

# LA PREVENTION & L'IDENTIFICATION DES RISQUES

## COMMENT SE PROTÉGER EN AMONT D'UNE CYBER-ATTAQUE ?

**Christophe Bianco, Managing Partner, Excellium Services S.A**  
**Guillaume Del Pizzo, Client Executive, Marsh**

# Vos Intervenants



Your first call when it comes to IT and security



**Christophe Bianco**

Managing Partner  
Excellium Services

+352 661 154 538

[cbianco@excellium-services.com](mailto:cbianco@excellium-services.com)



**Guillaume DEL PIZZO**

Client Executive,  
Marsh S.A.

+352 49 52 38 26 (office) |

+352 621 139 946 | (mobile)

[guillaume.delpizzo@marsh.com](mailto:guillaume.delpizzo@marsh.com)

# Qu'est ce qu'une cyber attaque?

Accueil > Économie > Entreprises

# Après une cyberattaque, Lise Charmel se place en redressement judiciaire

L'entreprise, qui a refusé de payer une rançon aux pirates, a perdu plusieurs millions d'euros.

Par **Cécile Crouzel**

Publié hier à 08:55, mis à jour hier à 08:55



LISE CHARMEL

# Une économie florissante?

Abonnés Faits divers

# Surdoués, immatures et flambeurs... ces hackers français ont réussi le cybercasse du siècle

La justice française enquête sur un groupe de jeunes hackers responsables d'un incroyable cyberbraquage à plus de 8 millions d'euros. Ces prodiges de l'informatique, qui ont dépensé leur butin en voitures de luxe, n'en sont pas à leur premier coup d'essai.



MARSH

Les quatre jeunes pirates français sont mis en examen depuis six mois après leur attaque de la plate-forme mondiale de cryptomonnaie GateHub. Clod

An advertisement for Le Parisien. It features a large, detailed illustration of a sea turtle swimming in the ocean. The text is overlaid on the image. At the top, the 'Le Parisien' logo is in a blue box. Below it, the text 'Initiatives environnement' is in a smaller font. The main headline reads 'Comment mieux gérer nos ressources' in large, bold, white letters. Below this, in smaller white letters, is 'EAU, RECYCLAGE, ÉNERGIE...'. At the bottom, there is a white button with the text 'CLIQUEZ ICI'. Below the button, it says 'EN PARTENARIAT AVEC' followed by the Suez logo and the word 'suez' in a stylized font.



# La Cyber criminalité est un business

Chantage à la rançon

Chantage aux données

Vente aux enchères



	<p><b>Bronze Edition</b></p> <ul style="list-style-type: none"> <li>This product is the improved version of Turkojan 3.0 and it has some limitations(Webcam - audio streaming and msn sniffer doesn't work for this version)</li> <li>1 month replacement warranty if it gets detected by any antivirus</li> <li>7/24 online support via e-mail</li> <li>Supports only Windows 95/98/ME/NT/2000/XP</li> <li>Realtime Screen viewing(controlling is disabled)</li> </ul> <p><b>Price : 99\$ (United State Dollar)</b></p>
	<p><b>Silver Edition</b></p> <ul style="list-style-type: none"> <li>4 months (maximum 3 times) replacement warranty if it gets detected by any antivirus</li> <li>7/24 online support via e-mail and instant messengers</li> <li>Supports 95/98/ME/NT/2000/XP/Vista</li> <li>Webcam streaming is available with this version</li> <li>Realtime Screen viewing(controlling is disabled)</li> <li>Notifies changements on clipboard and save them</li> </ul> <p><b>Price : 179\$ (United State Dollar)</b></p>
	<p><b>Gold Edition</b></p> <ul style="list-style-type: none"> <li>6 months (unlimited) or 9 months(maximum 3 times) replacement warranty if it gets detected by any antivirus (you can choose 6 months or 9 months)</li> <li>7/24 online support via e-mail and instant messengers</li> <li>Supports Windows 95/98/ME/NT/2000/2003/XP/Vista</li> <li>Remote Shell (Managing with Ms-Dos Commands)</li> <li>Webcam - audio streaming and msn sniffer</li> <li>Controlling remote computer via keyboard and mouse</li> <li>Notifies changements on clipboard and save them</li> <li>Technical support after installing software</li> <li>Viewing pictures without any download(Thumbnail Viewer)</li> </ul>

Vente de logiciel malveillant

Offre d'emploi pour une mule

## Job

### Regional Financial Representative

This is a part-time job position, you will be required to be available 1-2 hours a day. The purpose of this position is to be a part of company internal operational cash flow and deal with the local customer payments in particular. You will specifically be responsible to:

#### Duties and Responsibilities:

- Coordinate customer payments using your bank account
- Monitor payment delivery thoroughly
- Immediately notify when any payment arrives and inform company head office
- Process customer payments via Western Union and Money Gram services to the company regional warehouses
- Ensure each customer payment is dealt with in a quick, polite and efficient manner
- Make records on each new coming customer payment into a database
- Establish and maintain constructive working environment, so that to ensure high-speed payment delivery, provide the customers with the fastest possible service and attract extra customers.

#### Skills and requirements:

- Must be at least 18 years of age
- Proficient in Microsoft PC skills (Windows), etc. is a plus
- Excellent communication, organizational and interpersonal skills
- Attention to details and accuracy
- Ability to make decisions and resolve issues.
- Ability to demonstrate care & concern for customers
- Able to maintain composure during stressful situations
- Accepts direction from supervisors regarding various components of the tasks

This position reports to a supervisor or manager. You will be paid net 10% commission out of every customer payment you have to deal with, all the related expenses will be covered by the company.



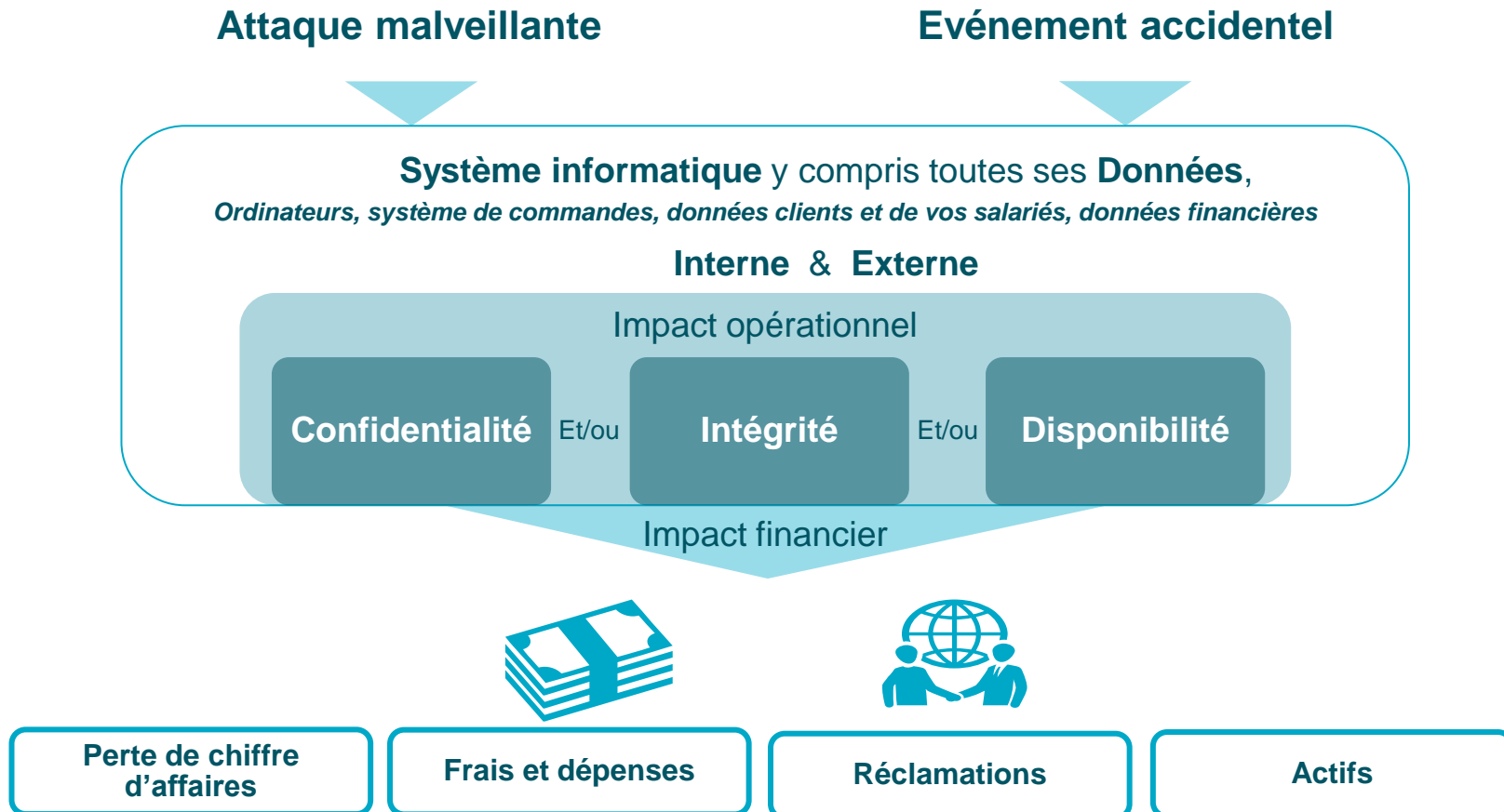
# L'enjeu – L'humain ....?

## MARSH

<https://www.leparisien.fr/economie/campagne-anti-phishing-orange-enseigne-la-mefiance-02-07-2019-8107623.php>

# Quelles sont les conséquences d'une cyber attaque?

# Les impacts

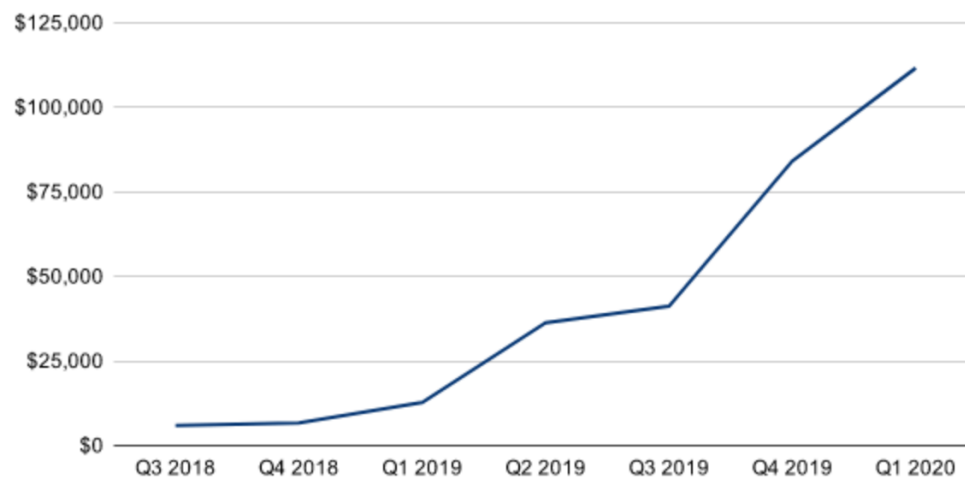


# Payer la rançon?

# Personne ne paye ....

## Average Ransom Payment by Quarter

Amounts are in USD



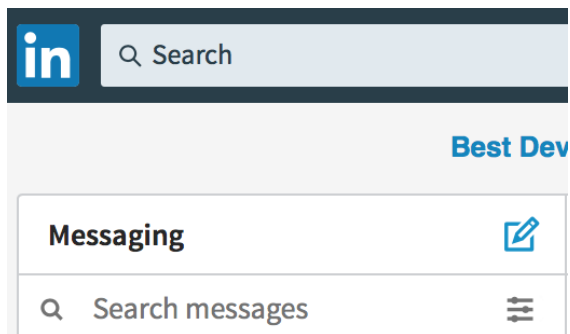
The average ransom payments made to ransomware attackers by quarter (Source: Coveware)



# **Comment les entreprises réagissent à une cyber attaque?**



# A priori pas toujours bien ...



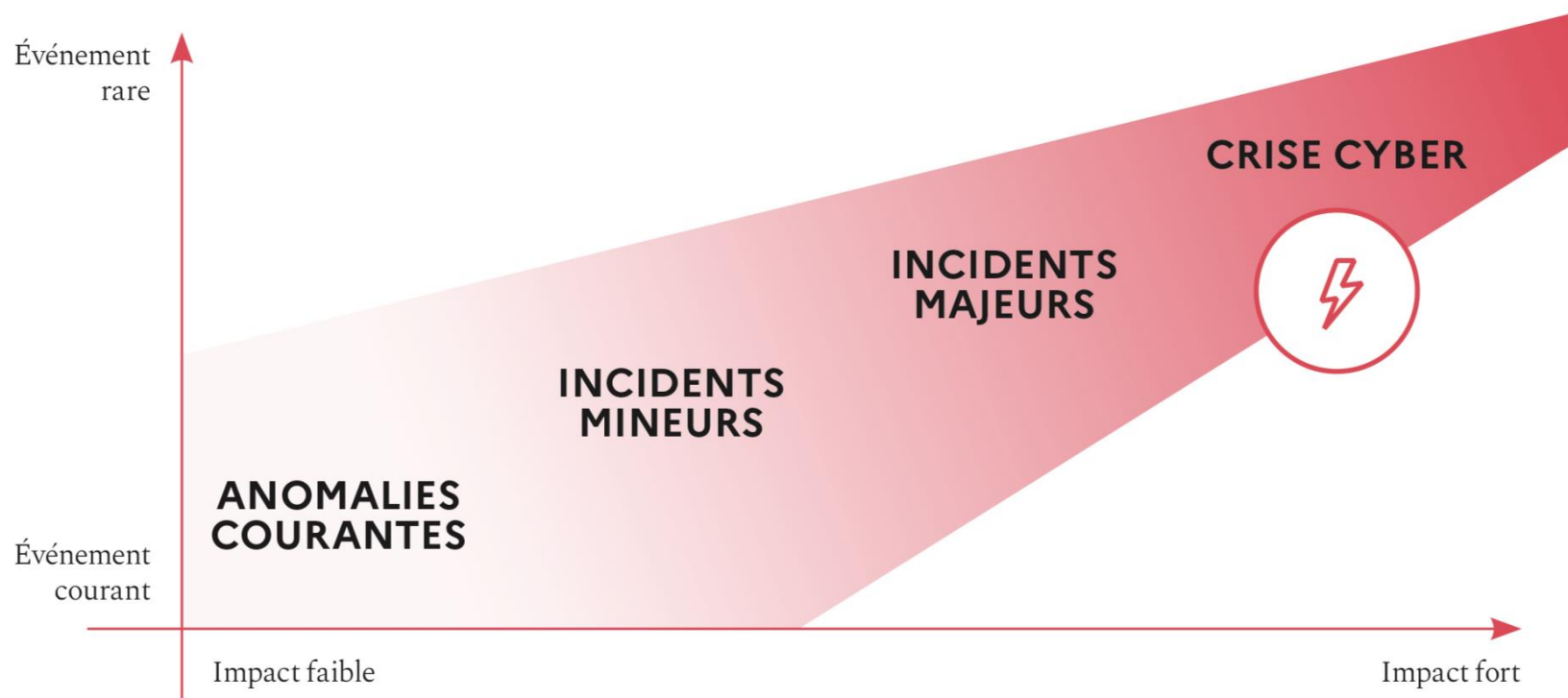
Aug 24

## Contact

Bonsoir

Pourriez vous me communiquer votre numero au cas où nous aurions besoin d excellium en toute urgence. Je contacte sur votre discrétion.

# Tout n'est pas un cyber incident !



Source ANSSI 2020

# Les constats et premières recommandations

## **Votre informatique est non opérationnelle**

- La première des choses est d'activer les mesures d'urgences et le support
- Après une attaque les systèmes ne peuvent plus être utilisés normalement
- Une perte de confiance dans le système d'information existe

## **Vous devez contenir l'attaque lorsqu'elle survient**

- Identifiez les contacts utiles
- Définissez les processus qui permettent de prendre de rapides décisions
- Stoppez l' »hémorragie », le temps joue en votre défaveur

## **Il faut se préparer à travailler sans IT**

- Pouvez vous travailler manuellement?
- Pouvez vous interrompre votre activité de manière contrôlée?
- Quelles sont les données dont vous avez besoins?
- Quels outils alternatifs avez-vous besoin?

## **Il va falloir reconstruire l'IT**

- Reconstruire doit être priorisé en fonction des besoins métiers
- Simplifiez et segmentez vos architectures pour de rapides reconstructions (oubliez les modifications historiques)

# Les équipes pour piloter la résolution de la crise



**12**  
personnes en  
moyenne

**440**  
personnes au  
maximum

Dont  
**25%**  
de prestataires  
en moyenne

## Combien de temps pour un retour à une **situation technique normale** ?



**1 semaine**

Pour un ransomware « simple » (i.e. sans propagation)



**3,5 semaines**

Pour une attaque ou un ransomworm ayant détruit une partie importante du système d'information



**Et au moins 6 semaines pour une reconstruction saine, avec deux actions clés :**

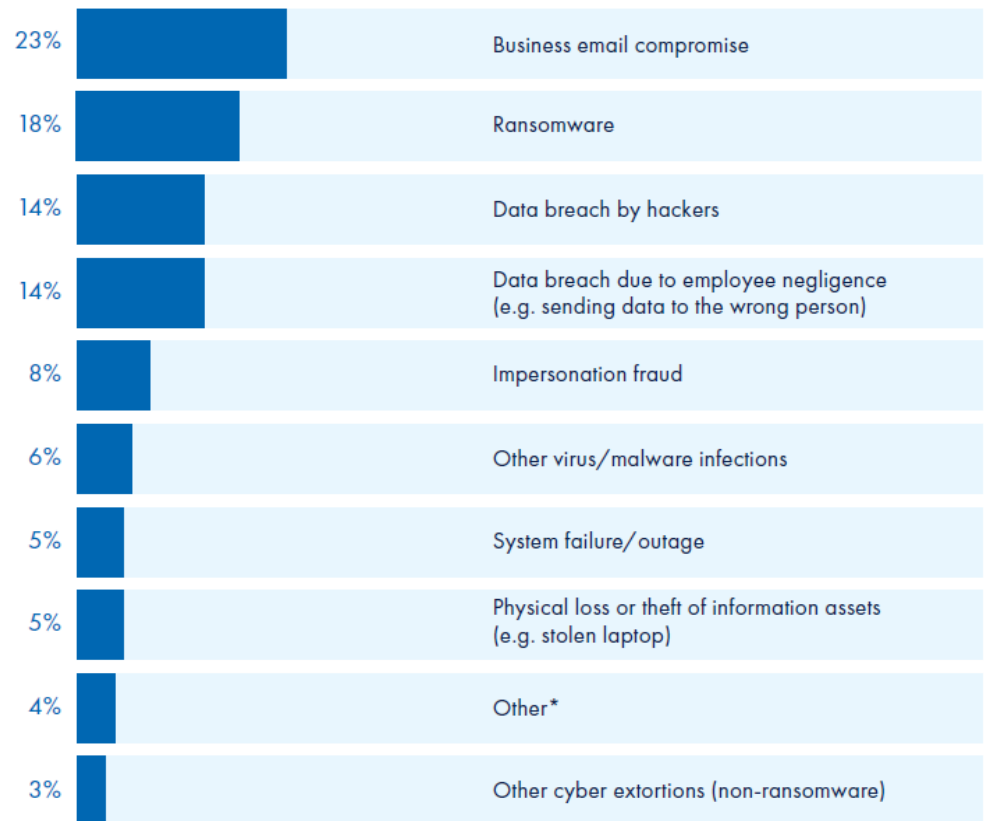
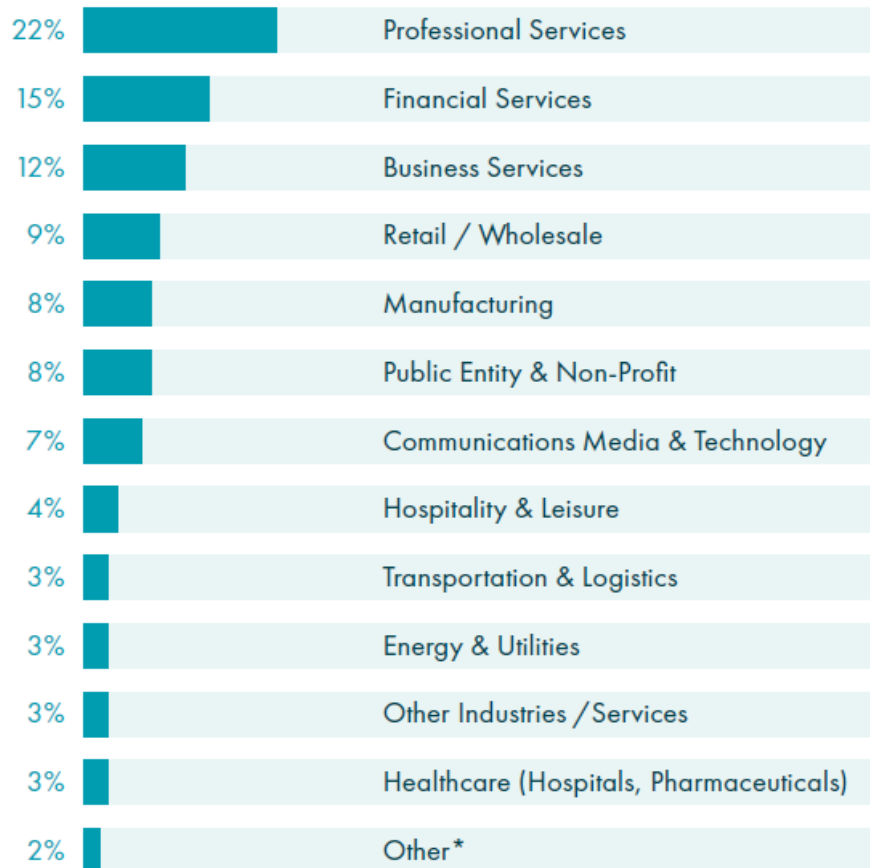
Reconstruction du cœur de confiance du SI pour bascule vers un nouvel environnement sain sur un week-end  
Nettoyage et réimportation des données métiers créées pendant la crise

<https://www.wavestone.com/app/uploads/2019/10/2019-Security-incident-response-benchmark-Wavestone.pdf>

**Du côté des assureurs que  
constate t-on?**

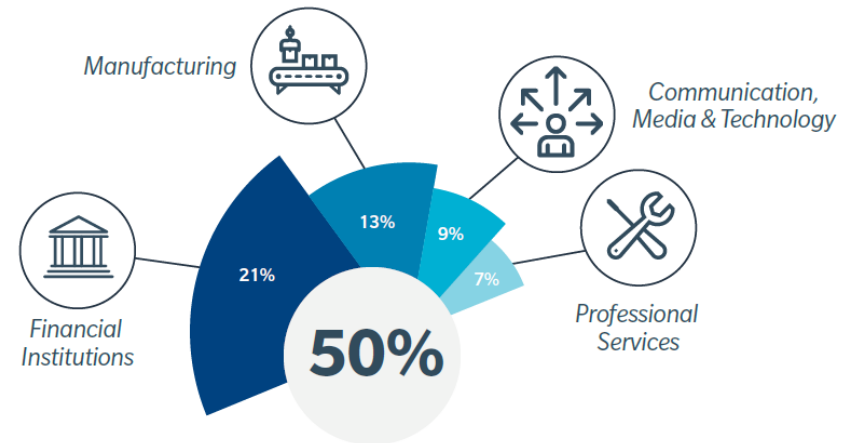
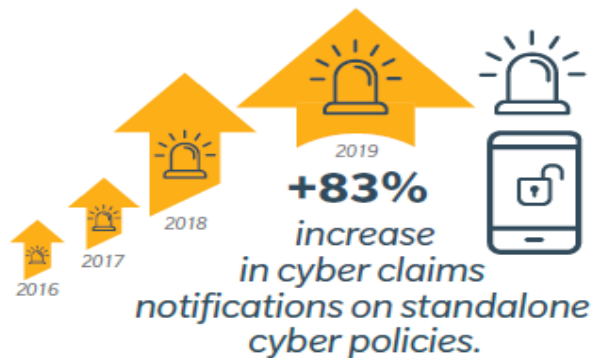
# Cyber Claims - EMEA 2018

## By Industry / Reported incidents

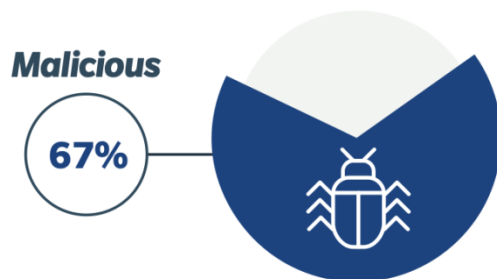


\*Denial of Service Attacks, Legal/Regulatory Proceedings based on violations of data privacy regulations

# D'après les incidents déclarés aux assureurs



Source: Marsh.



Based on all cyber claims that Marsh analysed, 67% of attacks were malicious and just 28% accidental.



**RANSOMWARE N°1  
2019**

**+100% à 500%**

JULY 2020

## The Changing Face of Cyber Claims



# Quelles sont les motivations des malveillants?

# Quelle est la menace / Motivation?

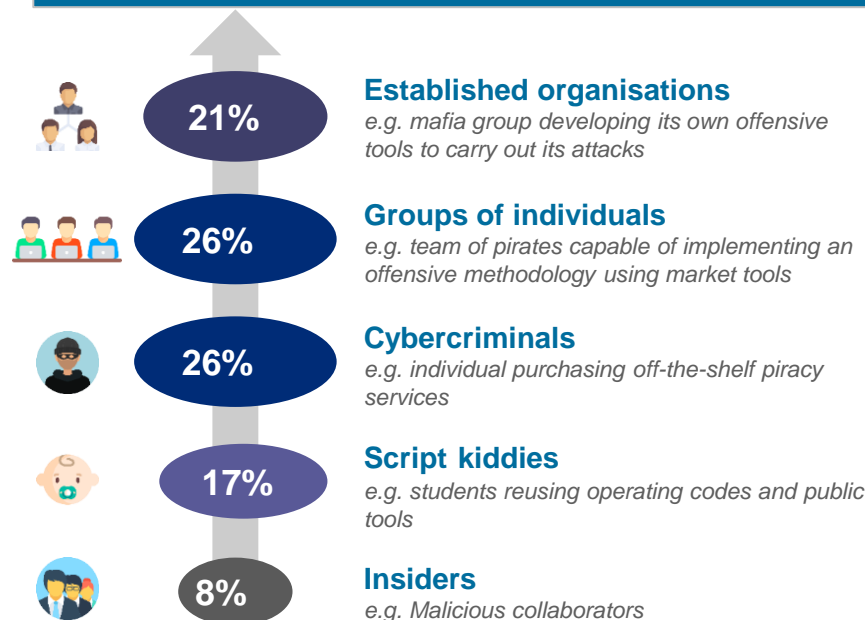
## What types of threat?

**65 % opportunistic threats:** often not highly technical; do not target a particular organisation, so if one is more secure than another, attackers will move to throw themselves onto the easiest prey.

**30 % targeted threats:** targets sensitive and precise information in the organisation. The attackers are mandated with a clear objective. They ensure all means are available to achieve their goals.

**5 % diffuse threats:** corresponds to the usual virus infections or spam; does not target a particular organisation and has a limited effect on the IS: denial of service, loss of user data....

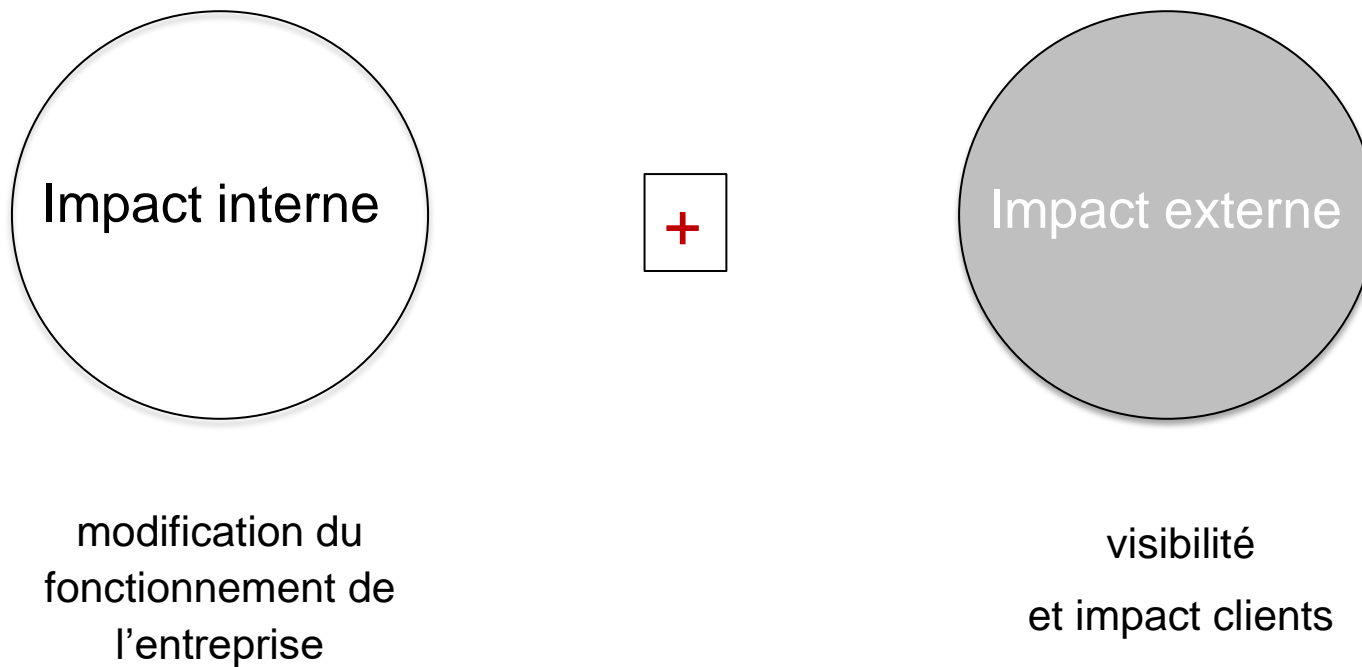
## Which attacker profiles?



Source Marsh

# Comment s'y préparer?

# Une crise Cyber c'est quoi?



# Pour préparer la crise!

## 1. Analyse des risques

- ☐ Le contexte
- ☐ Typologie et cartographie des risques
- ☐ Analyse des risques et recommandations
- ☐ Principales cibles de la communication

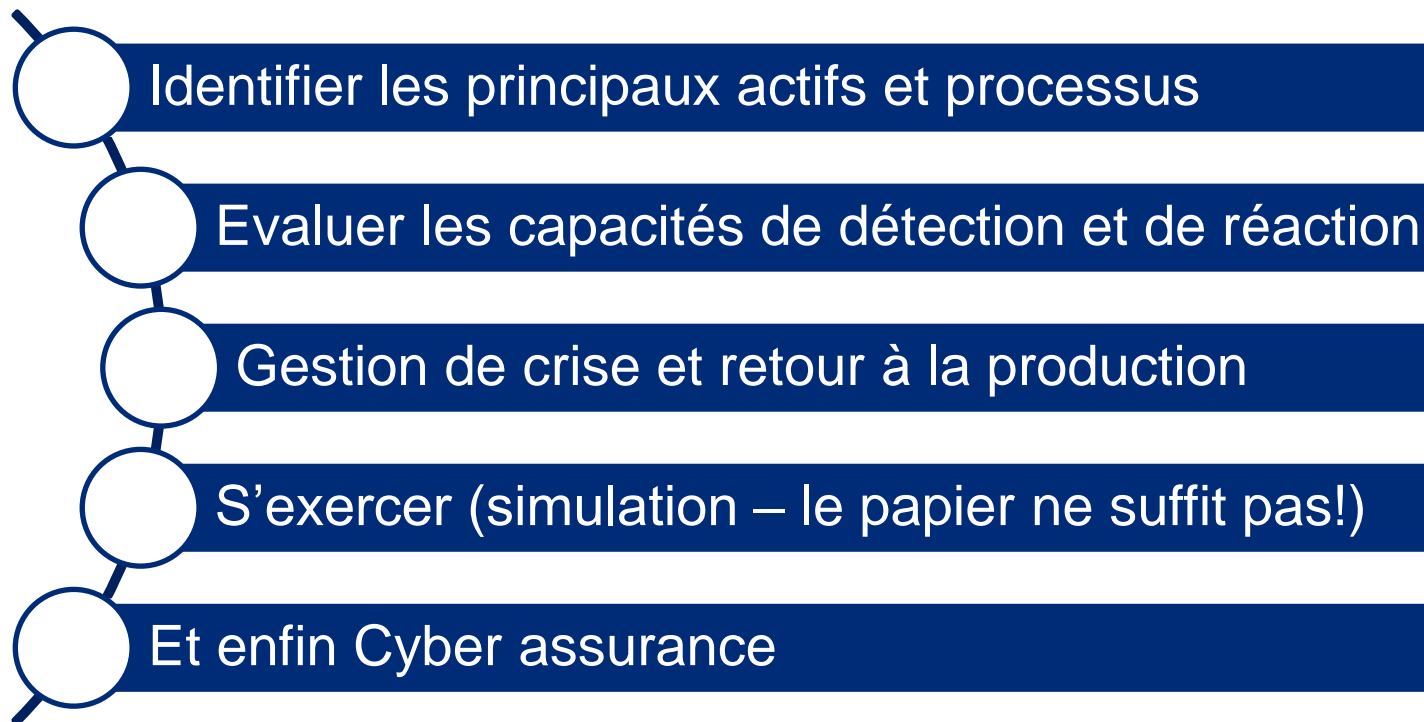
## 2. Manuel de crise

- ☐ Définition de la crise
- ☐ Composition de la cellule de crise
- ☐ Chaîne de l'information et procédures
- ☐ Protocoles de crise et messages-clé

## 3. Indispensables

- ☐ Contacts utiles
- ☐ Quelques règles pour bien communiquer

# La preparation à un cyber Incident



**Sans préparation, ne vous attendez pas à pouvoir vous en sortir !**

# **La cyber Assurance pourquoi?**



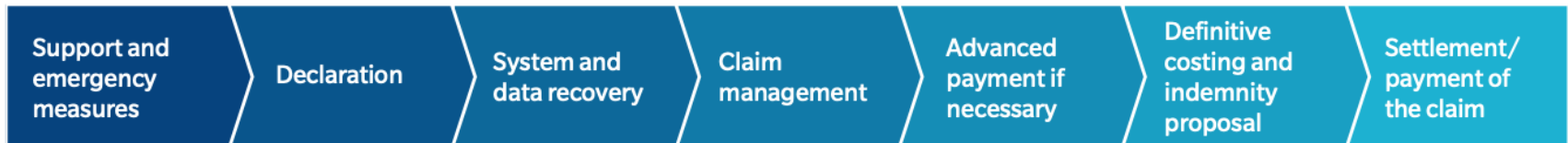
# Gestion de l'incident

## Incident and claims management steps

### Phases after a cyber incident



### Disruption of IT system



# Don't Be Worry, cela n'arrive qu'aux autres.

## #CyberRisksVsReality

« Mon 1er conseil : assurez-vous »

« Le premier conseil que j'aurais à donner : assurez-vous. Cela nous a énormément aidés. » Pour le dirigeant d'Altran, le fait d'avoir une assurance pour couvrir une partie des dégâts a certainement aidé à rassurer les actionnaires et la direction.

« attendez-vous à être attaqués. L'important ce n'est pas d'empêcher les attaquants d'entrer, c'est d'être capable de les détecter à temps et de rendre l'opération coûteuse pour eux »

Dominique Cerutti, PDG d'Altran

<https://www.zdnet.fr/actualites/ransomware-dominique-cerutti-pdg-d-altran-mon-1er-conseil-assurez-vous-39895949.htm>

# Rappelez vous!

La folie, c'est de  
refaire toujours  
la même chose,  
et s'attendre à ce  
que les résultats  
soient différents.

Albert Einstein



<https://www.ssi.gouv.fr/guide/guide-dhygiene-informatique/>

# Merci!

**EXCELLIUM**

Your first call when it comes to IT and security

 **MARSH**



**Christophe Bianco**  
Managing Partner  
Excellium Services  
+352 661 154 538  
[cbianco@excellium-services.com](mailto:cbianco@excellium-services.com)



**Guillaume DEL PIZZO**  
Client Executive,  
Marsh S.A.  
+352 49 52 38 26 (office) |  
+352 621 139 946 | (mobile)  
[guillaume.delpizzo@marsh.com](mailto:guillaume.delpizzo@marsh.com)