LES FONDAMENTAUX DE LA GESTION DE CRISE CYBER

.!CON

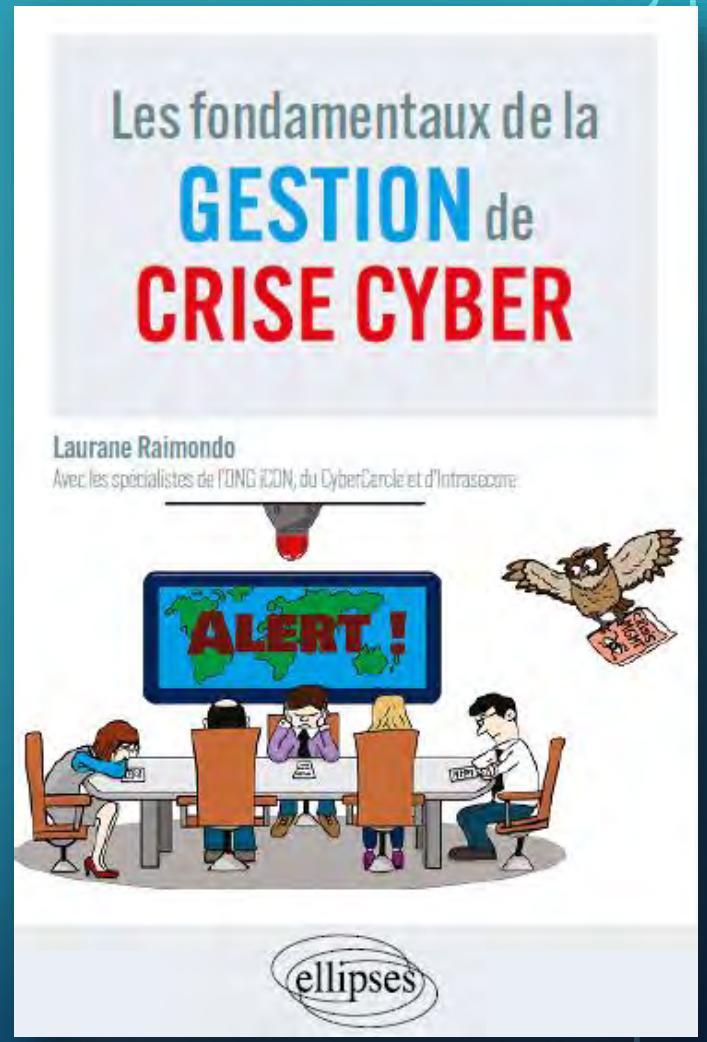
CYBER CERCLE

LRCS
Protection des données
Cybersécurité

ILERI
INSTITUT LIBRE DES RELATIONS INTERNATIONALES ET DES SCIENCES POLITIQUES

LAURANE RAIMONDO

- Directrice du Master Relations Internationales & Cyberespace – Ileri
- Chargée de cours magistral – Université Jean Moulin Lyon 3
- LRCS protection des données-Cybersécurité
- Advisor CyberCercle
- Stratégiste confiance numérique iCON NGO
- Prix du livre FIC 2022
- Prix de la femme chercheure cyber CEFCYS 2021
- Prix du Gouverneur militaire de Lyon 2019
- Auteure de La protection des données en 100 questions-réponses (2021 Ellipses)
- Auteure des Fondamentaux de la gestion de crise cyber (2022 Ellipses) rédigé avec un panel d'expert (iCON NGO, CyberCercle, Intrasecure)



2023 : L'ANSSI & LES 5 MESURES PRÉVENTIVES PRIORITAIRES

Renforcer l'authentification sur les systèmes d'information ; accroître la supervision de sécurité ; sauvegarder hors-ligne les données et les applications critiques ; établir une liste priorisée des services numériques critiques de l'entité ; s'assurer de l'existence d'un dispositif de gestion de crise adapté à une cyberattaque.

S'ASSURER DE L'EXISTENCE D'UN DISPOSITIF DE GESTION DE CRISE ADAPTÉ ÀUNE CYBERATTAQUE

Une cyberattaque peut avoir un effet déstabilisateur sur les organisations. Les fonctions support comme la téléphonie, la messagerie mais aussi les applications métier peuvent être mises hors d'usage. Il s'agit alors de passer en fonctionnement dégradé et dans certains cas, cela signifie revenir au papier et au crayon. **L'attaque cause en général une interruption d'activité partielle et, dans les cas les plus graves, une interruption totale.**

Définir des points de contact d'urgence, y compris chez les prestataires de services numériques et s'assurer d'**avoir les numéros en version papier** est particulièrement utile dans ces situations. Au-delà, il s'agit pour les organisations de **définir un plan de réponse aux cyberattaques** associé au **dispositif de gestion de crise** – quand il existe – visant à assurer la continuité d'activité, puis son retour à un état nominal. La **mise en œuvre d'un plan de continuité informatique** doit permettre à l'organisation de continuer à fonctionner quand survient une altération plus ou moins sévère du système d'information. Le plan de reprise informatique vise, quant à lui, à remettre en service les systèmes d'information qui ont dysfonctionné. Il doit notamment prévoir la restauration des systèmes et des données.

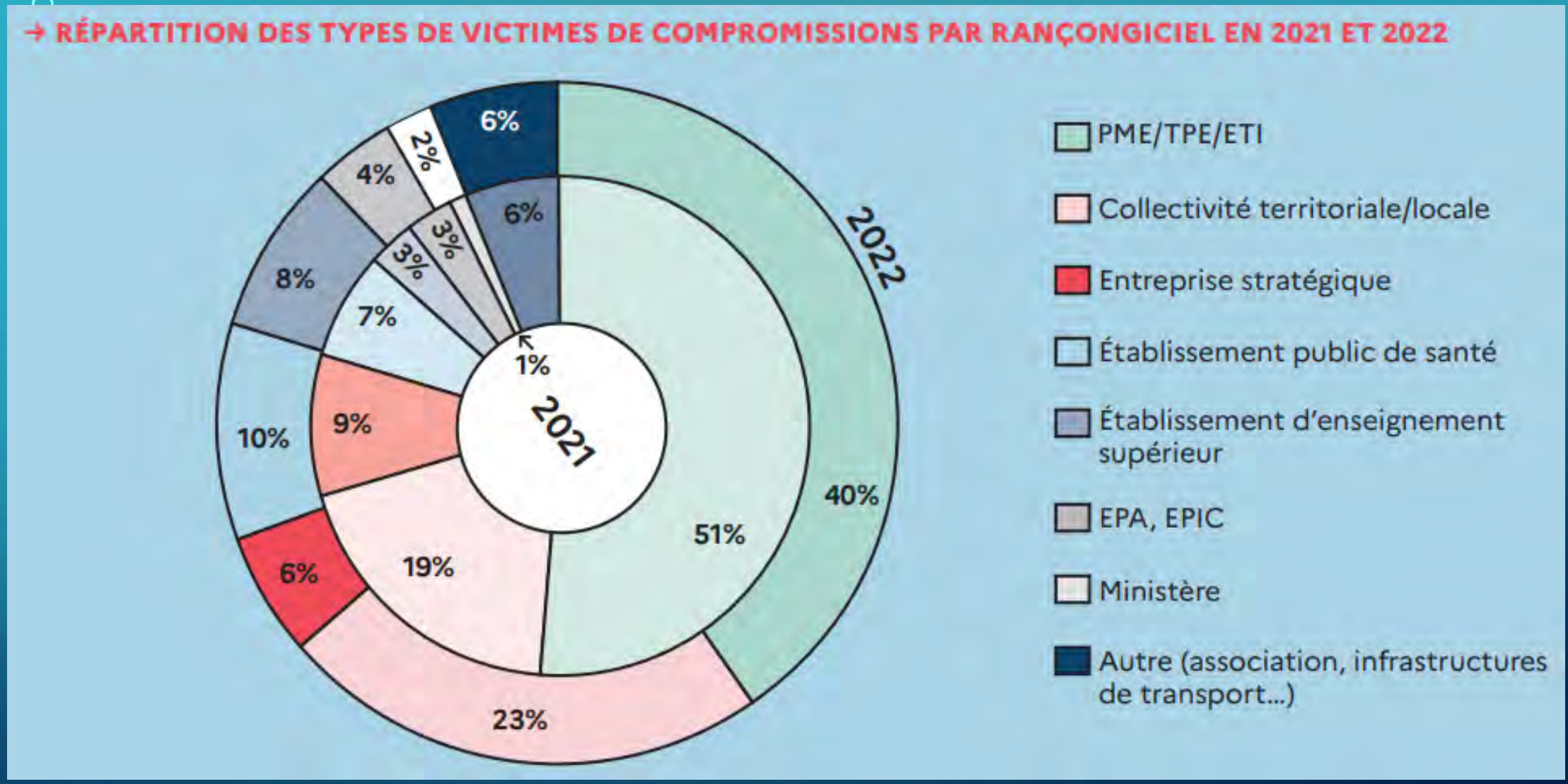


Figure 1 : La répartition des victimes de compromissions de rançongiciel (source : CERT-FR)

« IL NE PEUT PAS Y AVOIR DE CRISE LA SEMAINE PROCHAINE : MON AGENDA EST DÉJÀ PLEIN »

HENRY KISSINGER

La crise, un événement indésirable devenu nécessaire

I. Les origines & définitions de la crise cyber
II. La gestion de crise cyber et crise « classique », entre similitudes et divergences
III. L'anticipation de la crise cyber, clef de la réussite
IV. La législation, pilier d'anticipation et de réponse à la crise cyber
V. Technique et gouvernance, l'indissociable équipe
VI. Se former, préparer et animer une simulation ou un exercice de gestion de crise cyber
VII. Au cœur de la crise cyber, organiser et réagir avec efficacité
VIII. La communication de crise
IX. Savoir sortir de la crise et l'importance du retour d'expérience pour préparer la prochaine crise

I. LES ORIGINES & DÉFINITIONS DE LA CRISE CYBER

- Du grec ancien *krisis* au latin *crisis* : **action** de trier, séparer, distinguer différents ensembles de choses confondues, approchant le sens de « passer au crible »
- La crise désigne une situation inhabituelle, qualifiée de grave, exposant au danger avec un risque de mort (propre ou figuré), le terme a évolué. C'est donc devenu une **situation indésirable à laquelle personne ne souhaite être confronté au point de rejeter son idée** même.

Les Croods (2013), famille préhistorique pour qui toute nouveauté est synonyme de mort imminente

Les crises s'approchent :

- Par « impact »
- Par l'approche « sectorielle »
- **Par l'approche « complexe » :** un évènement « *inattendu, indésirable, imprévisible et impensable qui, la plupart du temps, produisent de l'incertitude et de l'incrédulité* ». C'est tout simplement l'expression même de l'incertitude la plus complète quant aux comportements d'un système d'une complexité qui nous échappe.

L'organisation affronte une situation inattendue, dans une incertitude omniprésente où il devient indispensable de s'adapter avec les moyens disponibles, voire d'improviser, pour limiter au mieux les conséquences voire même de prospérer de (et au sein de) cette instabilité.

« la crise est le produit d'une dynamique non-linéaire touchant un système complexe (une organisation) ou multi-complexe (un écosystème d'organisations) »

Raphaël de Vittoris

II. SIMILITUDES & DIVERGENCES

TOUTES LES CRISES

- La **chance**
- Le **timing**
- La **panique**
- La **continuité d'activité**
- La **communication**

LES CRISES CYBER

- La **gouvernance**
- La **décision de paiement**
- L'**absence de signaux avant-coureurs**
- La **croyance d'effet uniquement processuel et non pas humain**
- L'**embarras des décideurs**
- **Temporalité et espace**

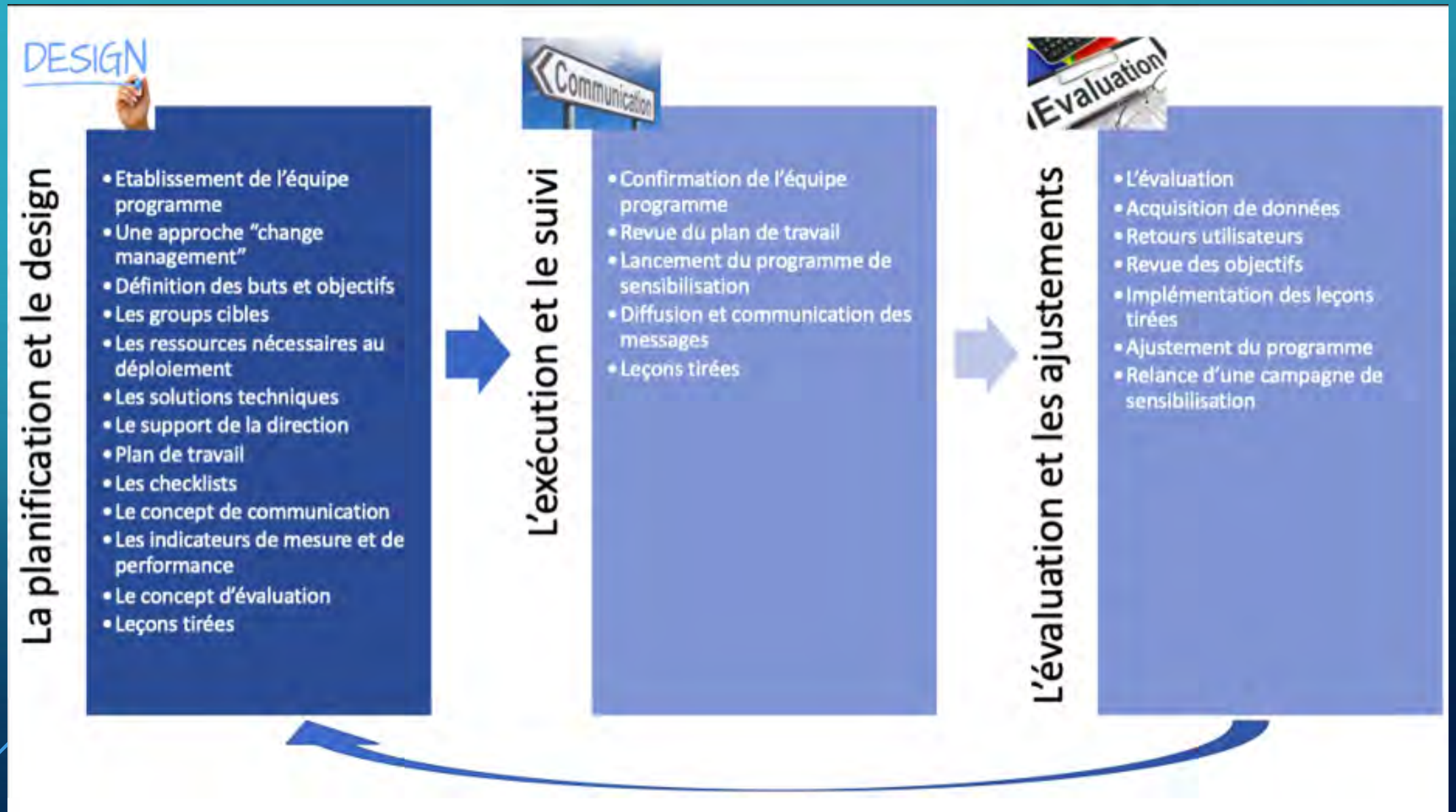
III. ANTICIPER, LA CLEF ?

« Mieux vaut prévenir que guérir »… sauf en matière cyber !

La **probabilité** de réussite d'une attaque doit être le centre de l'anticipation, pas son évitement.

La véritable clef : prévention permanente, technique et humaine

Vue complète du processus et des sous-processus de la méthode ENISA d'établissement d'une campagne de sensibilisation en entreprise (traduction et quelques légers ajustements libres de Pascal Steichen)



LES TEXTES, PILIER D'ANTICIPATION ET DE RÉPONSE À LA CRISE CYBER

- Règlement général sur la protection des données (RGPD) : Il s'agit d'un règlement de l'Union européenne (UE) qui établit un cadre juridique pour la protection des données personnelles dans l'UE.
- Directive NIS 2 (Network and Information Security) : Cette directive européenne vise à renforcer la cybersécurité au sein de l'UE en imposant des exigences aux opérateurs de services essentiels et aux fournisseurs de services numériques.
- Directive ePrivacy : Elle vise à protéger la vie privée et les communications électroniques en réglementant l'utilisation des données personnelles dans les services de communication électronique.
- Norme ISO/IEC 27001 : Bien qu'elle ne soit pas une législation ou une directive, cette norme internationale est largement utilisée comme référence pour la mise en place d'un système de gestion de la sécurité de l'information (SMSI).
- Règlement eIDAS : Ce règlement établit un cadre juridique pour l'identification électronique et les services de confiance au sein de l'UE, garantissant la sécurité des transactions électroniques et la reconnaissance mutuelle des identités numériques.
- Directive sur la protection des infrastructures critiques (Directive PIC) : Cette directive vise à garantir la sécurité des infrastructures essentielles dans l'UE, notamment en ce qui concerne les systèmes d'information critiques.
- Directive sur la sécurité des réseaux et de l'information (Directive SRI) : Cette directive européenne établit des exigences de sécurité pour les opérateurs de services essentiels et les fournisseurs de services numériques.
- Règlement sur la cybersécurité de l'Union européenne (UE) : Ce règlement, adopté en 2019, vise à renforcer la cybersécurité dans l'UE en établissant un cadre de certification des produits et services liés à la cybersécurité.
- Norme ISO/IEC 27002 : Cette norme fournit des lignes directrices pour l'établissement et la mise en œuvre de mesures de sécurité de l'information dans les organisations.

ETRE CONFORME EST NON SEULEMENT OBLIGATOIRE, MAIS FONDAMENTAL POUR LA SECURITE DE VOTRE ORGANISATION !!!

TECHNIQUE ET GOUVERNANCE, L'INDISSOCIABLE ÉQUIPE

TECHNIQUE ≠ GOUVERNANCE ?

Trois erreurs à éviter :

- Utiliser la gouvernance pour expliquer comment le travail doit être fait
- Essayer d'anticiper tous les scénarii possibles
- Exécuter en vase clos les préparations des différentes équipes

SE FORMER, PRÉPARER ET ANIMER UNE SIMULATION OU UN EXERCICE DE GESTION DE CRISE CYBER

.!CØN

CAPTURE THE FLAG

- Toutes les organisations doivent-elles réaliser des simulations de crise cyber ?

Pour qui, pour quels objectifs, quels coûts ?

AU CŒUR DE LA CRISE CYBER, ORGANISER ET RÉAGIR AVEC EFFICACITÉ

« L'ingrédient secret au cœur de la crise, c'est le pilotage ! » (Jérôme SAIZ)

- Le ROC : forte capacité organisationnelle, solides connaissances techniques, capacités d'écoute, de synthèse, de communication, ainsi que l'empathie, la ponctualité, l'attention aux détails, la capacité à résoudre les conflits, à organiser le chaos, à mener plusieurs tâches de front.
- Responsabilités : suivre la montée en charge du dispositif, du gréement des différentes cellules au suivi des premières actions techniques, compilation des premières synthèses managériales. Pas en charge de ces différentes actions mais doit s'assurer qu'elles ont bien lieu.
- Profil externe préférable

AU CŒUR DE LA CRISE

Cyberattaque :

- Phase 1 : découverte et déclenchement du plan de gestion de crise
- Phase 2 : intervention du prestataire ou des équipes internes pour la remédiation

Les premières heures :

- Tout consigner (même à la main)
- Activation des cellules de crise (décisionnelle & technique)
- Appeler l'assureur ou à l'aide
- Observation globale de la cellule décisionnelle : qu'est-ce qui fonctionne encore ? Qu'est-ce qui ne fonctionne plus ? Cela concerne quelles chaînes de production, ou quels bureaux ? Combien de collaborateurs ? Peut-on venir travailler demain ? Quels projets critiques ne pourront pas être livrés ?
- Observation globale de la cellule technique : piloter les mesures d'isolation et de collecter les informations nécessaires à la cellule décisionnelle

La crise installée :

- Rythme de croisière enclenché
- Ne jamais redémarrer trop vite : consacrer 48h à l'investigation
- La question épineuse de la date de compromission… Quels fichiers, par qui, pour quoi…
- Une rançon, doit-on payer ?
- Communiquer : à qui, comment et quand ?
- Quand et comment redémarrer ?
  - date d'intrusion initiale & « marqueurs »
  - **Changement des secrets**
  - **La réouverture d'Internet**
  - **La resynchronisation**
  - **Prendre soin des équipes**

COMMUNIQUER EN CAS DE CRISE CYBER

Cinq étapes vous aideront à communiquer de manière efficace pendant la crise

1. Une bonne préparation c'est presque la moitié de la bataille.

2. Afin de réagir de façon optimale, il convient tout d'abord de suivre les pistes de réflexion suivantes : Hiérarchie de l'information ; scénarios de la meilleure et de la pire éventualité ; scénarios de crise possibles (en globalité).

3. Qui, dans l'entreprise, est la personne de contact pour les personnes extérieures en temps de crise.

4. Pensez aux outils de veille digitale.

5. Une réponse rapide : la proactivité avant tout !

Le temps de réaction d'une entreprise en temps de crise représente souvent un avantage décisif. C'est pourquoi, en cas de crise, une chose en suit une autre : fournir une vue d'ensemble ; compiler des faits et des chiffres ; préparer des questions/réponses ; rédiger des communiqués de presse ; être disponible pour des demandes de renseignements ; communiquer en continu, la communication ne doit pas s'arrêter.

ATTENTION A L'INFODEMIE !

SAVOIR SORTIR DE LA CRISE ET L'IMPORTANCE DU RETOUR *D'EXPÉRIENCE* POUR PRÉPARER LA PROCHAINE CRISE

- Sortir de crise ≠ sortir de la gestion d'incident
- Sortie de crise si :
  - L'incident est terminé
  - L'incident perdure : épuisement des équipes, difficultés de mettre en place les actions, coûts démesurés

  →Identifier le bon moment
- Arrêt ou diminution des mesures spécifiques, attention aux répercussions

« Il ne faut pas confondre vitesse et précipitation… mais il faut savoir prendre des décisions »

Christophe Frey

- Quelqu'un doit décider de la sortie de crise
- Rédiger un Procès-Verbal de fin de crise
- Réaliser un bilan « à chaud » de la crise
- la cellule de crise passe le relais à l'équipe de gestion des incidents
- Continuer de communiquer
- Continuer de se faire accompagner
- Ne pas rater sa communication de fin de crise
- Passer au RETEX :
  - Ne pas clore le chapitre, faire un RETEX à chaud, tiède ET à froid, individuel & en groupe
  - Etudier les éléments collectés, débriefer
  - Si possible, travailler avec un observateur extérieur
- Formaliser les observations et formuler des recommandations

Pour vous accompagner

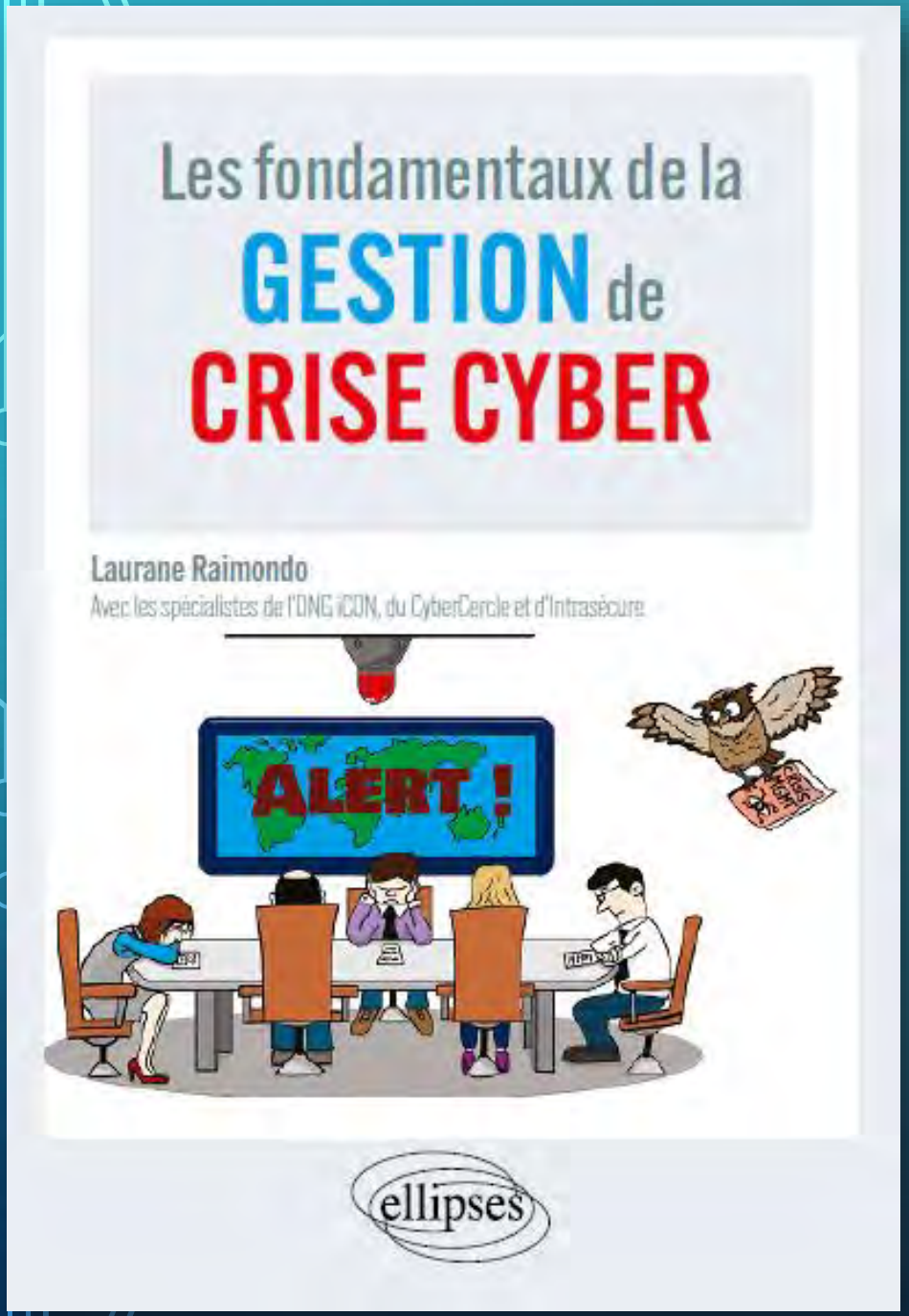
- Le guide des crises d'origine cyber, gestion opérationnelle et stratégiques de l'Anssi : https://www.ssi.gouv.fr/particulier/guide/crise-dorigine-cyber-les-cles-dune-gestion-operationnelle-et-strategique/

- La méthode de référence française : EBIOS - https://www.ssi.gouv.fr/administration/management-du-risque/la-methode-ebios-risk-manager/

- La méthode optimisée d'analyse des risques CASES Luxembourg : MONARC - https://www.cases.lu/services/monarc_fr.html

- La norme internationale qui traite de la gestion des risques en matière de sécurité de l'information ISO/IEC 27005

- La Norme pour le management de la continuité d'activité ISO 22301:2019



La cybersécurité est devenue une préoccupation majeure de toute organisation en termes de sécurité. Si l'aspect technique est essentiel, **tenir compte du facteur humain** ne l'est pas moins. Ainsi, connaître les origines des crises, les divergences entre celles d'hier et celles de demain, les modus operandi des cybercriminels, se tenir informé sur les outils à disposition, se former aux réflexes à adopter, les différentes législations, constituent les clefs d'une gestion de crise efficace, qui seule permet la résilience des organisations face aux cyberattaques.

Les crises sont inévitables. S'il n'est pas possible de les anticiper toutes, il est possible de s'en sortir avec des dommages négligeables si on s'y prépare. De la création de la cellule de crise à la communication interne et externe jusqu'au retour d'expérience, les étapes détaillées dans le présent ouvrage permettent d'avoir un coup d'avance sur les cyberincidents et les cyberattaques.

Entrepreneur, manager, élu, étudiant ou toute personne intéressée par la **gestion du risque et de la menace cyber** : voici le premier manuel de gestion de crise cyber traitée sous un angle humain par des experts issus du monde francophone.

Ont contribué à l'ouvrage : Stéphane Duguin – David Ferreira – Nicolas-Loïc Fortin – Christophe Frey – Lennig Pedron – Myriam Quemener – Juan Ramos – Jérôme Saiz – Pascal Steichen – Bertille Vallet – Raphaël de Vittoris – Paul Wang

Et ont participé : Aris Adamantiadis – Mélanie Bénard-Crozat – Phedra Clouner – Samuel Dixneuf – Jean-Pierre Therre