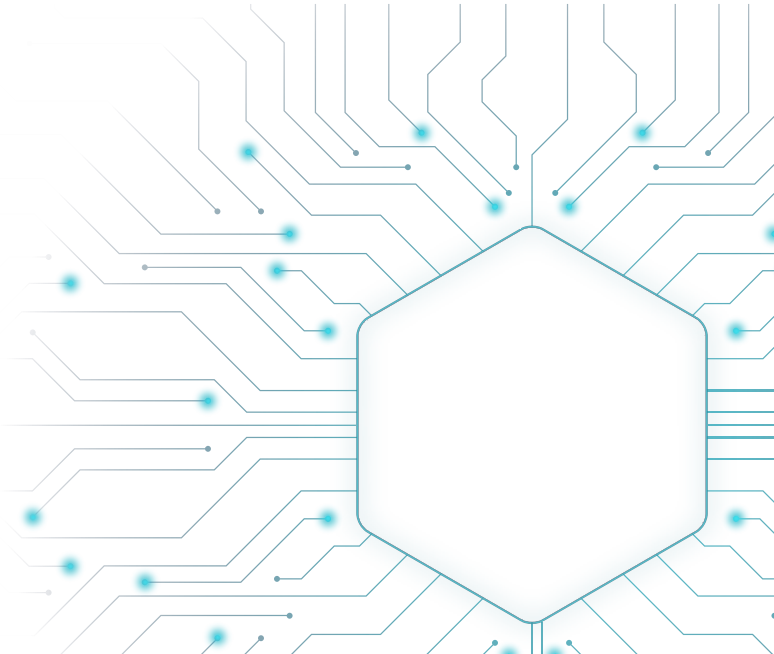
CYBER CRISE DAY
19/09/2022
PARIS

La gestion des crises cyber au-delà des SI

LIVRE BLANC

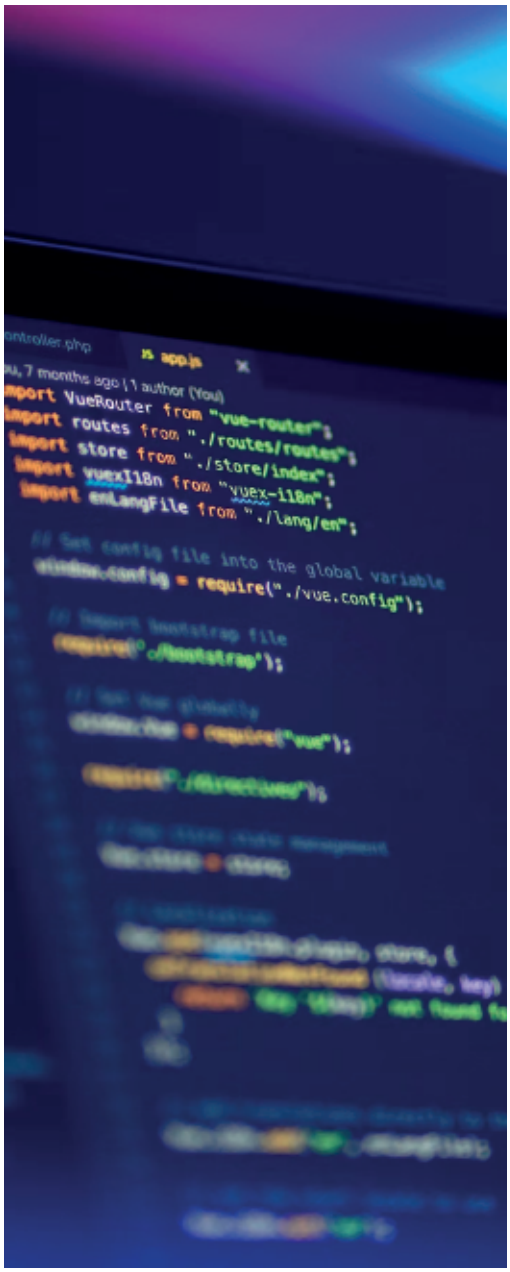


Remerciements
Merci à *Veille Magazine, Cazals & Partners* et *element,* pour l'organisation de cyber-day.info, à Thierry Marchand pour son professionnalisme, à l'ensemble des intervenants, à Johnny Maroun et à Julie Simons pour la réalisation de ce Livre Blanc.

Editeurs : Veille Magazine / element

Sommaire

Introduction



Le Livre Blanc que vous vous apprêtez à découvrir n'est pas une liste de recommandations et encore moins de principes directeurs. Il est le fruit de l'expérience et de la prise de hauteur de professionnels reconnus dans le domaine de la gestion de crise cyber.

Tous ont répondu à l'invitation de Mme Jacqueline Sala et au constat que nous avons formulé ainsi François Cazals et moi : la gestion de la cybercrise est un enjeu de gouvernance des institutions et ne saurait être limité à l'approche exclusivement SI, sans tenir compte des enjeux vitaux des organisations (ressources humaines, supply chain, financier, communication, etc.).

Hisser la gestion de crise cyber au rang de défi stratégique, c'est mettre en avant l'importance de préserver la continuité d'activité et l'ensemble des actifs d'une organisation. C'est également préserver la confiance de l'ensemble des parties prenantes et constituantes de nos entreprises et collectivités territoriales.

Ce Livre Blanc est le résultat d'une journée d'échanges, de débats et de partages d'expérience. C'est aussi une invitation à se préparer à éviter et affronter le risque cyber.

Au nom de tous les intervenants, je vous souhaite une bonne lecture !

Natalie Maroun
Directrice associée *element*

La Gendarmerie face aux cybermenaces

Général Marc Boget
Commandant de la gendarmerie dans le cyberespace

Considéré comme un officier atypique et après une première carrière dans le privé, j'ai désormais une double casquette que je cultive tout au long de mon parcours professionnel.

Officier général, spécialisé dans les systèmes d'information, prenant régulièrement des postes opérationnels sur le terrain, cette remise en cause permanente me permet d'exercer mes capacités de meneur d'hommes et de mesurer l'impact des systèmes, leurs éventuels manques qui subsistent et les besoins opérationnels émergents.

Désormais à la tête des cyber-enquêteurs de la gendarmerie, j'ai enrichi mon panel de connaissances de cet écosystème spécifique en pleine expansion.

Le commandement de la gendarmerie dans le cyberespace (COMCyberGEND) est en charge de la lutte contre la cybercriminalité, de la coordination des actions de prévention cyber pour la gendarmerie nationale et du pilotage et de l'animation du réseau CyberGend.

LE COMCYBERGEND C'EST :

- **8 900** collaborateurs en 2022, avec l'intention d'atteindre **10 000** en 2024.
- Une entité qui va de la **prévention** (pour développer l'hygiène numérique des organisations) jusqu'à **l'investigation.**
- Un grand commandement qui a son **budget propre** pour accroître son agilité.
- **400 interactions par jour** sur la plateforme en ligne magendarmerie.fr
- **101 000** procédures judiciaires traitées.
- **508 000** personnes sensibilisées en 2022.

QUELQUES CHIFFRES :

- En 2020, la cybercriminalité a coûté entre **6 000 à 7 000 milliards de dollars** au plan international et a généré environ 1 500 milliards de revenus pour les cyberdélinquants.
- Les attaques par rançongiciel se produisent toutes les **11 secondes** de par le monde.
- Entre 2020 et 2021, les faits d'attaques ont connu une **augmentation de 24%**.
- Le COMCyberGEND estime qu'une plainte est déposée auprès de ses services pour **250 attaques**.
- En 2021, le nombre d'entreprises touchées par des attaques a augmenté de **13%**.

Les systèmes informatiques sont de plus en plus interpénétrés, complexes et internationaux ; ce qui induit une augmentation des vulnérabilités, plus de 50 sont actuellement découvertes par jour. Selon le COMCyberGEND, **les périodes**

de vente ou d'achat de société sont les plus favorables à la pénétration des systèmes d'information par les délinquants. Il convient donc de les sécuriser d'autant plus durant ces périodes.

L'intérêt d'une telle entité rattachée au directeur général de la Gendarmerie nationale, c'est qu'elle fonctionne selon le principe de subsidiarité : la réponse est adaptée au niveau de l'attaque. Les services en charge de la gestion de l'attaque vont évoluer selon sa criticité et sa complexité. Le COMCyberGEND dispose de divisions de :

- Proximité numérique
- Investigation numérique
- Expertise numérique
- Stratégie numérique

EN CAS D'ATTAQUE, LA MARCHE À SUIVRE EST :

- ✔ Contacter immédiatement la gendarmerie
- ✔ Préserver la scène de crime en débranchant le système d'information du réseau **sans les éteindre**
- ✔ Communiquer régulièrement en interne et en externe
- ✔ Éviter les négociations parallèles et ne pas activer une entreprise de remédiation sans coordination avec les forces de l'ordre
- ✔ La gendarmerie et les unités du ComCyberGend se déplaceront alors immédiatement auprès de la victime et s'intégreront à son dispositif de gestion de crise pour récupérer immédiatement les traces numériques et aider celle-ci à gérer au mieux la crise cyber.

DES RÉFLEXES À ADOPTER EN CAS DE CYBERATTAQUE

Pour contacter le COMCyberGEND

Tel : 17 ou 112

magendarmerie.fr

Retrouvez l'intégralité de l'intervention sur la chaîne YouTube de cyber-day.info

Gestion d'une cybercrise, ou comment être prêt le jour où une crise majeure arrivera

Arthur Chédeville
BU Manager chez ITEC SECURITY

Anthony Sbong
RSSI chez ITEC SECURITY

Arthur Chédeville
Après avoir évolué au sein de plusieurs cabinets de conseil et ESN dans le domaine de la cybersécurité, j'ai rejoint le management de la filiale ITEC SECURITY afin de développer l'activité autour des métiers fonctionnels de la cybersécurité, de la continuité d'activité et de la gestion de crise.

Au cours de mes différentes expériences, j'ai eu l'opportunité d'accompagner de nombreux clients (de tous secteurs) dans la structuration de leur stratégie de cyber-résilience, ainsi que dans leur mise en œuvre. J'accompagne également mes clients dans la réalisation et l'animation d'exercices de gestion de crise cyber.

Anthony Sbong
Après plusieurs expériences en tant qu'ingénieur et expert en infrastructure, réseau et sécurité au sein d'ESN ou de clients finaux, j'ai rejoint la Société Générale en tant que RSSI.

En 2020, j'ai fondé le cabinet ITEC Security (au sein du Groupe ITEC). J'accompagne depuis les DSI et RSSI sur des problématiques de sécurité et cyberdéfense des SI. Au cours de ma carrière, j'ai eu l'opportunité d'intervenir sur plusieurs crises cyber majeures.

Bien gérer une cybercrise commence par savoir qu'elle se caractérise par :

- Sa **double temporalité**, qui implique de prendre des décisions rapidement mais peut générer des impacts à long terme. Il faut en ce sens adapter le niveau de réponse selon l'urgence ;
- **L'absence d'unicité de lieu**, c'est-à-dire qu'elle peut avoir des impacts à divers endroits simultanément ;
- Une **incertitude permanente** dans laquelle l'organisation impactée n'a d'autre choix que de prendre des décisions. Il est alors essentiel d'avoir effectué un travail préparatoire pour pouvoir prendre les décisions adéquates ;
- **L'incompréhension de l'identité et les motivations de l'attaquant**, qui rendent parfois difficile une riposte de la part de l'organisation.

Quatre piliers sont identifiés pour se préparer efficacement à faire face aux crises :

- Mettre en place un **processus de gestion de la continuité d'activité ;**
- Définir et mettre en œuvre une **organisation, une gouvernance et des processus de gestion de crise ;**
- Mettre en place l'**outillage nécessaire** permettant de supporter ces processus ;
- **Entraîner** l'ensemble des populations à faire face à des crises.

Pour adapter les procédures de gestion de crise de manière fluide, il faut :

- **Définir en amont l'organisation** générale de crise : la composition des cellules opérationnelles et décisionnelle, les rôles et responsabilités des acteurs clés, les processus d'escalade et d'activation des cellules de crise ;
- **S'assurer de la disponibilité des bonnes ressources** en cas de crise (équipe d'experts, analyse SOC, équipes forensiques, etc.) ;
- **Mobiliser les expertises nécessaires** au bon pilotage de la crise (RH, communication, juridique, etc.).

Lorsqu'une crise cyber se déclenche, les premières réponses que l'on va apporter sont primordiales pour la gestion future. **Même si la crise est cyber, son impact est organisationnel et systémique**, ce qui requiert de facto une mobilisation des ressources humaines et de la communication.

L'entraînement est aujourd'hui la clé d'une gestion de crise réussie. Il permet de :

- **Adopter les bons réflexes** en se confrontant à des situations de crise ;
- **Simuler des crises** pour tester l'efficacité des processus de crise, l'organisation et l'outillage ;
- **Partager les bonnes pratiques** de gestion de crise, de communication, et familiariser les acteurs à leur rôle ;
- **Impliquer l'ensemble des acteurs** (opérationnels, décideurs, top management) dans la démarche de cyber-résilience.

Il est primordial de sensibiliser les équipes de manière régulière. La gestion de la crise et les réflexes à avoir doivent devenir naturels pour les collaborateurs, de sorte que leur réponse sera assurée en situation de crise. En effet, **la préparation permet de diminuer le facteur de stress grâce aux automatismes.** Elle augmente de fait la résilience de l'organisation et sa capacité à gérer la situation.

Retrouvez l'intégralité de l'intervention sur la chaîne YouTube de cyber-day.info

Ransomware : une fatalité qui ne doit pas etre fatale

Linley Brasse
CEO de ITEC STRATEGY et ITEC SECURITY

Linley Brasse
Diplômé de SUPINFO International University, je suis aujourd'hui CEO de ITEC STRATEGY et ITEC SECURITY, après avoir été directeur de la Stratégie d'EVA Group/BSSI et RSSI d'Adisseo.

De l'entreprenariat sur le marché français à l'ouverture de filiales à l'étranger, je suis en charge de l'innovation technique et du déploiement de technologies adaptées au développement et à l'efficacité des activités du groupe ITEC. Homme de terrain, j'aime aller au cœur de la difficulté et en résoudre tous les aspects. Mon profil technique est un vrai plus pour trouver la meilleure solution au bon moment.

Dans un monde dont l'interconnexion est croissante, la cybercrise est inévitable pour une organisation. **La question n'est pas de savoir si elle va avoir lieu, mais quand**. Pour s'y préparer de la meilleure des manières, de nombreux moyens existent pour anticiper, réagir et reconstruire.

Tout d'abord, en amont de l'attaque, il faut que l'organisation adopte une démarche d'hygiène informatique par des actions simples :

- **Avoir une vraie gouvernance** avec des outils, de la documentation, des processus, des directives, des politiques, des guidelines, et se préparer techniquement ;
- **Réaliser des audits** organisationnels ou techniques qui permettent de construire et suivre les plans d'amélioration, notamment pour les vulnérabilités identifiées ;
- **Former et éprouver les équipes** sur les technologies afin qu'elles soient en capacité de bien utiliser les outils de détection et de correction pour minimiser les effets d'une attaque potentielle ;
- **Identifier un prestataire de réponse** à incident pour vous accompagner, une fois la crise survenue, dans votre plan d'actions ;
- Mettre en place les **outils de protection adéquats**, tant pour les usages professionnels que personnels.

Une fois cette première phase effectuée, il faut former l'organisation sur les réflexes à avoir en cas d'attaque cyber :

- **Figer la situation** : ne pas débrancher ou éteindre, isoler ce qui a été compromis, couper du réseau interne (une deuxième charge d'attaque peut se déclencher en décalé en cas de coupure d'internet), garder la partie impactée isolée. Il est primordial de penser l'architecture de son réseau pour éviter une propagation rapide de l'attaque ;
- **Préserver les preuves** pour que les équipes de *forensics* puissent les analyser, comprendre la stratégie des attaquants et mieux protéger le SI de l'organisation. Cette étape permet également de relancer plus rapidement le système ;
- **Communiquer en interne** sur les actions que doivent prendre les

utilisateurs et les procédures à mettre en place ;
- **Mettre en place un canal de communication** non adhérent au SI qui permet de conserver un accès aux données en cas de chiffrement.

Une fois que l'attaque survient, plusieurs procédures sont à dérouler :
- **Phase de forensique** : étudier le comportement, l'attaque, par quel chemin elle est arrivée ;
- **Déclarations légales** : dépôt de plainte à la CNIL, alerter l'ANSSI en cas d'attaque ;
- **Communication externe au besoin** : partenaires, fournisseurs, clients, les personnes qui peuvent être impactées par l'attaquant ;
- **Planifier la reconstruction ;**
- **Mettre en œuvre la reconstruction** : avec un plan précis.

Retrouvez l'intégralité de l'intervention sur la chaîne YouTube de cyber-day.info

Anticiper, s'assurer et gérer les risques cyber : quelles étapes

Ludovic Van Egroo
Manager GRC Conformité, Cybersécurité

Gaëlle Baldet-Ladan
CEO GEODESK

Emeline Segarra-Chabot
Directrice des Opérations adjointe

Ludovic Van Egroo
Je dispose de 12 années d'expérience dans le domaine du conseil en matière de gestion des risques, d'évaluation et de protection des actifs.
Manager en gestion des risques cybersécurité et conformité au sein de SSG, j'accompagne les entreprises et les administrations dans leurs démarches de prévention et de protection par l'identification des actifs, la mise en œuvre de mesures de cybersécurité (organisationnelles et juridiques dont les contrats d'assurance cyber)

Gaëlle Baldet-Ladan
CEO de Geodesk, j'ai plus de 20 ans d'expérience en accompagnement et en assurances à l'international. La protection des personnes et des biens et les enjeux liés à la sécurité et au Cyber sont au cœur de mon activité.

Émeline Segarra-Chabot
J'ai passé 16 années au sein du Ministère des Armées marquées par la participation active à de nombreuses gestions de crise en lien avec la sécurité des personnes puis 3 années au pilotage d'une équipe pluridisciplinaire composée d'ingénieurs cyber et d'analystes géopolitiques chargés d'investiguer et de contextualiser les cyber attaques au profit des autorités. Je me suis ensuite orientée vers le métier de consultant en gestion de crise au sein de SSG où je supervise en qualité de Product Manager une équipe qui opère depuis un peu plus d'une année l'accompagnement client sur la définition de dispositifs de gestion de crise et la réalisation d'exercices.

En 2021, les cotisations d'assurance pour couvrir le risque cyber ne s'élevaient qu'à 3% des cotisations globales d'assurance pour les dommages professionnels. Deux raisons peuvent être invoquées : **la sous-estimation du risque cyber** et la **difficulté à en estimer les impacts.**
Des disparités existent selon la taille de l'entreprise : **84% des grandes entreprises sont assurées contre moins de 0,3% pour les PME.**

En souscrivant à une assurance cyber,

les entreprises sont accompagnées sur trois axes :

- **La cartographie,** qui permet de comprendre les activités de l'organisation et d'analyser les réflexes des collaborateurs. Elle identifie les activités critiques et sensibles, qui sont à protéger en priorité. Le système d'information est évalué pour déterminer les éventuelles failles qui pourraient bénéficier aux pirates.
- **La crise,** lors de laquelle l'assurance accompagne l'organisation pour comprendre comment l'attaque est survenue, les activités qui sont impactées et donner la marche à suivre quant à l'intervention.
- **La prise en charge des coûts** induits par le paiement éventuel d'une rançon, mais aussi des dépenses nécessaires en communication ou encore sur le plan juridique.

La sélection de la bonne police d'assurance passe par différents process en interne : une cartographie des risques, une cartographie du système d'information, l'évaluation de la criticité, de l'exposition et des impacts.

Pour transcrire ensuite le contrat en processus opérationnels, les assurances déterminent 3 étapes :

- **Les procédures de déclenchement,** en définissant les indicateurs
- **Les procédures d'assistance,** par la définition des services d'assistance et la préparation des moyens d'accueil des services d'assistance
- **La procédure d'indemnisation,** qui évalue les pertes et recueille le montant des coûts

Le recours à l'assurance cyber permet à l'organisation de **bénéficier de contacts certifiés en cybersécurité** et de s'assurer de contacter la bonne personne. En outre, elle peut prendre en charge les frais liés à la **remise en état du système d'information**, la perte d'exploitation ou encore au paiement de la rançon.

La police d'assurance peut quant à elle inclure, selon la maturité de l'organisation, des prestations différentes :

- L'intervention ponctuelle d'experts (Informatique, juridique, communication),
- Les services d'assistance,
- La réponse à un incident,
- La gouvernance de crise,
- Un retour d'expérience sur l'incident et le déploiement d'un plan d'actions.

Dans l'approche de l'assurance cyber, il y a une prise en compte certaine de tout l'aspect préventif. Le contrat est fortement conditionné au volet préventif afin que les entreprises minimisent les risques sur leur système d'information.

Retrouvez l'intégralité de l'intervention sur la chaîne YouTube de cyber-day.info

Les apports de la direction juridique à la gestion de crise cyber

Sandrine Cullaffroz-Jover
Avocate Associée, Ernst & Young Société d'Avocats, Financial Services

Nicolas Bourgeois
Data Protection Officer

Sandrine Cullaffroz-Jover
Je suis Avocate Associée au sein de Ernst & Young Société d'Avocats, Financial Services.

J'anime la pratique « droit du numérique » au sein de l'organisation FSO dédiée aux acteurs des services financiers et accompagne, tant en conseil qu'en contentieux, une clientèle française et internationale du secteur financier sur des questions liées à l'innovation et à la protection du patrimoine informationnel (protection des données personnelles, droit des nouvelles technologies, propriété intellectuelle, et cybercriminalité).

Je figure également dans les classements Legal 500, et du Magazine Décideurs (Innovation, Technologies & Télécoms).

Nicolas Bourgeois
J'ai un parcours scolaire juridique classique (DESS Paris X droit des nouvelles technologies) adossé à des études d'histoire des médias à la Sorbonne. Après un parcours de juriste spécialisé en droit des nouvelles technologies pendant 13 ans, (Telecoms, Retail) je suis devenu DPO en 2017.
Je suis membre de l' International Association of Privacy Professionals (CIPM / CIPP/E) et de l'AFCDP, dont je co anime le groupe régional "Nord". J'interviens comme consultant indépendant et formateur en protection des données sur la protection des données depuis 2021, ansi qu'en tant qu'enseignant vacataire à l'Université des Sciences Juridiques de Lille ainsi qu'à l'Université Catholique de Lille.

En gestion de crise cyber, différentes directions interviennent dans la cellule de crise. Parmi celles-ci, la direction juridique est essentielle, notamment lorsque la protection des données ou des actifs de l'organisation est compromise.

Trois rôles fondamentaux mais distincts interviennent au sein de cette direction juridique : le directeur juridique, le *Data Protection Officer* (DPO) et l'avocat.

- **Le directeur juridique** est une figure de neutralité, de connaissances et d'expertise juridique au sein de l'organisation. Il apporte un regard dans la protection des actifs de l'entreprise, coordonne la crise avec les directions fonctionnelles pour apporter un niveau d'information granulaire et spécifique si nécessaire et détermine à quel moment il aura besoin de s'adjoindre les conseils d'un avocat.

- **Le DPO** est le chef d'orchestre qui s'assure de la conformité des traitements de données à caractère

personnel. Il n'est pas responsable personnellement mais doit piloter la démarche de protection des données de l'entreprise. Il travaille avec toutes les directions et fonctions pour garantir une bonne coordination des directions métier, technique, juridique avec l'ensemble des responsables métier et les directions. En situation de gestion de crise, il intervient aux côtés de la direction juridique dans la cellule de crise, et si besoin auprès des personnes concernées par la fuite des données ou d'institution comme la CNIL en tant qu'interlocuteur privilégié.

- **L'avocat** a quant à lui une compétence tant en matière de conseil qu'en contentieux, et traite régulièrement avec des autorités judiciaires et réglementaires. Il peut apporter des éclairages et conseiller le directeur juridique, s'agissant notamment de la défense des intérêts de l'entreprise et de la prise de décision du comité de direction dans le cadre de la gestion de crise. L'avocat est soumis au secret professionnel.

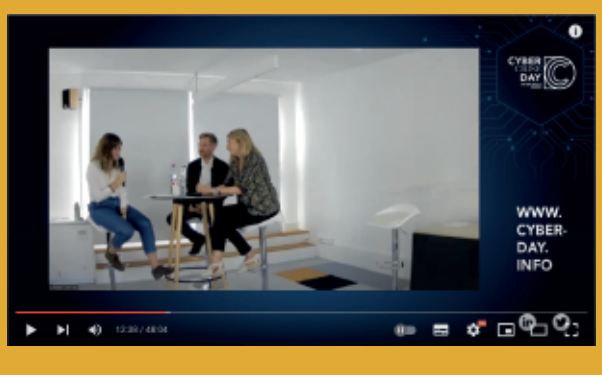
La protection des données de l'entreprise et des personnes est l'une des composantes majeures de la gestion de crise cyber. Pour savoir si elles ont été compromises par l'attaque, il faut réaliser un diagnostic technique et juridique, qui prend la forme d'état des lieux : identifier les activités et données concernées, déterminer les dispositions réglementaires et les éventuelles obligations de notification, notamment en ce qui concerne la protection des données individuelles.

La coordination au niveau de la communication – qu'elle soit interne, externe ou avec les tiers partenaires de l'entreprise – est indispensable pour une gestion optimale de la crise. L'anticipation, par l'identification des besoins et l'entrainement préalable, est essentielle pour une gestion plus apaisée de la crise. Par exemple, la recherche de prestataires de service forensique, d'un huissier si nécessité de faire un constat, d'autorisation pour encadrer les mesures conservatoires et probatoires qui pourraient être nécessaires dans le cadre d'une démarche précontentieuse peuvent faciliter la gestion sur le moment. Ces questions figurent dans la feuille de route du directeur juridique.

En situation de crise, l'équipe juridique, en collaboration avec les autres services/directions de l'entreprise, doit mettre en place une stratégie qui passe par trois étapes :

- **La protection** de l'entreprise, ses dirigeants et ses activités ;
- **L'alerte** aux pouvoirs publics, aux salariés et aux autorités compétentes ;
- **Le secours**, qui passe par la remédiation.

Retrouvez l'intégralité de l'intervention sur la chaîne YouTube de cyber-day.info



La communication de crise en cas de cyberattaque

Natalie Maroun
Directrice associée d'element

Thierry Fusalba
Fondateur et directeur de l'Agence C4

Céline Delysse
Fondatrice Le Cab.org

Natalie Maroun
J'ai une expérience de 15 ans en conseil, formation et recherche en gestion des risques et des crises. J'ai exercé au sein de la sous-direction de la planification et de la gestion des crises du ministère de l'intérieur, puis au cabinet Heiderich et au sein de l'Observatoire International des Crises où j'ai occupé le poste de Directrice du développement jusqu'en 2021. Intervenant en coopération internationale pour l'OMS, la Banque Mondiale, Expertise France ou encore la GIZ, j'interviens dans les cycles internationaux ou des missions de coopération de l'INSP en leadership de crise.

Thierry Fusalba
Ancien colonel chargé de la communication et de la contreinfluence, j'ai quitté l'armée après 25 années de service.
En 2009, j'ai créé l'Agence C4 qui regroupe des experts indépendants et propose aux entreprises une expertise en communication et gestion de crise.
Au titre de la réserve opérationnelle, je me suis rendu au Kosovo comme directeur du Joint Operational Center puis comme conseiller influence en Estonie dans le cadre de la mission de l'OTAN face à la Russie.
Enseignant à l'université de Tours, à l'IRIS et à l'Institut Diplomatique de Paris, je suis membre du conseil scientifique de l'Institut d'étude des crises de Lyon.

Céline Delysse
Je suis fondatrice du Cab.org, une unité capable de se mobiliser pour les décideurs dont le métier fait sens avec l'intérêt général. Chef d'entreprise à 27 ans, j'ai développé de nombreux projets pour des marques internationales avant d'occuper des postes importants en ministère, en cabinet, dans la sécurité sanitaire.

En situation de crise, et notamment de crise cyber, la communication devient essentielle.
Son enjeu principal est celui d'authenticité : informer les publics de la meilleure des manières et les alerter rapidement pour éviter d'autres victimes.

La mise en œuvre de la communication de crise peut néanmoins s'avérer compliquée, d'autant plus que **les canaux de communication traditionnels peuvent parfois être indisponibles.** L'incertitude quant à l'identité de l'attaquant et ses intentions, mais également sur les causes de l'attaque, ne doit pas être minimisée.

La gestion des cybercrises ne diffère pas fondamentalement de la gestion de crise. Si la crise cyber a des spécificités, **il y a un risque à tronçonner la gestion de crise et à l'aborder sous le seul angle cyber** ; ce serait omettre les autres aspects que la crise peut prendre (réputationnel, interne, rachat, etc.).

Trois écueils sont principalement à éviter en cas de crise cyber :

- L'effet de mode sur la cyberdéfense (travailler son e-réputation permet de répondre à tous les problèmes),
- L'effet réducteur de la technicité (tout le monde doit être impliqué dans la résolution de la crise),
- L'effet de segmentation (considérer qu'une crise est uniquement cyber).

Pour s'en prémunir, il est essentiel de :

- Favoriser la collaboration entre le technicien et le manager, notamment en termes de communication pour adopter les mêmes messages,
- Prendre en compte la sphère interne et externe à l'organisation, en intégrant la sensibilité des salariés aux obligations qui leur sont faites,
- Comprendre la porosité entre le réel et le virtuel.

Cette communication doit être mise en place selon trois principes : **la liberté d'action, l'économie des forces et la concentration des moyens.**

Contrairement à ce que l'on pense, il y a un réel paradoxe dans la communication en cas de crise cyber. Le communicant n'est pas toujours intégré à la cellule de crise bien qu'on ait tendance à croire qu'il est apte à régler la crise seul. Or, il est essentiel qu'il y soit convié pour élaborer les messages à faire passer avec chacun des responsables.

En cellule de crise, la gestion de l'information (par les flux entrants et sortants) constitue un problème plus prégnant que la communication. **Il est nécessaire de travailler en transversalité tout en conservant un système décisionnel permettant au communicant d'adapter sa communication.** Il est effectivement confronté à l'incertitude de l'adversaire et la nécessité de réagir très rapidement en respectant les principes de subsidiarité et de redondance.

Un bon communicant doit prendre le temps de **poser la stratégie,** pour travailler dans l'urgence mais non pas dans la précipitation.

Dès le déclenchement de la crise, il faut déterminer :

- Les messages à passer dans un catalogue de messages, en n'oubliant pas que chacun parle à son niveau ;
- Les audiences à valeur ajoutée, c'est-à-dire rester pragmatique sur les publics qui sont concernés en premier lieu ;
- Les vecteurs de communication (médias, coup de téléphone).

Dans le cas des crises cyber, il faut toujours commencer par l'interne : déjà car les collaborateurs doivent être les premiers informés, ensuite pour fluidifier la remontée d'information aux autorités compétentes.

Il ne faut pas oublier que la crise peut être une opportunité quand les publics sont satisfaits des informations qu'ils ont reçues. Malgré son caractère négatif à l'origine, la crise peut finalement se dévoiler bénéfique à l'organisation ; c'est pourquoi il ne faut pas négliger la communication.

Retrouvez l'intégralité de l'intervention sur la chaîne YouTube de cyber-day.info

Stratégie cyber et antifragilité

François Cazals
Professeur à HEC, colonel de Gendarmerie

Linley Brasse
Je suis professeur adjoint à HEC Paris.

Spécialiste des stratégies innovantes, de la transformation numérique des organisations et de la valorisation des données (Big Data, Data Science, intelligence artificielle), je dirige mon propre cabinet de conseil en stratégie. Je suis également auteur de nombreux ouvrages et articles sur ces sujets.

Par ailleurs, je suis colonel (réserve opérationnelle) de la Gendarmerie Nationale, affecté au cabinet du directeur général au pôle « Stratégie et prospective ».

Nous ressentons tous que nous vivons un moment singulier où les crises se multiplient, s'accélèrent et l'incertitude est généralisée.

Nassim Nicholas Taleb a décrit cet environnement nouveau et ses dynamiques : c'est l'ère des « cygnes noirs », où surviennent des événements systémiques totalement imprévisibles, qui transforment profondément notre monde. Quel sera le prochain cygne noir et comment l'affronter ? C'est la question que se pose tous les organes de directions des organisations, publiques ou privées, partout dans le monde.

La menace Cyber devient tellement importante et sa croissance si rapide qu'elle figure naturellement parmi les cygnes noirs les plus probables. Et ceci change tout ! Autrefois reléguée dans la famille des risques « techniques », elle était exclusivement envisagée sous l'angle opérationnel et prise en charge par le management intermédiaire, au sein des directions des systèmes d'information, généralement. Nous percevons que la menace Cyber change de nature et de dimension et met en cause, aujourd'hui, potentiellement, la pérennité des organisations, voire des états. De ce fait, elle devient une véritable problématique stratégique qui doit être abordée dans les équipes de direction des entreprises et les plus hautes sphères de décision des organisations publiques. Ceci n'est pas facile, car les dirigeants manquent souvent de culture technologique et n'envisagent les technologies de l'information que comme une commodité opérationnelle, dont la finalité est principalement d'augmenter la productivité de l'organisation.

Le défi est d'une tout autre nature : pouvoir affronter des crises Cyber qui déstabilisent et mettent en danger l'organisation, évidemment, mais aussi savoir acquérir un savoir-faire différenciant. Cette capacité exceptionnelle à faire d'une crise une opportunité a été également étudiée et conceptualisée par Nassim Taleb : il s'agit de l'antifragilité.

Pour devenir antifragile, il faut évidemment complètement repenser son logiciel stratégique.

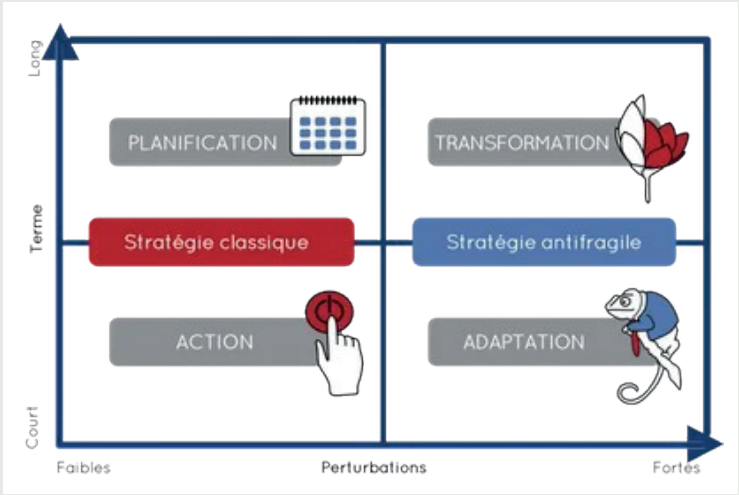
Si la planification et la conception de plans d'actions préventifs ou curatifs (« plan de continuité de l'activité / PCA » Cyber) sont

évidemment nécessaires, ils ne sont plus suffisants.

Il faut maintenant intégrer dans les organisations des capacités d'adaptation et de transformation face à des perturbations très fortes de l'environnement, comme les crises et la menace Cyber.

Pour qu'il ne s'agisse pas uniquement d'injonctions, il faut revoir son modèle de fonctionnement en profondeur. Deux approches stratégiques innovantes peuvent favoriser ce changement de paradigme : l'effectuation et la stratégie océan bleu. Ces méthodologies sont fondées sur deux grands principes. Le premier, l'effectuation, suggère de s'inspirer du management stratégique des petites entreprises et de concevoir une « stratégie minimale viable », en cas de crise forte, fondée sur la prise en compte des moyens disponibles et non pas sur les buts désirés, dans une logique de « perte acceptable ». Le second principe propose une véritable réinvention du modèle organisationnel, fondé sur « 4 actions » (Eliminer, réduire, augmenter, créer/ERAC) : arrêter certaines pratiques devenues inutiles, obsolètes ou néfastes, revoir l'intensité de certaines actions (à la hausse et à la baisse) et créer de nouvelles variables stratégiques totalement innovantes.

« Remonter » la menace Cyber au niveau stratégique semble donc aujourd'hui incontournable. Il faut donc concevoir une véritable « stratégie Cyber », pour diminuer ses vulnérabilités, évidemment, mais également pour tendre vers l'antifragilité. Ceci induit la nécessité d'une nouvelle posture managériale, des équipes opérationnelles, mais peut-être d'abord et surtout des dirigeants.



Retrouvez l'intégralité de l'intervention sur la chaîne YouTube de cyber-day.info

Collaboration experts et décideurs : la clé d'une gestion de crise

Marie Odile Crinon
Administratice du Clusif et présidente du cabinet MRC2

Michel Séjean
Directeur scientifique du Code de la cybersécurité

Cathy Loiseau
CEFCYS

Marie-Odile Crinon
Je suis administratrice du CLUSIF où j'apporte en particulier mon expertise en pilotage de crise et en maîtrise du risque cyber. Je participe au comité de programme du CLUSIF et interviens dans ses conférences.
Présidente du Cabinet MRC2 spécialisé dans le Management des Risques et Crises Cyber (www.mrc2.fr) que j'ai créé en 2014, je conseille les entreprises dans leur stratégie de cyber-résilience (analyses de risques, missions de sensibilisation à la résilience, exercices de crise, …).
Je suis également auditrice de l'IHEDN et de l'IHEMI et colonel de réserve citoyenne.

Michel Séjean
Je suis professeur agrégé de droit privé et sciences criminelles à l'Université Sorbonne Paris Nord (Paris 13). Chercheur associé à la Chaire CYBER de l'IHEDN, je suis auditeur de la Session Nationale Souveraineté Numérique et Cybersécurité de l'IHEDN. Je suis directeur scientifique du Code de la cybersécurité en versions papier et numérique, paru aux éditions Dalloz (1ère éd. 2022).

Cathy Loiseau
J'ai 22 ans d'expérience dans le domaine de l'informatique sur les postes de consultante technique, de cheffe de projets et de responsable de la sécurité des systèmes d'information.
Je suis membre active du CEFCYS (le cercle des femmes de la cybersécurité) qui a pour mission de promouvoir et faire progresser la présence et le leadership des femmes dans les métiers relatifs à la sécurité des systèmes d'information.

L'interface entre les experts et les décideurs est au cœur de la gestion de crise en général et de la cybercrise en particulier. Elle couvre l'ensemble des 5 étapes qui fondent la gestion de crise cyber :

1- L'organisation du dispositif de crise : les bonnes personnes avec les bons outils
2- La qualification de l'incident et de ses impacts
3- La prise de décision dans l'incertitude
4- La communication (interne et externe)
5- L'anticipation en crise.

Souvent, des biais cognitifs influencent la perception d'une situation et peuvent altérer

le jugement que s'en font les décideurs.

- **Le biais de similarité** fait référence à une situation de crise déjà vécue sur laquelle on se base pour acter l'organisation et les décisions à prendre.
- **Le biais d'autorité** peut surévaluer l'opinion d'une personne ayant l'autorité hiérarchique, même si le stress ou la fatigue biaise son jugement ou sa capacité de décision.
- **Le biais d'expertise** qui se focalise sur le fait générateur de la crise. Il empêche d'adopter une vision élargie de la crise et se réfère seulement à la personne en charge du domaine de l'incident générateur, sans même consulter les autres responsables impactés par la crise.

En situation de crise cyber, **la prise de décision inclut des composantes variées, dont la composante juridique dans le temps court**. Mais les textes juridiques sur la cybersécurité étaient peu accessibles, car ils sont dispersés dans plusieurs codes, textes internes, européens et internationaux. D'où une initiative éditoriale, qui ne crée aucun texte nouveau, mais qui les rassemble au sein d'un recueil intitulé « Le Code de la cybersécurité » (éd. Dalloz, 2022). Il organise les textes en vigueur selon trois ensembles : le droit de la sécurité des systèmes d'information, le droit de la lutte contre la cybercriminalité et le droit de la cyberdéfense. Ce recueil est agrémenté de commentaires rédigés en langage courant pour que les non-juristes qui sont usagers du droit de la cybersécurité, comprennent les règles qui s'appliquent à eux.
Lors d'une crise d'origine cyber, pour optimiser la prise de décision, le responsable de la sécurité des systèmes d'information (RSSI) va s'adjoindre l'aide des équipes opérationnelles. Son rôle est de **synthétiser la situation** auprès de la direction de façon compréhensible, de faire des reportings réguliers, de **communiquer avec les autorités et les différentes parties prenantes** (clients, régulateurs, communauté cyber, etc.), en veillant à une bonne synchronisation avec les autres canaux de communication.

Les deux fonctions, RSSI et responsable juridique, doivent en permanence tenir compte de l'incertitude et des informations manquantes. De nombreuses démarches sont à effectuer en cas de cyberattaque ou de fuite de données : prévenir la Cnil, informer les personnes dont les données personnelles ont fuité, l'ACPR en cas de fuite de données bancaires, déclarer l'incident à l'ANSSI, l'autorité de santé… La préparation à froid est donc essentielle pour ne pas se retrouver dépourvu quand la crise survient, par exemple concernant l'accès aux datacenters, l'identification d'experts pouvant intervenir rapidement, etc.

Dans l'optique de gérer efficacement la crise, l'élaboration de fiches réflexes en amont peut avoir un effet bénéfique sur la future gestion. De même, l'identification des potentielles parties prenantes peut être élaborée en prévention pour faciliter par la suite la communication. Il faut également réfléchir à des éléments de langage qui pourront facilement être utilisés avant d'avoir plus d'informations (la situation, les mesures qui ont été/vont être prises, la continuité d'activité). En situation de crise cyber, les mots d'ordre sont humilité et transparence !

Une bonne préparation de la crise en amont est donc fondamentale pour en réduire les conséquences. En situation de crise, on ne doit plus essayer de traiter les causes de la crise, mais avant tout ses conséquences.

CYBER CRISE DAY
19/09/2022
PARIS

www.cyber-day.info