EY Cyber

Ransomware : Pourquoi et comment négocier avec un hacker

Octobre 2019

Olivier HERISSON, Manager en sécurité numérique

The better the question. The better the answer.
The better the world works.

Building a better working world

CONTEXTE

1

Une conduite à tenir

- Ne pas payer la rançon.

2

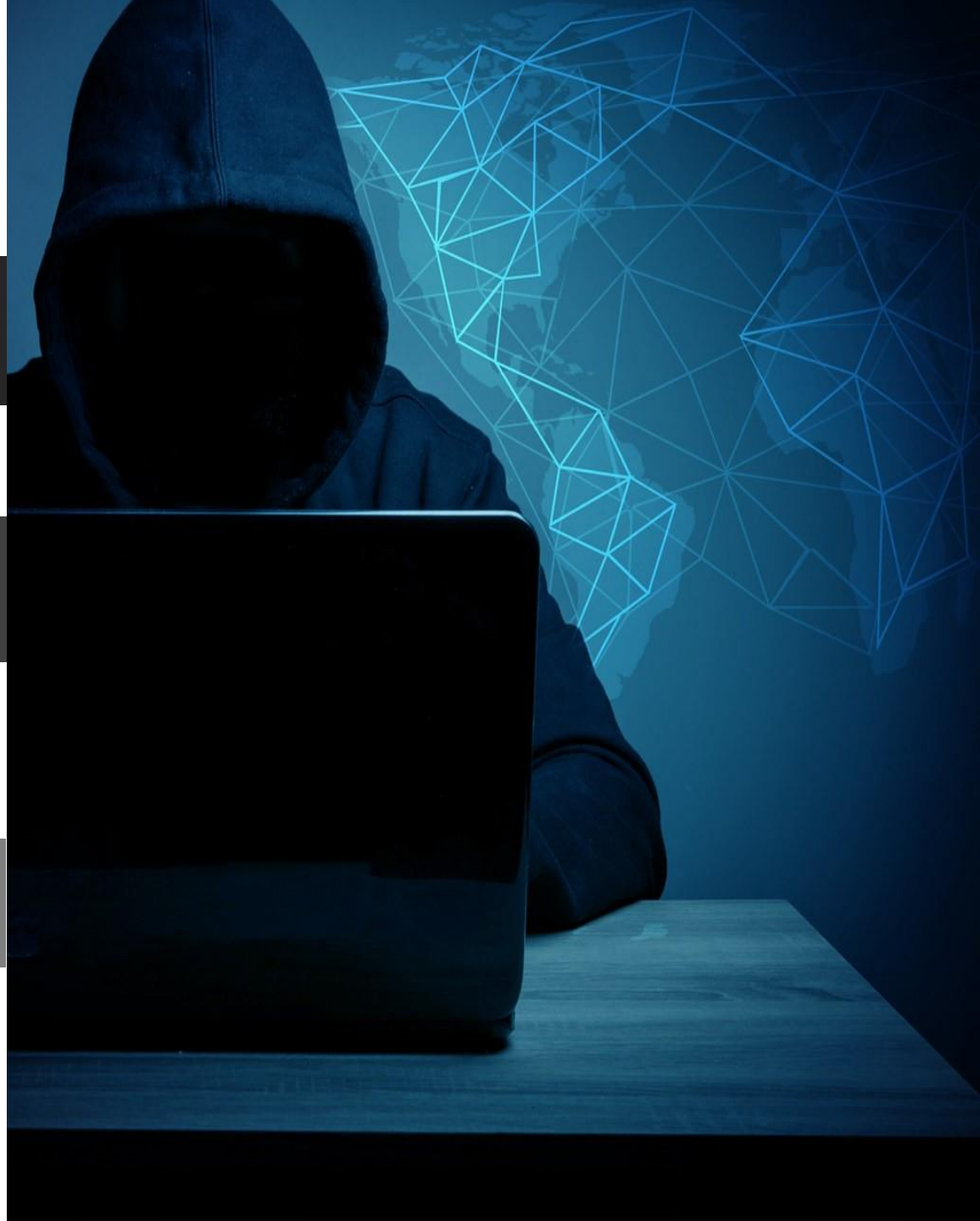
Une réalité bien différente…..

- Quelques exemples

3

Une expérience a partager

- Des exemples réels.
- Proposer quelques outils




LE THÈME

Cyber # Training

Votre sous-traitant en charge de l'application « gestion de la paie » (mode Saas) vous annonce qu'il vient d'être victime d'une attaque de type Ramsomware.
Le malware a chiffré l'ensemble de la base contenant les données des fiches de paie de vos salariés (3000 personnes concernées) :

- **Le hacker affiche sur les écrans son adresse email permettant de le contacter.**
- **Vous avez 24h pour payer 20 bitcoins. Passé ce délai les données seront détruites.**
- **Vos dernières sauvegardes ont 6 mois.**
- **Le malware est connu sur « nomoramsom » mais la souche a été modifiée !**

Toute ressemblance avec des cas vécus par des participants présents dans la salle est fortuite !

LA NÉGOCIATION

POURQUOI NEGOCIER ?

Gagner du temps

Diminuer l'impact Business

Diminuer l'impact sur la vie privée

- Répondre à l'incident
- Organiser, déclencher la cellule de crise
- Organiser la reprise d'activité
- Diminuer le montant de la rançon
- Empêcher la diffusion
- Prévenir les victimes


RISQUE
JURIDIQUE ?

LA CELLULE DE CRISE CYBER

COMMENT S'ORGANISER ?

1

Identifier les différents acteurs

- En fonction de votre société
- Le coordinateur
- Le négociateur
- Le décideur

2

Intégrer le Data Protection Officer,

- Gestion de la violation de données à caractère personnel
- Analyse des risques sur la vie privée (AIVP)
- Communication ?

Cellule de crise Cyber

#Rôles

#Coordination

#action

3

Coordonner, Décider, agir

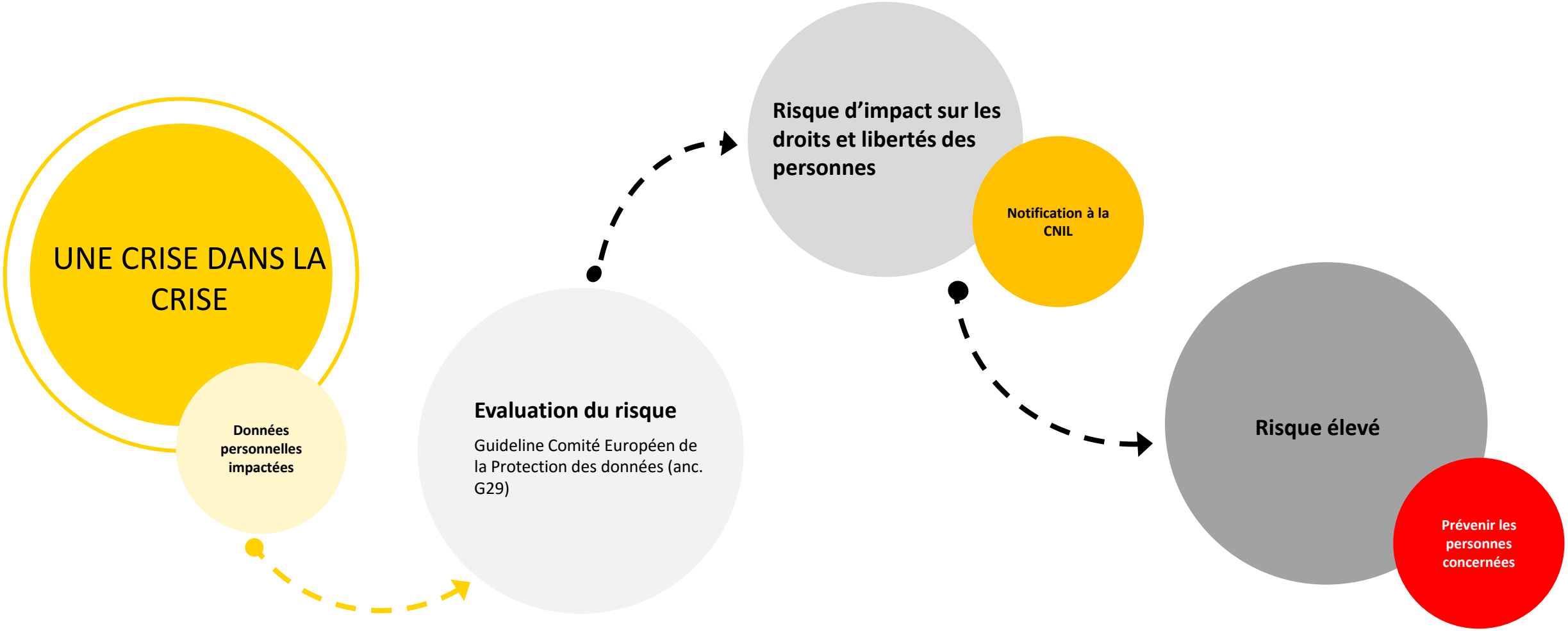
- Piloter
- Communiquer efficacement
- Relation avec les autorités
- Remédier

4

Clôturer l'incident

- Débriefer
- Capitaliser

ZOOM SUR LE RÔLE DU DATA PROTECTION OFFICER (DPO)



Guideline CEPD*

- *DICP, nature et sensitivité des données , volume des données*
- *Faciliter d'identification des personnes concernées, sévérité des conséquences pour les personnes, caractéristiques spéciales des personnes*
- *Nombre de personnes concernées, caractéristiques spéciales du RT, contexte général et vraisemblance.*


COMMENT
NÉGOCIER ?

CONSEILS POUR OPTIMISER LA NÉGOCIATION

1 Le décideur ne négocie pas !

- Le décideur en retrait, défini la stratégie.
- Inflation narcissique (Cf. Laurent Combalbert, ADN)
- Perte de l'effet fusible, situation de confort

2 Mettre son égo dans sa poche

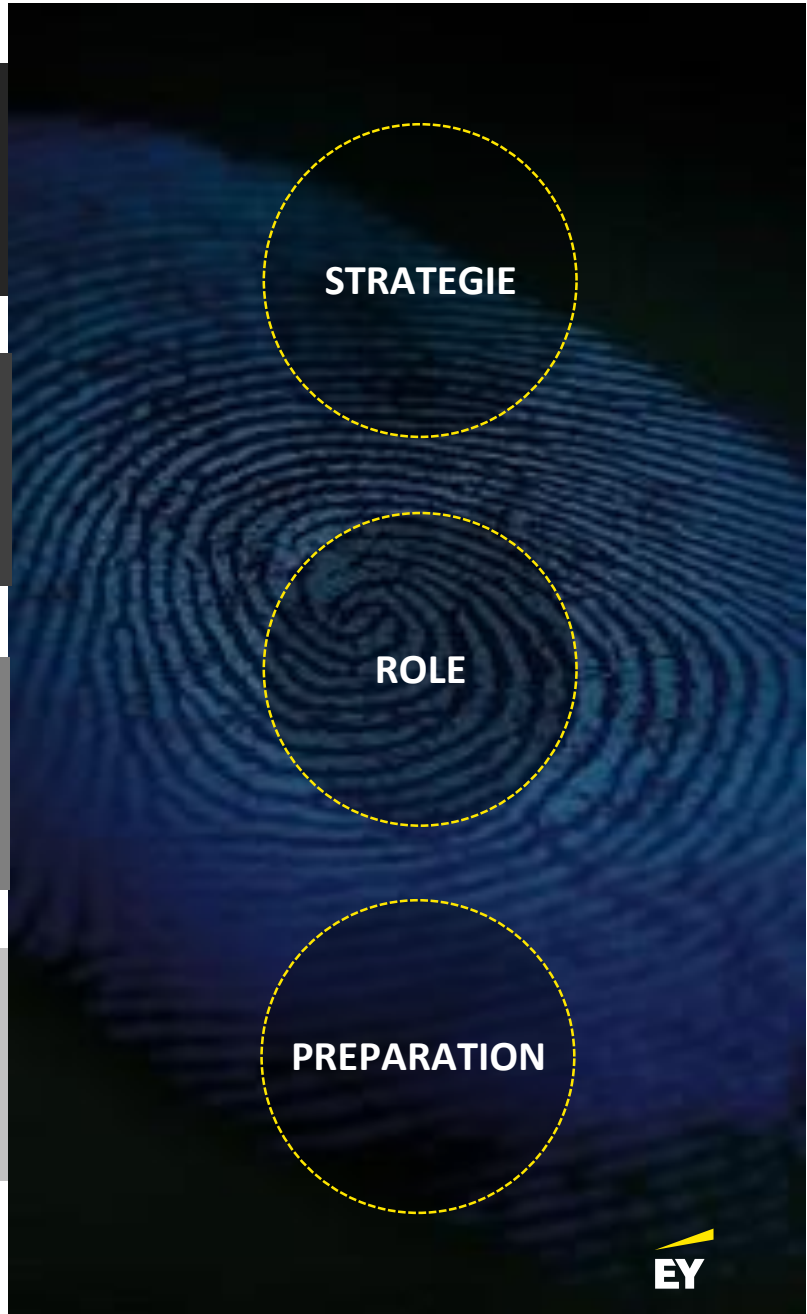
- Le hacker est en position de force
- Ne pas montrer l'inversion du rapport de force

3 Définissez votre stratégie

- Le mandat du négociateur
- Parler de la tactique ?

4 Différencier la position, l'objectif et l'intérêt

- Position affichée : 20 btc, (l'ultimatum n'est qu'un moyen de pression)
- Parler du Ramsomware auto vs vol de données (ubber)



CONSEILS POUR OPTIMISER LA NÉGOCIATION

5

Protéger votre intérêt !

- Tous les moyens sont bons …

6

Poser des questions

- Collecter de l'information sur votre adversaire (connectivité, verbatim, profil)
- L'égo du hacker……

7

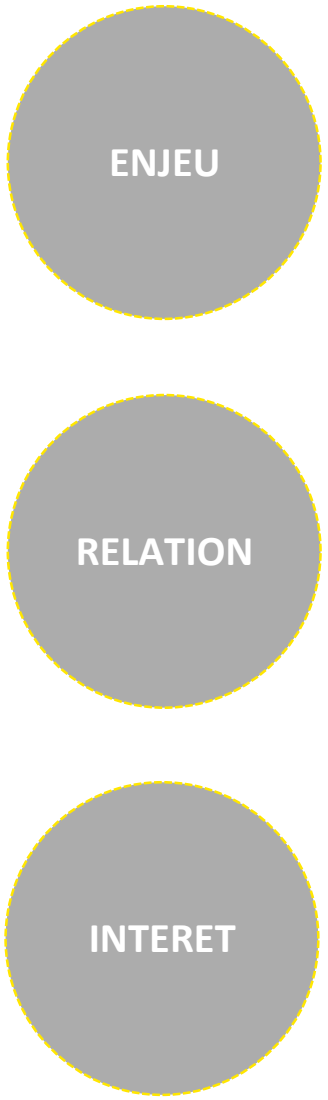
Créer un lien avec le hacker

- Dédiabolisation
- Visualisation et empathie

8

Diminuer l'enjeu

- Pour moi négociateur, quels sont mes risques ?



POUR RÉSUMER :

1 Anticipez !

Rédigez et testez vos procédures

Organisez votre cellule de crise

Préparez votre négociation 2

Définissez vos stratégies, votre intérêt à négocier

3 Pendant la négociation

Adoptez une position basse

Créer un lien avec le hacker (si vous pouvez)

Adaptez votre stratégie

Clôturez votre négociation quand vous avez atteint votre objectif

Débriefez ! 4

Echangez sur les déroulement de l'incident, conserver une main courante

Enrichissez vos procédures


MERCI

EY | Audit | Conseil | Fiscalité & Droit | Transaction

EY est un des leaders mondiaux de l'audit, du conseil, de la fiscalité et du droit, des transactions. Partout dans le monde, notre expertise et la qualité de nos services contribuent à créer les conditions de la confiance dans l'économie et les marchés financiers. Nous faisons grandir les talents afin qu'ensemble, ils accompagnent les organisations vers une croissance pérenne. C'est ainsi que nous jouons un rôle actif dans la construction d'un monde plus juste et plus équilibré pour nos équipes, nos clients et la société dans son ensemble.

EY désigne l'organisation mondiale et peut faire référence à l'un ou plusieurs des membres d'Ernst & Young Global Limited, dont chacun est une entité juridique distincte. Ernst & Young Global Limited, société britannique à responsabilité limitée par garantie, ne fournit pas de prestations aux clients. Retrouvez plus d'informations sur notre organisation sur www.ey.com.

Studio EY France – 1802SG126
SCORE France N°2018-23
ED 042018

ey.com/fr