CCI CÔTE-D'OR Dijon Métropole

DIJON métropole

Groupe des acteurs de la Cybersécurité en Côte d'Or

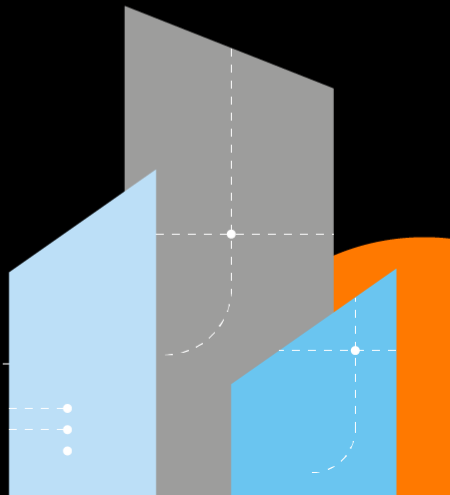
Orange Cyberdefense

SECUREware

Gestion de Crise Cyber

Comment anticiper une attaque et se préparer à la gestion de crise ?

Webinaire Cybersécurité
30 juin 2021

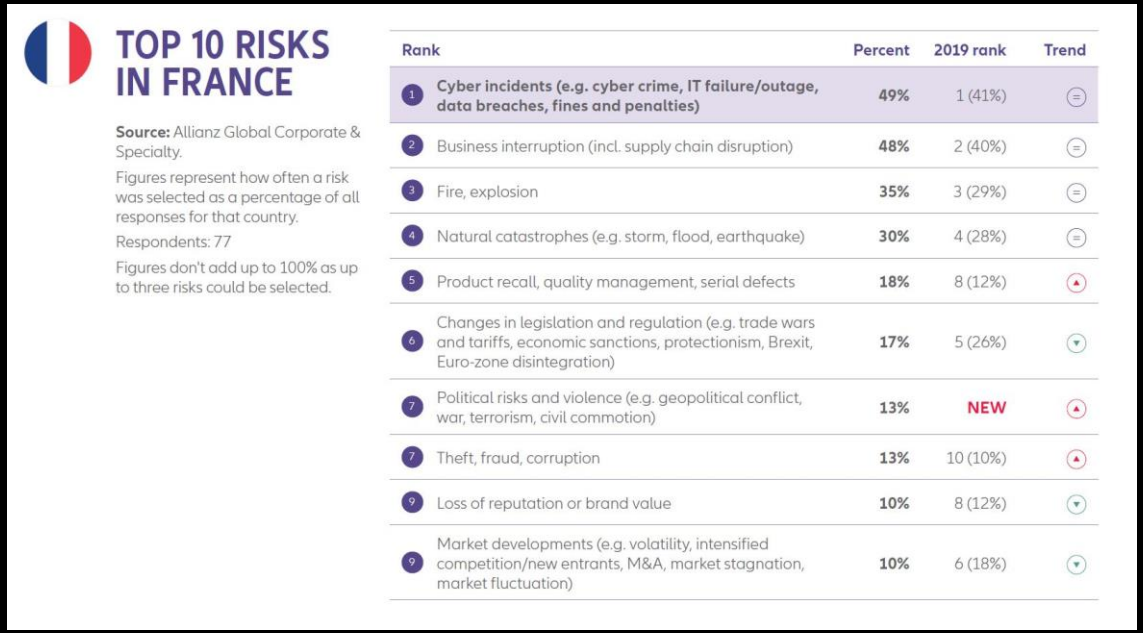


Nos intervenants

Frédéric DANIEL
Consultant Manager
Conseil et Audit
Orange Cyberdefense

Gilles LERAT
CEO
Fondateur
SECUREWARE

Le risque Cyber



TOP 10 RISKS IN FRANCE

Source: Allianz Global Corporate & Specialty.

Figures represent how often a risk was selected as a percentage of all responses for that country.

Respondents: 77

Figures don't add up to 100% as up to three risks could be selected.

Rank		Percent	2019 rank	Trend
1	**Cyber incidents (e.g. cyber crime, IT failure/outage, data breaches, fines and penalties)**	**49%**	1 (41%)	=
2	Business interruption (incl. supply chain disruption)	**48%**	2 (40%)	=
3	Fire, explosion	**35%**	3 (29%)	=
4	Natural catastrophes (e.g. storm, flood, earthquake)	**30%**	4 (28%)	=
5	Product recall, quality management, serial defects	**18%**	8 (12%)	▲
6	Changes in legislation and regulation (e.g. trade wars and tariffs, economic sanctions, protectionism, Brexit, Euro-zone disintegration)	**17%**	5 (26%)	▼
7	Political risks and violence (e.g. geopolitical conflict, war, terrorism, civil commotion)	**13%**	NEW	▲
7	Theft, fraud, corruption	**13%**	10 (10%)	▲
9	Loss of reputation or brand value	**10%**	8 (12%)	▼
9	Market developments (e.g. volatility, intensified competition/new entrants, M&A, market stagnation, market fluctuation)	**10%**	6 (18%)	▼

*« Il y a **cinq ans**, la rançon exigée se serait généralement élevée à **quelques dizaines de milliers de dollars**. **Aujourd'hui**, elle **peut atteindre plusieurs millions**. »*

*« Pour **50% des entreprises ayant subies une cyber attaque**, le **risque de défaillance augmente** en moyenne de **80%** dans les trois mois qui suivent l'annonce de l'incident cyber. »*

*« Dégradation de la **valeur patrimoniale** de l'ordre **de 8 à 10%** et une **augmentation de 55 %** du nombre de jours de **retard de paiement** six mois après l'attaque. »*

*" Une attaque représente en moyenne, en plus des vols de données et de réputation mise en jeu, **100 000 euros de perte de chiffre d'affaires pour une PME.** Les frais en réparation et de formation des équipes n'étant pas négligeables. "*

Top 4 des cyber attaques

1. **Attaques ciblées et attaques en profondeur (APT) / (Rançongiciel, …)**
2. **Détournement et vol données**
3. **Déni de service (DDos)**
4. **Défiguration de sites web**

A ces attaques se rajoutent les problèmes issus de pannes matérielles (incendie, perte du nom de domaine, problème de connectivité,…)

Menaces : les acteurs

Enseignements

Les rançongiciels : un *business*, pas une technologie

L'essor des cryptomonnaies et leur valorisation a apporté aux pirates l'élément essentiel leur permettant d'opérer à distance en toute impunité. Ils sont à l'origine, pour les pirates d'un nouveau « business model » qui vient suppléer, voire remplacer les autres modèles financiers.

Par ailleurs, les polices d'assurance cyber, en payant des rançons pour les victimes ont paradoxalement contribué à asseoir ce modèle.

Les ransomwares s'imposent comme des produits emblématiques sur le marché de la cybercriminalité, ils ne sont pas prêts de disparaitre.

Ransomware : les techniques utilisées par les attaquants

1. Reconnaissance externe
- Scan de vulnérabilités
- Recherche d'identifiants compromis hors SI de la victime

2. Intrusion
- Phishing
- Exploitation de vulnérabilités
- Compte légitime sur accès distant
- Malspam

3. Reconnaissance interne
- Découverte des machines du domaine
- Identification des solutions de sécurité
- Optionnel : localisation des sauvegardes

4. Elévation de privilège
- Mimikatz
- LaZagne

5. Contrôle de l'infrastructure
- CobaltStrike/Metasploit
- Accès distant légitime
- RAT

6. Exploitation
- Optionnel : exfiltration de données
- Chiffrement
- Optionnel : identification et déstruction des sauvegardes

En cas d’attaque, comment réagir ?

- Isolez votre réseau de l’Internet mais ne mettez pas hors tension les machines (au risque de rendre difficile voire impossible l’investigation et la recherche de preuves).
- Anticipez et maîtrisez la communication de crise en interne et en externe.
- Assurez-vous rapidement de disposer de sauvegardes fiables et mettez les en sécurité.
- En cas de doutes/difficultés, faites-vous aider par des experts.
- Portez plainte auprès de la Police ou Gendarmerie.
- Reconstruisez sur des bases saines.
- Et surtout ne payez pas la rançon !

Anticipation de la défaillance technique et du sinistre majeur

Anticipation de la **défense** du Système d'Information

Etes-vous prêt ?

- Plan de **Gestion de Crise Cyber** (gouvernance / communication / moyens)
  - Prendre en compte les spécificités de la Crise Cyber

- Plan de **Défense Cyber** (organisation de la réponse opérationnelle)
  - Comment retrouver la confiance dans le SI

- Plan de **Continuité Métiers** adapté (organisation de la continuité des Métiers)
  - Poursuivre l'activité métier sans informatique, sur des temps longs.

Les réponses à apporter lors d'une crise

Comment suivre la gestion de crise ?
Check-list de crise
Main courante
Journal de crise

Quels sont les documents pour initier la cellule de crise ?
Feuille d'émargement
Checklist de salle de crise
Fiches actions par rôles
Gouvernance type

Comment réagir en situation de crise ?
Fiches réflexe par scenario
Mesures conservatoires et d'urgence
Plan de reconstruction d'un SI

Qui convoquer en cellule de crise ?
Fiches de contact / Annuaires

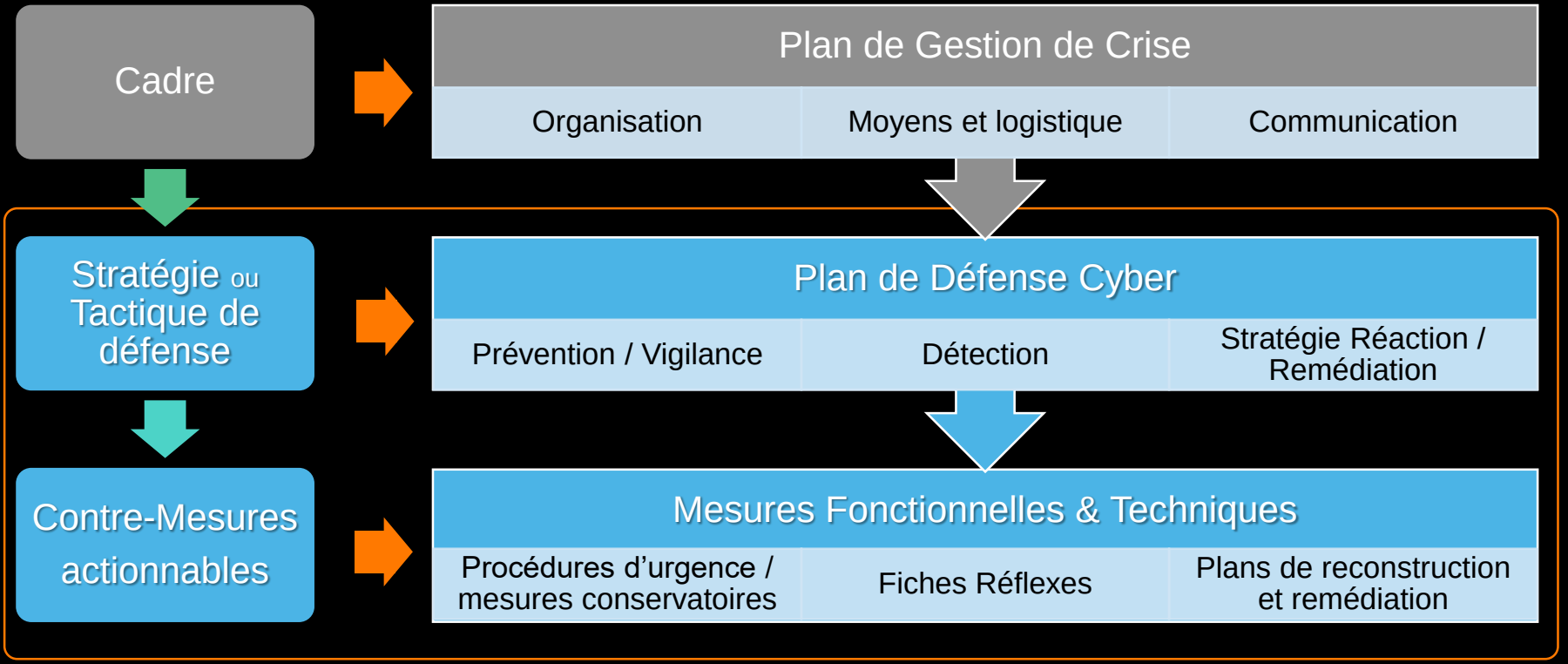
Comment communiquer en situation de crise ?
Schéma de communication
Moyens de communication
Outils de communication
Messages référencés

Comment mobiliser ?
Fiche de mobilisation

Quand passer en crise ?
Fiche de qualification et d'alerte

Comment gérer la sortie de crise ?
Bilan à chaud
Capitalisation à froid

Plan de Défense Cyber et Plan de Gestion de Crise



Plan de Défense : Référentiel guidant les choix de la Cellule de Crise

Reposant sur un **dispositif opérationnel de défense**

- Anticiper les stratégies de défense
  - Préserver les actifs essentiels
  - Limiter la propagation
  - Séquestration de preuves
  - Mettre sous surveillance
  - Évincer l'attaquant
  - Stratégie de restauration / remédiation….
- Établir et mettre en œuvre des mesures actionnables et les modes opératoires
  - Isoler des sites
  - Couper des flux (internet,…)
  - Changer les mots de passe en urgence
  - Patcher
  - Rétablir…
- S'exercer

L’humain toujours en première ligne

95%

Des cyberattaques commencent par l’humain: hameçonnage, erreur

Ces attaques sont évitables avec la bonne sensibilisation

Les points d'attention majeurs en 2021

1. Se préparer à la crise…

…en définissant un processus de gestion de crise documenté et en s'entrainant (exercice régulier de gestion de crise).

#Kit de crise (Plan de gestion de crise, Communication de crise, Fiches reflexe)

2. Renforcer les capacités de détection des attaques cyber…

…en étudiant ou déployant des solutions et des processus/services associés adaptés au contexte et sources de risques.

#EDR, #SIEM, #CYBERSOC

3. Reconsidérer la Politique de gestion des accès…

…en agissant à chaque niveau et en s'adaptant aux nouveaux usages (télétravail massif, Cloud) par le biais des technologies appropriées (double authentification, protection EDR des postes de travail,…)

#HardeningAD, #MFA, #ZeroTrust

4. Protéger le dernier rempart qu'est la sauvegarde…

…en isolant totalement les systèmes de sauvegarde du reste du SI, en multipliant et externalisant les copies, en vérifiant l'intégrité de celles-ci.

#Airgap, #3-2-1, #WORM

5. …et les « bases » (patcher, sensibiliser, auditer, …)

L'écosystème de la Cybersécurité

Editeurs / constructeurs de solutions technologiques de cybersécurité.

Intégrateurs de solutions technologiques de cybersécurité.

Opérateurs de services managés de cybersécurité (SOC, CERT, …).

Cabinets de conseil en cybersécurité.

Acteurs institutionnels / Autorités.

Orange
Cyberdefense

SECUREware

Merci