Communication de crise : une perspective utile pour la cybersécurité

CoRIIN 2018
Lille, France

Bonjour

*Je suis **Rayna Stamboliyska***

Consultante sécurité (gesrisques/gescrise) et gouvernance

Auteure *“La face cachée d’Internet”*

@MaliciaRogue

www.face-cachee-internet.fr


Mais pourquoi la crise ?
Boarf, une histoire de vie.

1

La gestion de crise

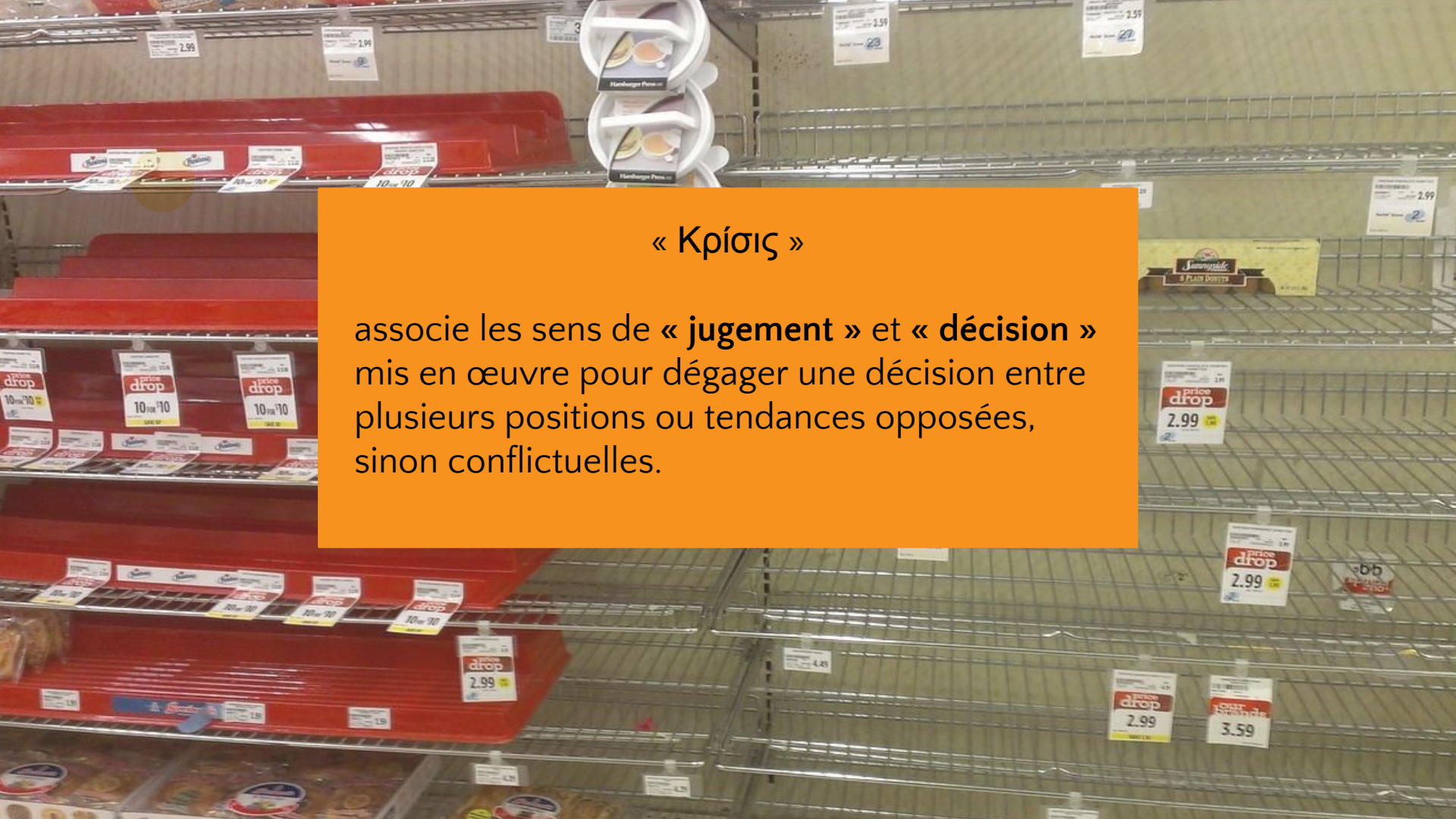
Parce que la comm’ est juste une partie du tout, en fait

La crise

Une période de tension conflictuelle ou une situation de déséquilibre grave ou de rupture préoccupante.

La décision stratégique

- L’environnement & les acteurs
- La situation & les évaluations possibles
- Les scénarios & la validation de pertinence
- La mise en œuvre & les adaptations
- La résolution des problèmes & le suivi
- L’analyse post-action & le RetEx



« Κρίσις »

associe les sens de **« jugement »** et **« décision »** mis en œuvre pour dégager une décision entre plusieurs positions ou tendances opposées, sinon conflictuelles.

Les crises aujourd’hui sont des crises mille-feuilles

(et ce n’est pas du gâteau…)

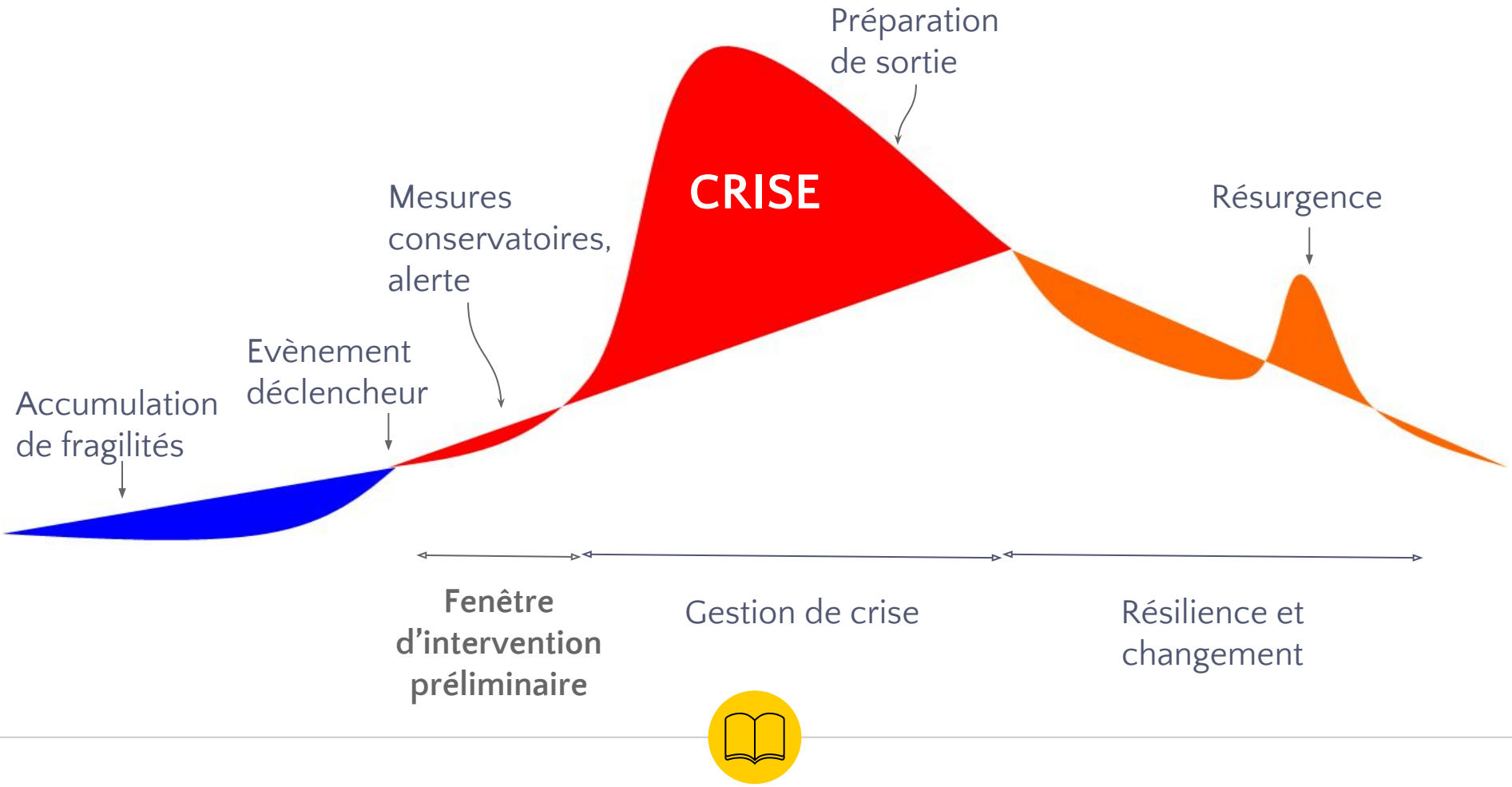
Autrement dit, it’s complicated

- Systèmes de + en + complexes –> fragiles
- Relais média & public demandeur
- Implication croissante de la justice
- Mouvements associatifs
- Réseaux sociaux & temps réel
- Lanceurs d’alerte

2

Comm != gestion

Oh fsck...


Préparation
de sortie
CRISE
Mesures
conservatoires,
alerte
Résurgence
Evènement
déclencheur
Accumulation
de fragilités
Fenêtre
d'intervention
préliminaire
Gestion de crise
Résilience et
changement

Les 5 fronts

L’organisation d’une entité en situation de crise

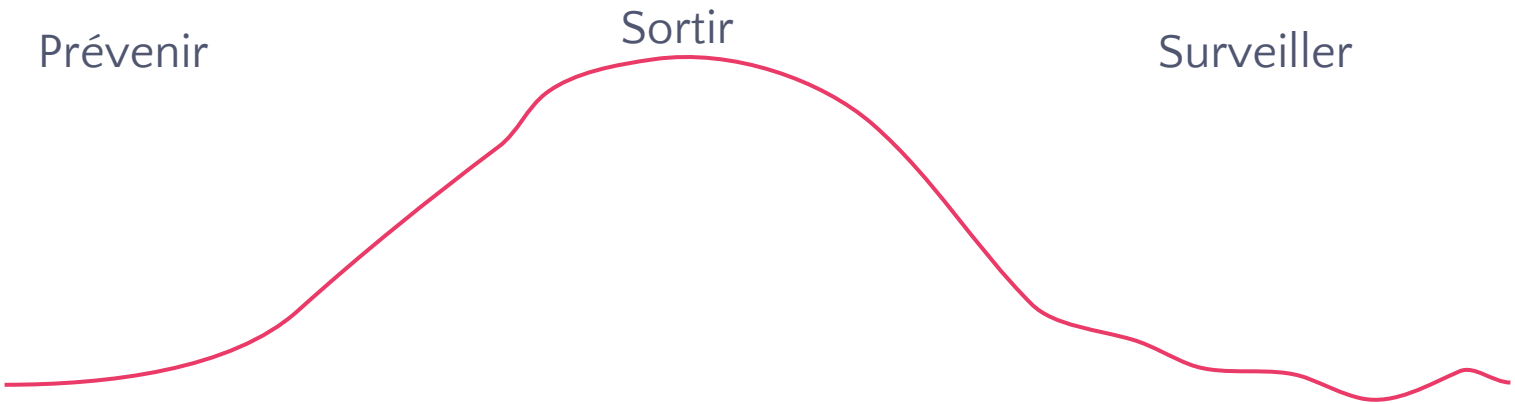
- Un évènement grave à combattre
- Des zones d’incertitude à réduire
- Des enjeux à maîtriser
- Des acteurs à prendre en compte
- Le temps à gérer

Le temps

“Les premières 6 heures sont cruciales et la sortie de crise en dépend”

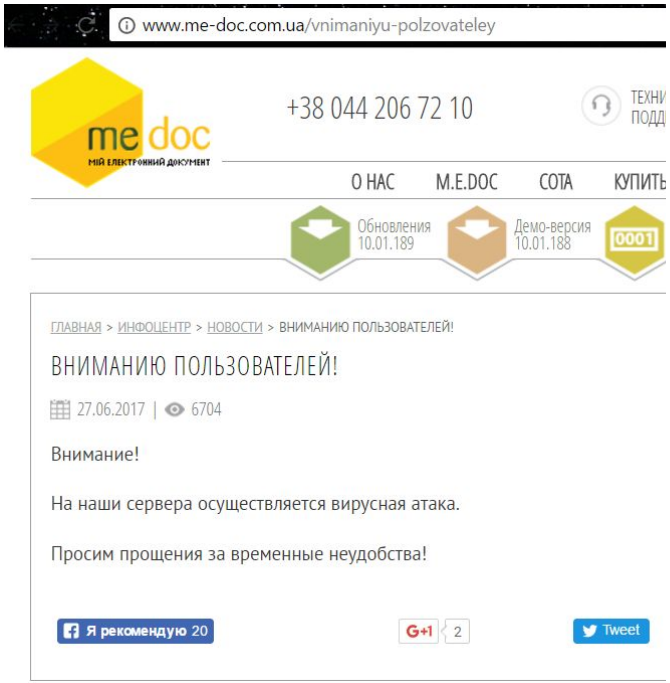
-> Est-ce toujours vrai pour les crises résultant d’un incident numérique ? (plutôt oui)

Les attitudes pendant



La communication, c’est l’ensemble des actions :

- planifiées
- mises en oeuvre
- coordonnées
- de tous les domaines
- poursuivant objectifs cohérents avec stratégie
- en temps contraint



La comm' de crise de MeDOC

Euh... non.

Légitimité et confiance

Agir sans sur-réagir

- Identifier ce que l'on protège
- Définir les objectifs de communication
- Mobiliser les messagers et les canaux
- Ciseler le message et assumer ses risques
- Arbitrer les silences

La communication = APT

1. J’ai connaissance

Je maîtrise le timing de déclenchement, les scénarii (“j’ai tiré les donc”).

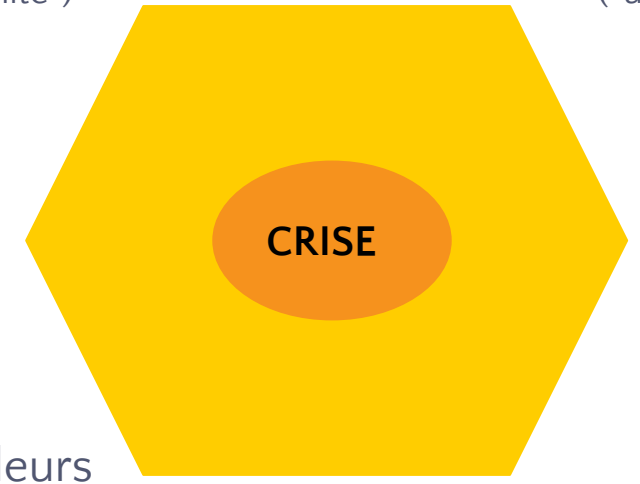
2. Surprise sur prise

Beh…

Les acteurs à qui parler

Les concurrents
(“une opportunité”)

Les victimes
(“un malheur”)



Les médias
(“un scoop”)

Les témoins
(“un spectacle”)

Les décideurs
(“un souci”)

Les salariés
(“un risque pour l’emploi”)

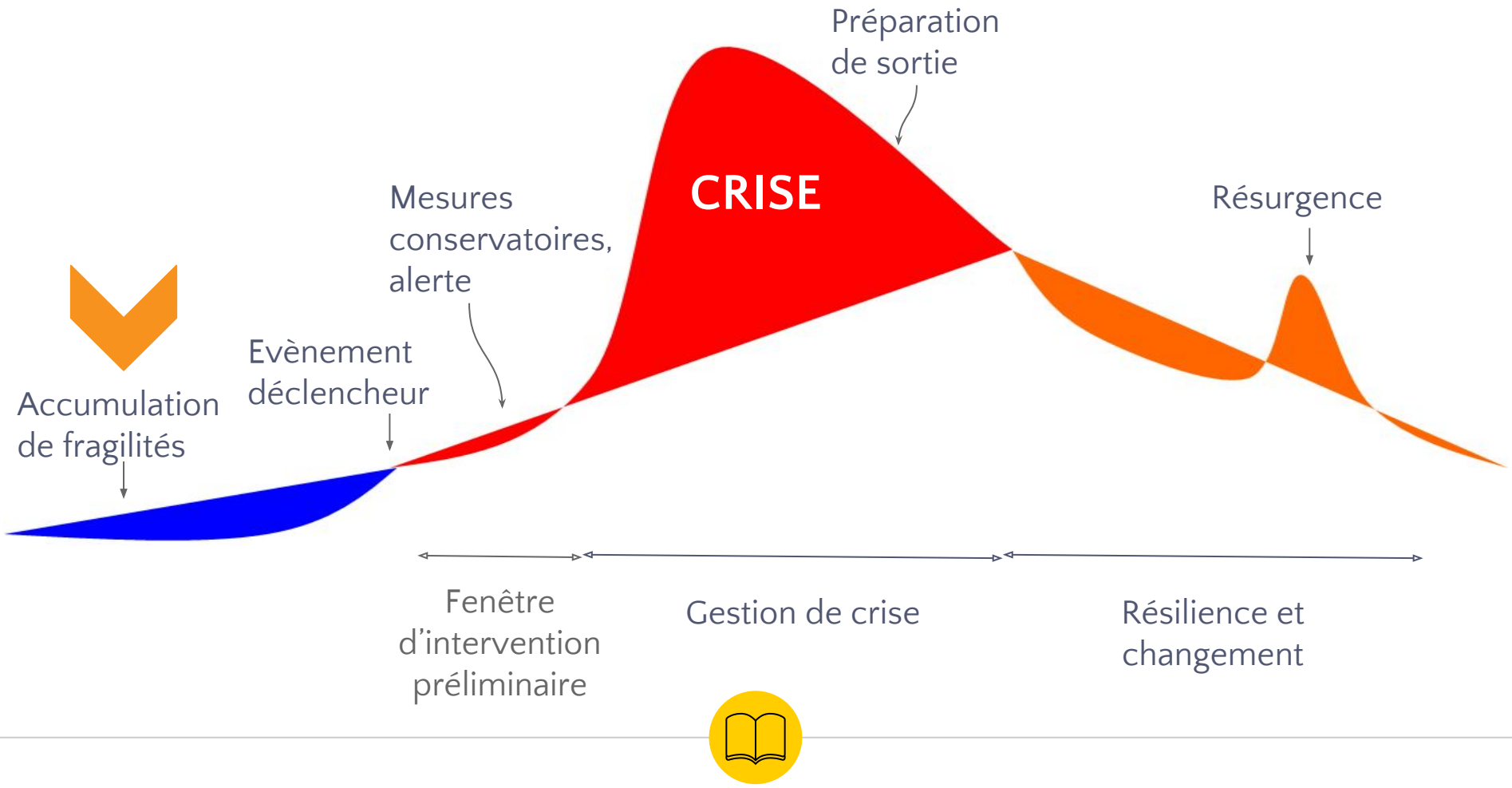
Acceptabilité et légitimité

La communication (de crise) n’est pas ce que je dis,
mais ce que tu entends.

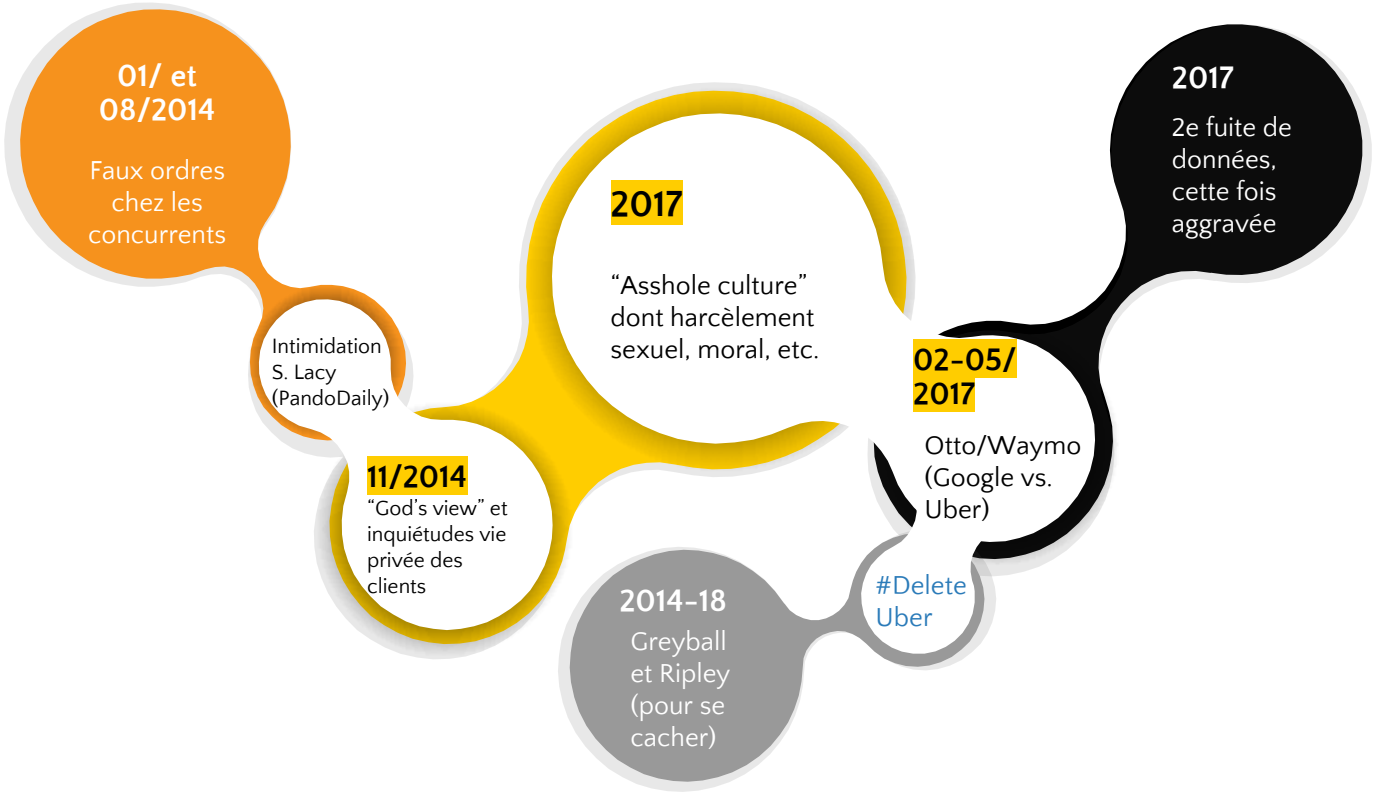
3

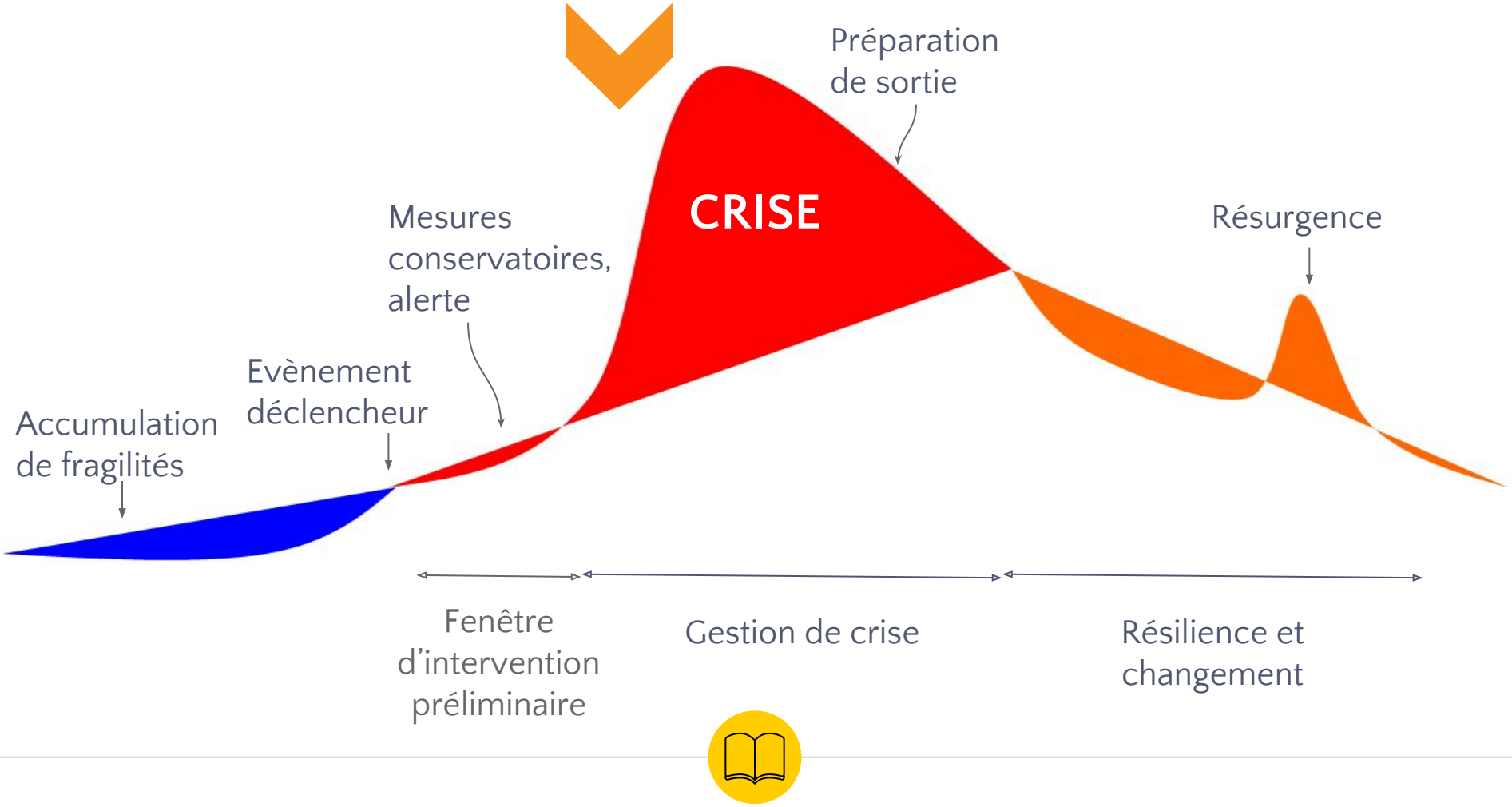
La comm crisogène

Hey Equifax, Deloitte, Uber,...


Préparation
de sortie
CRISE
Mesures
conservatoires,
alerte
Résurgence
Evènement
déclencheur
Accumulation
de fragilités
Fenêtre
d'intervention
préliminaire
Gestion de crise
Résilience et
changement

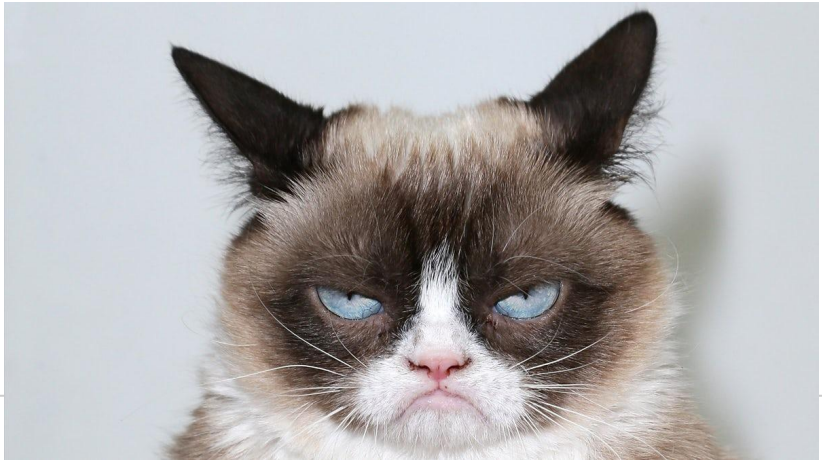
Les ennuis sont des pleutres




Préparation
de sortie
CRISE
Mesures
conservatoires,
alerte
Résurgence
Evènement
déclencheur
Accumulation
de fragilités
Fenêtre
d'intervention
préliminaire
Gestion de crise
Résilience et
changement

La comm’ de crise d’Equifax
Alégorie

Les cadres dirigeants d'Equifax sont *"désappointés"*et *"déçus"* de la compromission. Le PDG a rassuré : les *"bases principales de calcul de scoring de crédits"* n'ont pas été atteintes. *"Nous sommes désolés pour la frustration que cet accident cause à nos clients"*



Cybersecurity Incident & Important Consumer Information

Consumer Notice FAQs Potential Impact Enroll TrustedID Premier Contact Us

equifaxsecurity2017.com

Equifax Releases Details on Cybersecurity Incident, Announces Personnel Changes

September 15, 2017

ATLANTA — As part of the company's ongoing review of the cybersecurity incident announced September 7, 2017, Equifax Inc. (NYSE: EFX) today made personnel changes and released additional information regarding its preliminary findings about the incident.

The company announced that the Chief Information Officer and Chief Security Officer are retiring. Mark Rohrwasser has been appointed interim Chief Information Officer. Mr. Rohrwasser joined Equifax in 2016 and has led Equifax's International IT operations since that time. Russ Ayres has been appointed interim Chief Security

Recent Updates

Equifax Releases Details Cybersecurity Incident, A Personnel Changes
September 15, 2017

A Progress Update for Co
September 14, 2017

A Progress Update for Co
September 13, 2017

A Progress Update for Co
September 11, 2017

EQUIFAX Return to equifax.com

To enroll in complimentary identity theft protection and credit file monitoring, click here.

Cybersecurity Incident & Important Consumer Information Which is Totally Fake, Why Did Equifax Use A Domain That's So Easily Impersonated By Phishing Sites?

Consumer Notice FAQs Potential Impact Enroll TrustedID Premier Contact Us

Equifax Announces Cybersecurity Incident Involving Consumer Information, Because of Incompetence

Equifax should have hosted this on equifax.com with a reputable [EV] SSL Certificate.

Instead they chose an easily impersonated domain and used a jelly-bean SSL cert that any script kiddie can impersonate in 20min.

Their response to this incident leaves millions vulnerable to phishing attacks on copycat sites.

This is why you don't put your security incident website on a domain that looks like a scam (with an Amazon SSL cert), no-one can tell the difference between the real thing an a phishing site. Try the form by clicking "Potential Impact"

securityequifax2017.com

Tweet @equifax to get them to change it to equifax.com before thousands of people lose their info to phishing sites!

Comm officielle pendant 2 semaines :

Equifax Inc.
@Equifax

Follow

Replying to @eqloprtntyhtr

Hi! For more information about the product and enrollment, please visit: securityequifax2017.com. -Tim

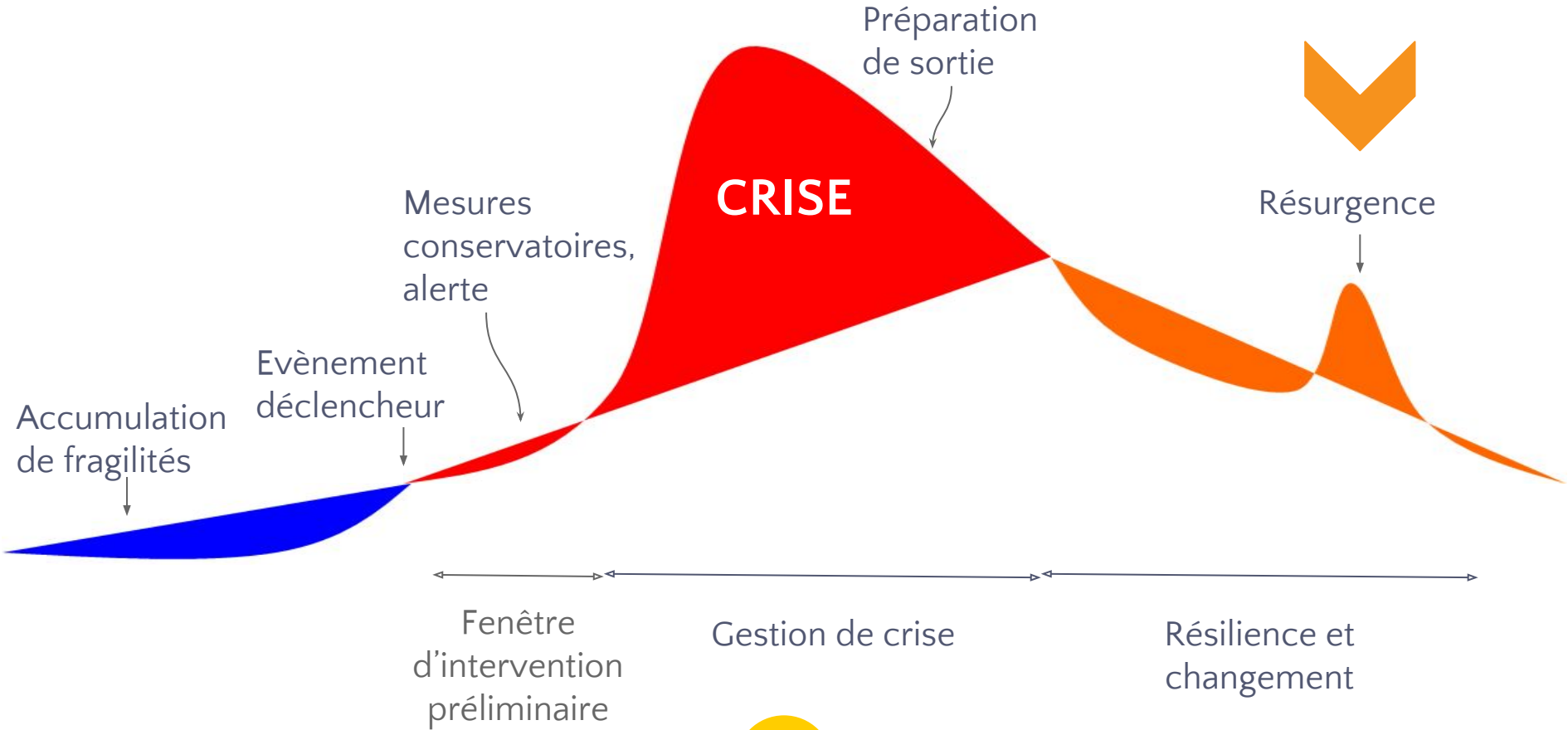
3:11 PM - 19 Sep 2017

5 Retweets **12** Likes

8 5 12

Source

- Gel du dossier payant
- TrustedID est un produit Equifax
- Les CGU interdisent toute poursuite judiciaire
- 200k numéros CB stockés en clair fuités
- Warning à l’escroquerie par le gouvernement


Préparation
de sortie
CRISE
Mesures
conservatoires,
alerte
Résurgence
Evènement
déclencheur
Accumulation
de fragilités
Fenêtre
d'intervention
préliminaire
Gestion de crise
Résilience et
changement

Lawmakers want credit reporting agencies to pay potentially billions in fines if their data gets stolen and for victims of the breach get a big chunk of the money.

Introduced on Wednesday by Sens. Elizabeth Warren, D-Mass., and Mark Warner, D-Va., the Data Breach Prevention and Compensation Act would raise the security requirements for data stored at credit agencies and give the organizations more to lose when that information gets stolen. It's the third piece of legislation aimed at tightening the leash on credit reporting agencies in the wake of the 2017 Equifax data breach.

"Equifax allowed personal data on more than half the adults in the country to get stolen, and its legal liability is so limited that it may end up making money off the breach," Warren said in a statement. "This bill will ensure that companies like Equifax ... are taking appropriate steps to secure data that's central to Americans' identity management and access to credit."

The 'Equifax Law'

Non, vous ne souhaitez pas que votre société reste connue comme la boîte qui a vraiment gaffé. Et attention à la résurgence...

Source

Del_H @MatthieuDelach

« Nous avons affaire à la crème de la crème de la #cyberattaque. C'est du jamais vu. Une enquête est toujours en cours », confie Michael Bittan, responsable des activités cybersécurité Deloitte France, à propos de l'attaque informatique révélée en septembre 2017 par le @guardian

15:53 · 18 janv. 18

1 Retweet 2 J'aime

Del_H @MatthieuDelach · 3j

« Ce type d'attaque informatique nécessite une expertise technique très pointue et des moyens financiers colossaux. Nous avons pu reconstituer le scénario. Nous allons pouvoir mettre à profit cette expertise pour améliorer la sécurité de nos clients », précise-t-il.

1

¯_(ツ)_/¯

```
#rdps for flux

//asundhar
10.26.131.101
User Name : USDEVasundhar
Password : [redacted]

//mrazak
10.26.216.61
USDEVmorazak
Password : [redacted]

//vpn credentails for deloitte

https://aexternal.deloittenet.deloitte.com/my.policy#
sipatra
[redacted]

//flux database info
10.25.112.22; Database=Flux; User Id=Flux_User; Password=[redacted]

#test server web site flux
https://ddisclosureanalytics.deloitte.com/flux/uploadtb
usdevleeldridge
[redacted]

#other flux info
//tfs
http://tfs.deloitte.com:8080/tfs/its/FluxAnalysis/FluxAnal
dhamb
[redacted]

//build forge
http://buildforge.deloitte.com:8080/jas/LoginServlet;jsess
UserName : asundhar
Password: [redacted]

//project portfolio management
https://ppm.deloitte.com/itg/web/knta/crt/RequestDetail.js
```

VPN credentials sur GitHub public

Hernan Moreno ▸ Deloitte 38w

proxy-
proxy.corp.globant.com
puerto
3128

[redacted]

BIG-IP logout page
aexternal.deloittenet.deloitte.com

+1

Login proxy sur G+ public

137	udp	netbios

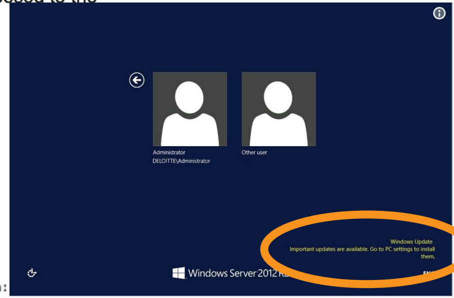
```
NetBIOS Response
Servername: PRDTAXDDNS01
MAC: 00:50:56:b4:5e:da

Names:
WORKGROUP       <0x0>
PRDTAXDDNS01    <0x0>
PRDTAXDDNS01    <0x20>
```

Dᵈăᵃńʲ ᴺŤᵗėᵉňᴺťʲ ĺᴸėᵉŕʳ @Viss

Hey look, a deloitte server with 445 exposed to the internet shodan.io/host/199.38.21… production tax dns server
what could possibly go wrong?

8:00 PM - Sep 25, 2017



3389	tcp	rdp

```
Remote Desktop Protocol
\x03\x00\x00\x0b\x06\xd0\x00\x00\x124\x00

SSL Certificate
Certificate:
    Data:
        Version: 3 (0x2)
        Serial Number:
            17:02:6b:b1:d2:88:38:a2:4a:79:68:1a:99:7a:
    Signature Algorithm: sha1WithRSAEncryption
        Issuer: CN=Deloitte-AD-02.Deloitte.local
        Validity
            Not Before: May 18 10:35:01 2017 GM
            Not After : Nov 17 10:35:01 2017 GM
        Subject: CN=Deloitte-AD-02.Deloitte.loc
        Subject Public Key Info:
            Public Key Algorithm: rsaEncryption
                Public-Key: (2048 bit)
                Modulus:
```

Dᵈăᵃńʲ ᴺŤᵗėᵉňᴺťʲ ĺᴸėᵉŕʳ @Viss

'a;sljfasdfjadjaserfaweakjwtgfaehasrhfasd;laksfkasroha as;faskdga'seraowhjasjdfasdlfasgajhsdfjarfhoae;ahd

11:04 PM - Sep 25, 2017

64 258 519

Dᵈăᵃńʲ ᴺŤᵗėᵉňᴺťʲ ĺᴸėᵉŕʳ

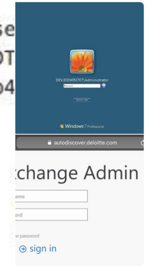
Kevin Beaumont @GossiTheDog

Suivre

Deloittes' US offices have everything from Netbios to RDP to Exchange Admin (single factor) etc etc etc. They should get an auditor.

```
NetBIOS Response
Servername: PRDT
MAC: 00:50:56:b4

Names:
WORKGROUP
PRDTAXDDNS01
PRDTAXDDNS01
```

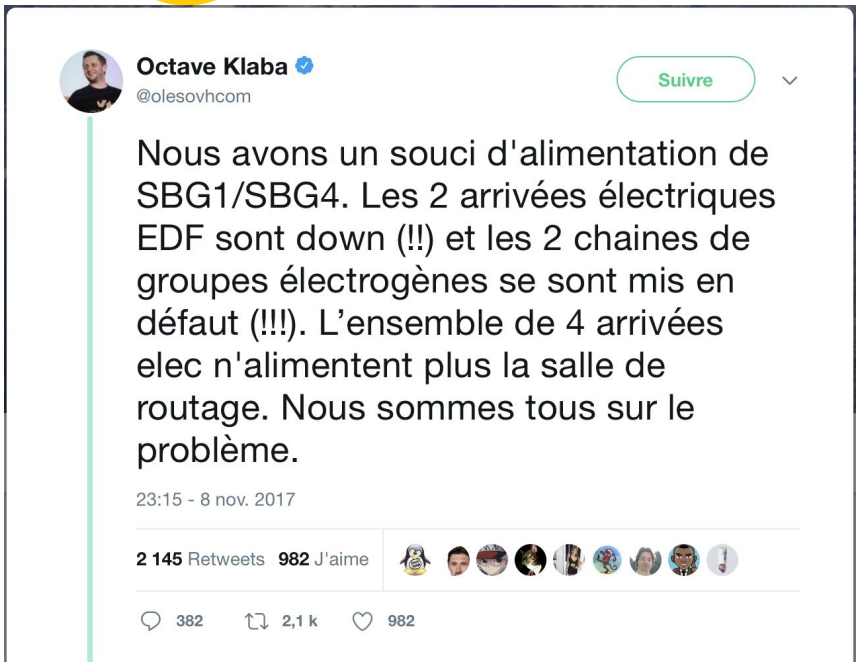


13:02 - 25 sept. 2017

4

Peut mieux faire

Hey OVH, Disqus, Online !



Source

Communication #OVHgate

Les + Transparence, suivi de l'incident, canaux adéquats, gestion de l'émotion, post-mortem public

Les – Messages mal adaptés à la majorité des clients, légitimité parfois chancelante

Approche globale

Prévention + réaction + exploitation

Objectifs cohérents

Communication + choix + décisions

Sortir par le haut

Méthode + entraînement + sang froid

Merci !

Des questions ?

Je trolle, donc je suis :

- @MaliciaRogue
- www.face-cachee-internet.fr