages créent un environnement en perpétuelle évolution, qui ne facilite pas la maîtrise de la sécurité des systèmes d'information*

*1. Comprendre la menace cyber*

## 2. Anticiper et gérer le risque cyber

*3. Réagir face au risque cyber : la crise d'origine cyber*

# Cybersécurité : quelques règles d'hygiène à appliquer




| | |
|---|---|
| **Sensibiliser et former** | ▪ Sensibiliser les utilisateurs au risque numérique |
| **Mettre en place un niveau de sécurité minimal** | ▪ Mettre en place les solutions de type pare-feu et anti-virus<br>▪ Limiter les droits des utilisateurs<br>▪ Sauvegarder les données vitales sur des supports déconnectés |
| **Authentifier et contrôler les accès au SI** | ▪ Mettre en œuvre les règles de bonnes pratiques relatives aux mots de passe ou mettre en œuvre des mécanismes d'authentification forte |
| **Maintenir le SI à jour** | ▪ Appliquer les mises à jour de sécurité pour tous les logiciels |
| | ▪ Gérer l'obsolescence des systèmes et des applications (ex. d'actualité fin de support de *Windows 7* et *Windows Server 2008* en janvier 2020) |
| **Sécuriser l'intérieur du réseau** | ▪ Cloisonner le réseau (ex. réseaux bureautique et industriel) |
| **Surveiller les systèmes** | ▪ Superviser les systèmes et les réseaux |
| **Sécuriser l'administration du réseau** | ▪ Appliquer les bonnes pratiques relatives aux comptes d'administration |

# L'analyse du risque cyber : un outil stratégique

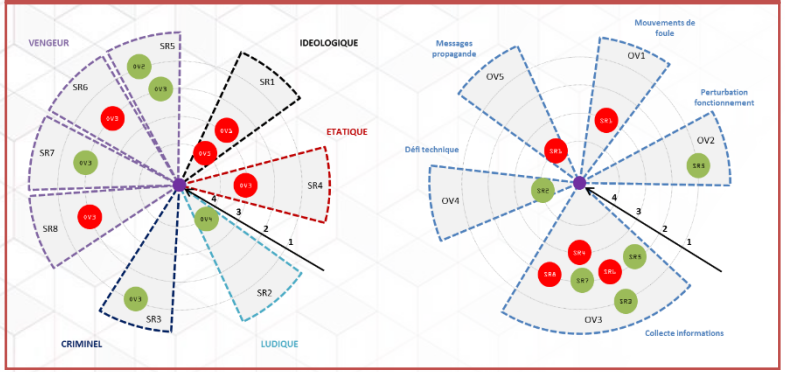

> *Le risque numérique est* **un risque d'entreprise transverse** *qui draine des enjeux stratégiques, économiques, politiques, d'image…*

> *À ce titre, il doit entrer dans la* **politique globale de gestion des risques** *des organisations.*

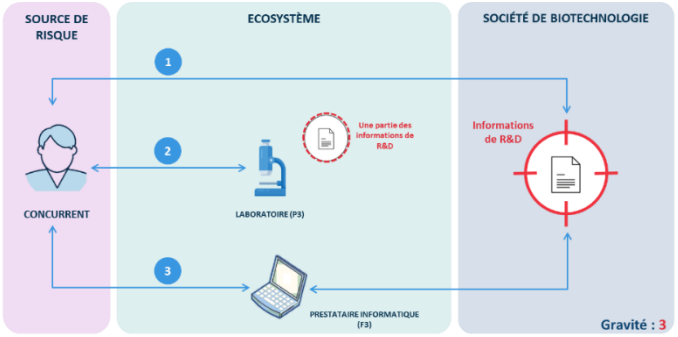
> *Si les experts de la sécurité numérique et de la maîtrise des risques s'emparent de la question, les faire* **parler d'une même voix** *pour porter un message commun est essentiel,*

# Une méthodologie : EBIOS Risk Management

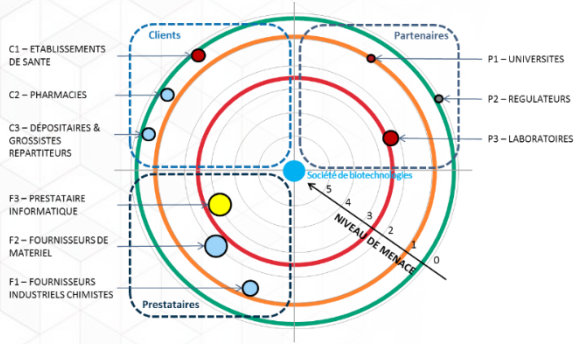
## CARTOGRAPHIE DE LA MENACE CYBER



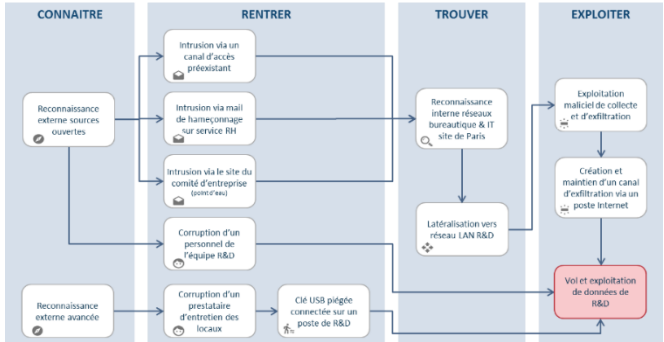

## SCENARIOS STRATEGIQUES




## CARTOGRAPHIE DU RISQUE DE L'ECOSYSTEME




## SCENARIOS OPERATIONNELS



# Focus sur la supply chain attack

- **Entreprise étendue** : *de plus en plus de partenaires, fournisseurs intégrés à l'entreprise*
- *Des* **dépendances** *avec des* **technologies** *mal ou peu maitrisées (outils de sécurité, cloud etc.)*
- *Un* **marché** *devenant de plus en plus* **centralisé** *: des vulnérabilités qui deviennent massives*

**Réaliser une priorisation de vos dépendances alignées avec votre chaine de valeur métier (*un petit prestataire peut être critique*)**

# Importance de la sensibilisation et de la culture : placer l'humain au centre du jeu

*FORMATION*

*SENSIBILISATION*

*ENTRAINEMENT*

# Assurance et risque cyber

- **Souscrire une assurance cyber ? Au-delà de la finalité de protection et couverture du risque résiduel, un « véhicule » pour rehausser son niveau de sécurité.**
  - Frais pris en charges : pertes directes/indirectes, frais de notifications/préservation-restauration de l'image/expertise technique/surveillance/justice/extorsion
  - Mesurer son exposition aux risques
  - Mesurer sa protection existante

*1. Comprendre la menace cyber*

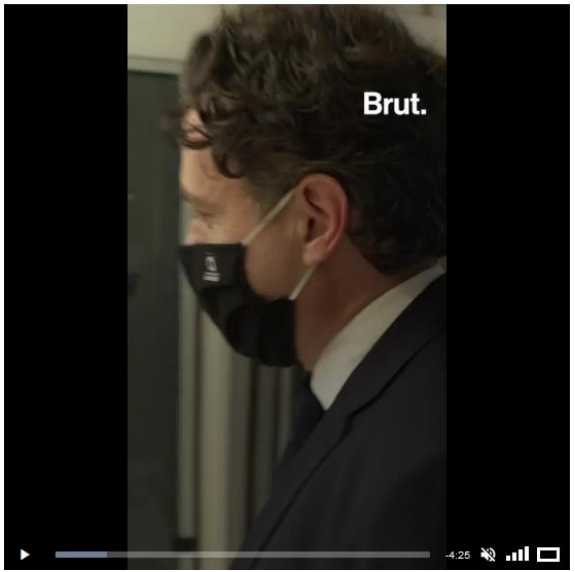
*2. Anticiper et gérer le risque cyber*

## 3. Réagir face au risque cyber : la crise d'origine cyber

# Cyber : prise de conscience du niveau de préparation et de protection

*"Je n'aurais pas cru qu'on serait amenés potentiellement à réactiver le fax du -1"*

*"On a plus que le téléphone et puis, plus d'informatique, bah plus d'Internet donc on a ressorti le code postal de 1989 qui va nous permettre d'avoir toutes les collectivités de France, avec leur code postal pour nous adresser leur courrier"*




**EXTRAIT VIDÉO « BRUT »**
**CYBERATTAQUE VILLE ANGERS**

https://www.brut.media/fr/news/victime-d-une-cyberattaque-les-services-de-la-ville-d-angers-paralyses-98ef8f15-267b-45a9-8413-10ca228d72c5

# Pourquoi gérer une crise cyber ?

**LIMITER LES IMPACTS D'UNE CRISE (ENTITÉ, ÉCOSYSTÈME, BÉNÉFICIAIRES)**

**ASSURER LA REPRISE DES ACTIVITÉS CRITIQUES DANS UN DÉLAIS ACCEPTABLE**

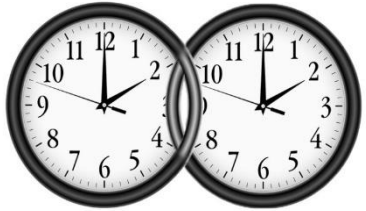
**MAINTENIR LA CONFIANCE DE L'ORGANISATION DANS SON ÉCOSYSTÈME**

Avec des ressources contraintes

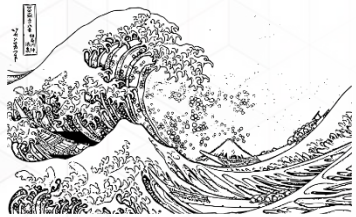
Sous pression en particulier « temporelle »

# Crise cyber : particularité à prendre en considération


Crise de nature technologique
centrée sur l'expertise



Double temporalité (effets immédiats et
remédiation longue)



Adaptation –
une menace intelligente qui s'adapte

Propagation –
Absence d'unicité de lieu

**/!\ IL N'Y A PAS DE CRISE CYBER, IL N'Y A QUE DES CRISES D'ORIGINE CYBER**

# RETEX : des dispositifs non adaptés à la menace cyber

- *Des dispositifs de continuité d'activité ou de reprise d'activité souvent* **non adaptés à la menace cyber** *: choc extrême « black-out numérique »*
- *Des dispositifs de crise* **non adaptés à des crises « longues »**
- *Une communication de crise* **pas** *suffisamment* **préparée et coordonnée**
- *De nombreux moyens opérationnels ou solutions de contournement* **non anticipés et non positionnés** *sur la chaine de valeur métier*
- *Une méconnaissance de la* **chaine de valeur** *et des* **systèmes critiques sous-jacents**

# Comment être résilient face à une crise d'origine cyber ?

**Je suis une organisation résiliente si je limite les impacts d'une crise d'origine cyber, je rétablis mes services critiques dans un délai acceptable et mon écosystème maintient sa confiance dans mon organisation et inversement**

**La résilience numérique désigne la capacité d'une organisation ou d'un secteur à :**

> *Définir des moyens opérationnels* de résilience adaptés aux scénarios de menaces cyber à mobiliser en cas de crise*

> *Prioriser et maintenir en mode dégradé les activités critiques impactées par la crise grâce à ces moyens*

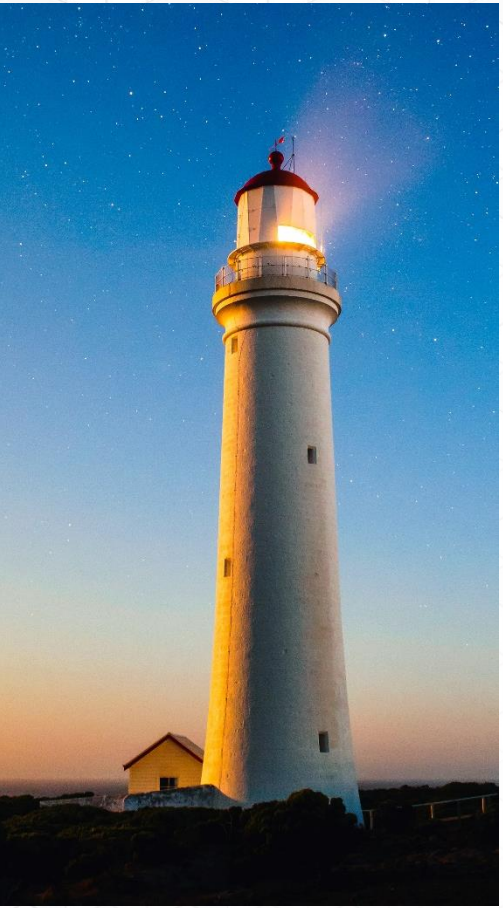
> *Reconstruire et rétablir les activités critiques internes comme externes dans un délai acceptable pour limiter les impacts*

***6 PILIERS OPÉRATIONNELS DE LA RÉSILIENCE**

- *Gestion de crise*
- *Communication de crise*
- *Continuité et reprise d'activité*
- *Gestion des tiers (y compris les fournisseurs de cloud)*
- *Cyberdéfense*
- *Reconstruction des systèmes d'informations*

*Cyber assurance inclus dans les différents aspects*

# Et le rôle du Risk Manager dans tout ca ?



- *Jouer le rôle de coordinateur pour focaliser les efforts de protection, défense et résilience sur ce qui est important pour l'organisation*
- *Comprendre quels dispositifs contribuent à faire face aux menaces et s'assurer qu'ils sont efficients : répondre à la question « pouvons nous faire face aux menaces ? » et le matérialiser pour la Direction Générale*
- *Prendre en compte les nouvelles technologies (IA, Cloud, ordinateur quantique etc.) et leur impact sur la chaine de valeur*

⇒ **Le risk manager joue un rôle de tour de contrôle (2ND ligne de défense), d'aide à la priorisation et à la valorisation du dispositif**

# Pour aller plus loin !

- **ATTAQUES PAR RANÇONGICIELS, TOUS CONCERNÉS – COMMENT LES ANTICIPER ET RÉAGIR EN CAS D'INCIDENT ?** https://www.ssi.gouv.fr/administration/guide/attaques-par-rancongiciels-tous-concernes-comment-les-anticiper-et-reagir-en-cas-dincident/
- **MAÎTRISE DU RISQUE NUMÉRIQUE – L'ATOUT CONFIANCE :** https://www.ssi.gouv.fr/administration/guide/maitrise-du-risque-numerique-latout-confiance/
- **LA MÉTHODE EBIOS RISK MANAGER – LE GUIDE :** https://www.ssi.gouv.fr/administration/guide/la-methode-ebios-risk-manager-le-guide/
- **GUIDE D'HYGIÈNE INFORMATIQUE :** https://www.ssi.gouv.fr/administration/guide/guide-dhygiene-informatique/
- **ORGANISER UN EXERCICE DE GESTION DE CRISE CYBER :** https://www.ssi.gouv.fr/administration/guide/organiser-un-exercice-de-gestion-de-crise-cyber/

DES QUESTIONS ?

Mathieu COUTURIER – mathieu.couturier@ssi.gouv.fr