CYBER-RESILIENCE

vers la Cyber-Reliance

LIVRE BLANC

ebrc

Cyber-Résilience

Yves Reding
CEO | *EBRC*

Le XXI[ème] siècle devra être hautement résilient

Depuis plus de 10 milliers d'années, depuis le début de l'ère néolithique, la civilisation humaine se développe par paliers successifs de plus en plus rapprochés, poussée par la Technique et la Technologie et à une vitesse aujourd'hui devenue exponentielle.

Portée par cette Technique et cette Technologie, l'Humanité s'est dotée d'une capacité à changer le monde. Elle a acquis de nouveaux savoirs, repoussé nombre de limites et rêvé à de nouvelles conquêtes. Elle a de ce fait également modifié considérablement l'écosystème de la planète Terre.

Dans cette recherche constante de progrès, l'Homme du XXI[ème] siècle devra affronter deux défis majeurs qu'il aura lui-même engendrés : l'un porte sur le monde réel, celui de la Nature, l'autre sur le monde virtuel, celui du Digital. Deux challenges distincts certes, mais qui portent en eux le même impératif : la Résilience.

> **« La Résilience, c'est la capacité que possède une espèce, un état, une organisation, une entreprise ou un individu, d'affronter et de relever les inévitables défis, problèmes ou obstacles rencontrés au cours de son existence et d'en sortir grandi, plus fort et mieux armé pour s'engager dans l'avenir. »**

DE LA RÉSILIENCE DE LA NATURE...

Le défi principal de notre époque est sans conteste celui du réchauffement climatique, dont les effets sur la géophysique, l'agriculture et la biodiversité sont évidents. Il relève du monde physique. Il est palpable, observable et mesurable. Il est issu des première et seconde révolutions industrielles et de l'exploitation de ses ressources clés, le charbon et le pétrole.

Ce bouleversement climatique étant déjà engagé, il faut désormais entreprendre au côté des actions d'atténuation, des actions d'adaptation. En 2015, l'Accord de Paris, premier accord universel contraignant sur le climat, a amorcé une politique ambitieuse. Plus qu'une prise de conscience, il s'agit d'une véritable démarche planétaire de résilience concernant l'ensemble de l'écosystème terrestre. Il s'agit de contenir le réchauffement climatique « bien en dessous de +2 °C par rapport aux niveaux préindustriels » et aussi de « renforcer la riposte mondiale à la menace des changements climatiques ». Il s'agit notamment de préparer une énergie décarbonée, qui remplacera l'énergie fossile coupable d'émissions de gaz à effet de serre, et ainsi de permettre la résilience de la Nature...

... À L'ADAPTATION AU CHANGEMENT NUMÉRIQUE

Certes, c'est l'or noir, le pétrole, qui a soutenu l'économie mondiale jusqu'à nos jours. Mais un autre or noir a propulsé l'Humanité dans une nouvelle dimension issue de la troisième révolution industrielle en cours : la donnée. La prochaine vague, la quatrième révolution industrielle attendue d'ici la fin du XXI^{ème} siècle, concernera le virtuel, qui déferle tel un tsunami constitué d'une combinaison de technologies comme l'intelligence artificielle, la robotique poussée à l'extrême, le calculateur quantique, les nanotechnologies et le génie génétique.

Ce monde à venir sera tributaire du numérique ainsi que de la technologie et consacrera la donnée comme la nouvelle matière première qui fait fonctionner l'écosystème socio-économique global.

Demain, l'écosystème planétaire sera totalement dépendant du digital.

Les technologies digitales pourraient considérablement améliorer la condition humaine, comme avant elles la force motrice et l'électricité l'ont fait. Mais elles sous-tendent inexorablement de nouveaux risques et de nouvelles menaces qu'il s'agit d'identifier, de reconnaître et de maîtriser.

LA RÉSILIENCE DANS LE CYBERESPACE

Ce monde virtuel, le cyberespace, s'apparente pourtant au monde physique. Dans le monde physique et réel, Homo Sapiens reconnait naturellement les menaces et s'en protège. Son système immunitaire porte les adaptations de centaines de milliers d'années. Il connaît les risques et s'en prémunit autant que possible.

Incontestablement, Homo Sapiens s'est doté d'une haute résilience dans ce monde terrestre. Mais dans le monde virtuel, ce cyberespace immature, Homo Sapiens n'a pas encore pu développer l'équivalent de son système immunitaire hérité de générations d'exploits et d'adaptations face à l'adversité. Il ne reconnait pas naturellement les menaces digitales de base et doit même encore apprendre les gestes élémentaires d'hygiène numérique.

Le second défi de l'Homme sera donc celui-là, fruit de la quatrième révolution industrielle qui s'amorce : développer sa haute résilience dans le monde digital, la Cyber-Résilience.

Cette Cyber-Résilience constitue le prérequis incontournable qui doit permettre à notre civilisation de se développer en toute confiance dans le cyberespace.

Dans un précédent Livre Blanc « Digital needs Trust », nous avons montré que le numérique requiert avant tout la confiance.

La Cyber-Résilience est la clé de la Cyber-Confiance, de la Cyber-Reliance.

L'Homme et la Résilience

LA RÉSILIENCE, CARACTÉRISTIQUE INNÉE DE L'HOMME

Depuis des millions d'années, l'Homme a su s'adapter en développant naturellement des parades et défenses pour assurer sa survie, dans un monde physique souvent hostile. C'est souvent de façon innée qu'il fait face aux menaces multiples, tout en mémorisant les bons scenarii de défense qui se transmettent au fil des générations. Homo Sapiens cristallise la synthèse de ces adaptations, fruits de ses capacités de résilience et d'agilité qui lui permettent de dominer la planète faisant de lui un expert ultra-adapté au monde réel.

Façonné par des siècles d'évolution darwinienne, l'Homme s'est réalisé - lentement mais sûrement - pour prendre le contrôle sur son environnement, élaborant les réponses adaptées aux menaces qui l'entourent. Ce champion de l'adaptation dispose d'un système de défense immunitaire autonome et complexe assurant sa survie et sa sécurité au service de son développement.

Si dans son environnement réel et physique, l'Homme peut compter sur une résilience et des mécanismes de protection naturels et innés, il n'en est pas de même sur son nouveau terrain de jeu, le cyberespace.

LA CYBER-RÉSILIENCE, DÉFI MAJEUR POUR L'HUMANITÉ

Au cours des dernières décennies, soit une infime fraction à l'échelle de l'évolution de l'humanité, l'Homme a conçu avec le numérique un nouveau territoire de création et de développement s'étendant inexorablement et de manière exponentielle. Le digital s'est imposé, apportant de nouveaux services devenus indispensables et irremplaçables. À tel point que nous nous interrogeons régulièrement sur le « comment faisait-on avant ? ». Aujourd'hui, comment se déplacer sans GPS ? Comment payer sans carte à puce ou sans smartphone ? Comment réserver un billet d'avion, travailler, communiquer, s'informer ou encore investir sans Internet ? Tout y passe, même les objets les plus matériels, emblématiques du XX^{ème} siècle, comme l'automobile, seront demain autonomes et deviendront des objets digitaux. Confrontées à une croissance de la population qui se concentre dans les villes, les mégalopoles « smart-cities » utiliseront la puissance du numérique pour réguler leurs infrastructures et leur sécurité. L'agriculture sera optimisée via le digital. Le monde bancaire et financier, déjà précurseur, se transformera encore par l'adoption massive de l'Intelligence Artificielle. L'industrie manufacturière, les secteurs de la distribution, la logistique... seront entièrement automatisés et robotisés. Chaque profession telle que journaliste, avocat, policier, chirurgien... sera bouleversée par un recours total ou partiel à des ressources cybernétiques.

LE CYBERESPACE EST DÉJÀ LE NOUVEL UNIVERS D'HOMO SAPIENS

Le cyberespace s'impose tellement rapidement qu'il constituera, à terme, l'univers central de l'humanité. Parallèle au monde physique, mais impalpable et virtuel, l'Homme devra s'y adapter rapidement. Dans cet univers, les menaces sont d'autant plus difficiles à appréhender qu'elles sont imperceptibles pour les cinq sens humains. Même protégé, le cyberespace demeure un environnement risqué faute de disposer d'un système de défense de type immunitaire.

Ainsi, face à son écran connecté sur le Net et plongé dans les réseaux sociaux, Homo Sapiens, dépourvu de capacités de détection des menaces numériques est une proie fragile et facile, incapable de détecter le danger. Ce champion de la maîtrise des menaces du monde réel, à la conquête du cyberespace, doit faire face à des menaces invisibles et inodores : virus, malwares divers, attaques, avec comme conséquences destruction, modification et vol de données, atteintes à la confidentialité des secrets de fabrication, des données clients, à la vie privée, etc.

Pour survivre, il est devenu nécessaire d'adopter de toute urgence les principes de base d'une hygiène numérique, prérequis parmi tant d'autres.

Menaces
18 mois

ACCES PRIVILEGIES EN VENTE

Une journaliste indienne du quotidien indien « The Tribune » a affirmé avoir eu besoin de dix minutes et 500 roupies (moins de 7 euros) versées à un inconnu rencontré sur WhatsApp, pour accéder à l'immense base de données gouvernementale « Aadhaar », rassemblant les informations personnelles et biométriques de près de 1,2 milliard de personnes.

Elle a obtenu pour 300 roupies supplémentaires, un logiciel censé permettre l'impression de cartes Aadhaar - le document qui prouve sa présence dans la base de données et peut servir de preuve d'identité - à partir de n'importe quel numéro entré dans la base.

Qui plus est, le site d'information indien « The Quint », de son côté, a affirmé peu après qu'il était possible d'acquérir des comptes administrateur sur la base de données, permettant de créer autant de comptes que souhaité, y compris d'autres comptes administrateur.

Source : The Tribune India - 04/01/2018

Source : Le Monde - 10/01/2018

FUITE DE DONNÉES

Comme le rapportait « Wired » suite à la découverte de cette fuite : « Vous n'avez probablement jamais entendu parler d'Exactis ! Pourtant, Exactis avait entendu parler de vous ». Cette firme de marketing, fournisseur de données, a laissé au grand jour 2 Tera de données d'une base ElasticSearch placée devant un firewall. La base contenait près de 340 millions d'enregistrements de données personnelles...

Source : Wired - 27/06/2018

multidimensionnelles
au coeur de la tempête

VOL DE DONNÉES

Equifax, une des plus importantes institutions de crédits aux USA, a été victime d'une brèche qui a pu affecter 143 millions de clients. Cette fuite de données est reconnue comme l'une des plus importantes de 2017, notamment en raison du caractère particulièrement sensible des données exposées, dont l'identité des clients ou des numéros de permis de conduire et de sécurité sociale.

Source : U.S. Security and Exchange Commission, SEC - incident du 07/09/2017

FAILLES DE SÉCURITÉ

Le fabricant de puce TSMC, Taiwan Semiconductor Manufacturing Company, a été victime d'un virus qui s'est propagé dans des systèmes obsolètes et il a fallu près de 3 jours avant de recouvrer une situation normale. En dehors des coûts engendrés, la société a averti que l'incident pouvait porter sur 3 pourcents des revenus de son 3ème trimestre et que des retards de fabrication pourraient être constatés jusqu'à la fin de l'année.

Source : TSMC - 05/08/2018

CRIMINALITÉ

Le rançongiciel WannaCry, qui a déferlé sur le globe en mai 2017, a violemment affecté des entreprises comme Vodafone, FedEx ou la Deutsche Bahn. Victime, le National Health Service anglais a été contraint d'annuler des milliers de rendez-vous médicaux entre le 12 et le 18 mai 2017.

Source : National Audit Office, NAO - 25/04/2018

MANIPULATION

Le vendredi 5 mai 2017, soit deux jours seulement avant le second tour de la Présidentielle française, le bureau d'En-Marche, parti de celui qui allait devenir Président de la République, Emmanuel Macron, a reconnu dans un communiqué avoir été « victime d'une action de piratage massive et coordonnée ». Ceci dans un seul et unique but : nuire au processus démocratique en diffusant des faux #MacronLeaks...

Source : En-Marche - 05/07/2017

ERREUR HUMAINE

Un prestataire de Verizon, Nice Systems, a exposé publiquement une base de données hébergée sur Amazon S3. En raison d'une erreur humaine, un listing de 14 millions de clients américains a malencontreusement été laissé libre de toute protection ou encryption. En décembre 2017, Verizon a affirmé que seul le chercheur d'UpGuard qui a mis la faille à jour a eu accès aux données et qu'aucun vol ou perte de données n'a été constaté.

Source : Verizon - 07/12/2017

ERREUR LOGICIELLE

Le 3 avril 2018, l'application de gestion du ciel européen composé de plus de 36.000 vols quotidiens a cessé de fonctionner chez EuroControl. C'est un lien incorrect entre le test d'une nouvelle version du logiciel et le système d'exploitation qui a généré l'événement déclencheur de l'incident. EuroControl a assuré qu'aucune ingérence extérieure n'était à la source de la panne.

Source : Eurocontrol - 03/04/2018

Hygiène **numérique**

Evoluer et utiliser l'espace digital comporte des risques. Tout comme dans le monde physique, pour augmenter ses chances de survie, il est primordial d'adopter une hygiène de vie numérique comprenant des bonnes pratiques, d'avoir une culture avisée du monde digital et de ses risques, d'acquérir de bons réflexes par une sensibilisation régulière des utilisateurs et des professionnels qui seuls permettent de limiter l'impact des menaces. Une prise de conscience rapide s'impose.

Il est étonnant de comparer l'écart de tolérance qui existe entre un service dans le monde réel et sa version numérique. Prenons l'exemple du service postal remplacé par l'e-mail.

Dans le monde physique, le service de courrier postal est payant. Il est opéré par des entreprises publiques qui sont des symboles de réputation. Au cinéma, Audiard, dialoguiste, scénariste et réalisateur français, faisait référence à cette vertu des PTT françaises (Postes, Télégraphes et Télécommunications) avec cette réplique confiée à Jean Gabin dans « Le cave se rebiffe » : « Nous allons confier notre petit trésor aux seuls gens qui n'égarent rien. Aux employés de cette administration que le monde entier nous envie : j'ai nommé les PTT ». Les services postaux jouissent d'une excellente réputation et leurs services d'horodatage (le tampon de la poste faisant foi) ou de recommandé admis et reconnus de tous sont au cœur du fonctionnement des mécanismes légaux. De plus, les lettres et colis acheminés fermés restent par défaut fermés. Les différentes postes assurent la protection de la confidentialité des informations transmises.

Par contre, dans le monde virtuel, les messageries et les réseaux sociaux sont gratuits. Les données des utilisateurs en sont la monnaie du droit d'usage. Les informations acheminées sont scrutées, scannées pour être analysées massivement de manière permanente par des algorithmes en vue d'une exploitation commerciale très rentable. Pourtant qui en a conscience ?

Que diriez-vous si dans le monde physique, le facteur ouvrait votre correspondance et l'analysait pour vous donner une publicité en rapport avec vos centres d'intérêts ou vos préoccupations, s'il entrait dans chaque domicile, ouvrait les tiroirs, les armoires, scannait le frigo, analysait chaque recoin de votre maison et de votre jardin afin d'en tirer les informations pour mieux vous connaître et pour mieux vous cibler ?

Ce type de comportement dans le monde physique ne serait évidemment pas toléré, ni de façon isolée et encore moins à grande échelle. Véritable scandale dans les démocraties, la presse s'en emparerait pour dénoncer l'ingérence de l'état et une atteinte aux libertés essentielles. Cela ferait l'objet de plaintes judiciaires.

Mais de toute évidence, certainement faute d'être en mesure de le percevoir dans le cyberespace, les utilisateurs se soumettent à cette mise à nu inconsciente.

Et il en est de même pour les précautions élémentaires de bon sens.

Qui dans le monde physique laisserait les portes et fenêtres de sa maison grandes ouvertes ? Ou sans système d'alarme opérationnel ?

Dans le cyberespace en revanche, de nombreux utilisateurs ne prennent aucune mesure pour se protéger contre des utilisations malveillantes ou pour garantir un minimum de protection de la vie privée. Ils vivent portes et fenêtres ouvertes, sans avoir conscience des dangers qui les entourent. Ce sont autant de vulnérabilités que savent détecter les cyber-délinquants, cyber-malveillants, cyber-malfaisants afin de les exploiter et de les monétiser.

Appliquer les mesures de protection et d'hygiène de base du monde physique dans le monde digital permettrait d'éviter 90% des cyber-attaques.

NAVIGUER DANS LE CYBERESPACE N'EST PAS SANS RISQUES

> **CELUI QUI A INVENTÉ LE BATEAU A AUSSI INVENTÉ LE NAUFRAGE**
>
> *Lao Tseu*

Il conviendrait d'élargir cette citation en n'oubliant pas que celui qui a inventé le navire a aussi inventé le voyage, l'aventure, les échanges, le commerce lointain, le rapprochement des peuples... mais attention, comme dans le monde physique, l'Humanité doit apprendre à naviguer sur les cyber-océans, à affronter les tempêtes et les risques, et à prévenir les naufrages.

Car l'histoire est en marche et la civilisation humaine de demain reposera totalement sur l'océan digital. Elle a besoin de cette technologie pour décupler ses capacités et ne doit pas jouer aux apprentis-sorciers pour autant.

Afin de profiter pleinement des nouvelles opportunités de l'économie numérique, il convient d'adopter une démarche active en matière d'identification des menaces, des vulnérabilités et d'évaluer les risques pour chaque activité. Car accidents, erreurs et malveillances peuvent se transformer en naufrage dans cet océan digital virtuel, qui aura en revanche des conséquences immédiates dans le monde réel.

Il s'agit donc de comprendre les risques, de les anticiper, de protéger les navires, et en cas de réalisation des risques, d'assurer le sauvetage.

Le développement du monde numérique n'en est qu'à ses débuts. À titre d'illustration, la part des données stockées et accessibles via les data centres ou le cloud public va être multipliée par 10 d'ici 2020, pour atteindre 44 zettabytes (44 trillions de GB).

Les années 2017 et 2018 ont mis à rude épreuve les systèmes informatiques et les professionnels de la Cyber-Sécurité. Des attaques DDoS massives et plusieurs épidémies de ransomwares ont perturbé les activités de nombreuses organisations internationales. Des entreprises et des particuliers se sont vus pris en otage, paralysés par des attaques malveillantes. Des processus électoraux au sein de pays démocratiques ont même été perturbés par des cyber-activistes aux intentions douteuses. 2017 et 2018 ont été des années charnières dans le mouvement de nos sociétés vers une ère numérique. La révélation du détournement de l'utilisation des données Facebook par Cambridge Analytica, la production industrielle et malveillante de « fakenews » à des fins de manipulation, tout ceci met en évidence les fragilités de nos organisations et les failles de nos sociétés de plus en plus digitales.

Ces nouvelles menaces peuvent être dévastatrices pour les Etats, les organisations, les entreprises et les citoyens. Elles portent sur des risques liés à la disponibilité, à la confidentialité ainsi qu'à l'intégrité des données. Elles revêtent différentes formes. Malveillance, défaillance, négligence, délinquance, déviance... sont autant de comportements ou de dysfonctionnements déjà présents dans le monde Cyber.

Aller plus loin que la Cyber-Sécurité

UNE PRISE DE CONSCIENCE NÉCESSAIRE

Mesurer les impacts financiers, humains, sociétaux, réputationnels et légaux des défaillances dans le monde digital justifie l'urgente nécessité d'une meilleure connaissance du monde digital et surtout du renforcement de sa sécurité et de sa résilience. Dans le monde numérique, chaque acteur, qu'il soit un Etat, une communauté, une entreprise, une organisation ou encore une personne privée, devrait disposer d'un cadre de confiance garanti. Il s'agit de bénéficier des atouts du numérique en toute sécurité sans compromettre ses activités.

Jusqu'à présent, les accidents, erreurs, failles et malveillances n'ont impacté que des biens. Demain, avec la généralisation du digital à tous les aspects de la vie quotidienne, des vies humaines pourraient être en jeu. La malveillance n'a de limite que l'imagination et la motivation des terroristes ou criminels.

L'importance de ces risques appelle à une prise de conscience de nos sociétés.

DANS LE CYBERESPACE, LE RISQUE EST CERTAIN

La question n'est plus de savoir si le monde digital va connaître des défaillances mais plutôt quand cela va-t-il arriver et quel sera l'impact à encaisser en fonction de la cible touchée : particuliers, entreprises, Etats... ?

Alors que l'homme a su développer ses capacités et déployer son ingéniosité avec l'aide de ses sens pour dompter son environnement physique, il va devoir redoubler de créativité pour appréhender le cyberespace. Les menaces y sont certaines et leurs impacts majeurs. Ne pas les identifier, les négliger ou les sous-estimer consiste à prendre un risque d'autant plus élevé que les systèmes d'informations sont imbriqués et inter-opérants. Ainsi, la conséquence sera d'autant plus élevée si le risque n'est pas anticipé, détecté et contenu. Il convient désormais d'acter que chaque organisation peut être touchée, directement ou indirectement, et qu'il faudra savoir résister, donc devenir cyber-résilient.

La résilience du monde digital actuel n'en est qu'à ses balbutiements.

La bonne nouvelle, c'est que des méthodologies et des outils existent. Le marché de la Cyber-Résilience, du fait du retard pris, est en plein développement et les innovations sont nombreuses. Que ce soient les Etats dans leur rôle de législateur, les fournisseurs de services IT qui opèrent les systèmes, les universités qui forment les ingénieurs IT, les entreprises qui utilisent le cyberespace ou les utilisateurs et clients, partout la prise de conscience s'opère... lentement.

Véritables centres de commandement, les CERT (Computer Emergency Response Team, ou centres de réponse aux urgences informatiques) et les SOC (Security Operations Center, ou centres opérationnels de la sécurité) sont au cœur du dispositif de défense.

QU'EST-CE QU'UN CERT ?

Également appelé CSIRT (Computer Security Incident Response Team), le Computer Emergency Response Team est un centre de compétences en charge des alertes et des réactions face aux cyber-attaques. Il concentre les demandes d'assistance suite aux incidents de sécurité, traite les alertes, établit et maintient une base de données des vulnérabilités, diffuse les informations sur les précautions à prendre pour minimiser les risques et assure la coordination avec les autres entités telles que les centres de compétences réseaux, opérateurs et fournisseurs d'accès Internet et les CSIRT nationaux et internationaux. En résumé, il accumule la connaissance au bénéfice d'une réactivité et d'une anticipation maximales.

QU'EST-CE QU'UN SOC ?

Le Security Operations Center est un dispositif de supervision des systèmes d'information dont le but est d'assurer la détection et l'analyse des incidents ainsi que de définir la stratégie de réponse à l'incident de sécurité. Ses experts analysent continuellement les événements remontés par le système, et identifient les potentiels risques en matière de Cyber-Sécurité.

Son objectif principal est d'assurer une surveillance 24h/24 et 7j/7 du système d'information.

LA DIRECTIVE NIS

La directive européenne N.I.S. (Security of Network and Information Systems) vise à renforcer considérablement la résilience de l'Europe digitale et à renforcer la confiance. Elle concerne tous les acteurs et plus particulièrement les « opérateurs de services essentiels », comme certains acteurs des secteurs de l'énergie, des transports, des banques, des infrastructures de marchés financiers, de la santé, de la fourniture et de la distribution d'eau potable, mais également les « fournisseurs de services numériques ».

Cette directive vise également à renforcer la Cyber-Résilience de l'Europe digitale.

Les opérateurs de services essentiels ainsi que les places de marché en ligne, les moteurs de recherche et les services cloud seront donc soumis à de nouvelles exigences de sécurité et de notifications d'incidents. Le but ? Assurer un niveau élevé de sécurité des réseaux et des systèmes d'information commun à toute l'Union européenne.

Et si sécurité rime avec confiance, cette dernière sera renforcée grâce à cette directive qui prévoit qu'un réseau international de CSIRT/CERT (Computer Security Incident Response Team/Computer Emergency Response Team) soit établi. Il s'agit ainsi de contribuer au renforcement de la confiance entre les États membres et de promouvoir une coopération opérationnelle rapide et effective.

LE RÔLE ESSENTIEL DE L'ENISA

Par ailleurs, le Parlement européen et le Conseil de l'Europe ont conjointement convenu en septembre 2017 de doter l'UE d'une « Cyber-Sécurité solide » en s'appuyant sur des mesures de résilience, de dissuasion et de défense. En dehors des efforts visant à promouvoir la Cyber-Sécurité dans les États membres et dans les institutions ainsi que les agences et les organes de l'Union, l'Europe établit également une stratégie plus exigeante en matière de Cyber-Résilience. Cette stratégie dote l'ENISA (l'Agence européenne chargée de la sécurité des réseaux et de l'information) d'un mandat permanent et élargi pour renforcer la Cyber-Résilience et la capacité de réaction de l'UE face aux enjeux du cyberespace. « Un rôle essentiel à jouer dans le renforcement de la Cyber-Résilience et de la réaction de l'UE », indiquent le Parlement européen et le Conseil de l'Europe.

L'ENISA, en collaboration avec les organes compétents nationaux, et notamment le réseau des CSIRT/CERT, le CERT-UE, Europol et l'INTCEN (le Centre de renseignement et de situation de l'UE), contribuera à améliorer le cadre effectif de la Cyber-Résilience européenne, principalement dans le suivi régulier du paysage des menaces, et dans la réaction aux incidents transfrontaliers à grande échelle.

LA CYBER-
UN NOUVEAU

Préparer | Identifier

L'utilisation exponentielle du digital, son rôle central dans l'économie et la dépendance des moyens vitaux pour les sociétés humaines et les entreprises, font du cyberespace une zone exposée, cible potentielle privilégiée d'attaques. L'augmentation fulgurante des menaces digitales en est la preuve et a pour conséquence d'élever considérablement les niveaux de risque. L'ensemble des usagers du cyberespace sont vulnérables, 100% connaîtront un incident tôt ou tard.

Il est vital d'intégrer ce changement de paradigme : dans le cyberespace, la réalisation du risque Cyber est certaine pour tous les acteurs. L'accepter doit conduire chaque acteur à mieux anticiper, se défendre, se préparer à absorber le choc, réagir à toute éventualité et rebondir.

RÉSILIENCE PARADIGME

Protéger | Détecter | Analyser | Répondre | Récupérer

Dans ce contexte, la Cyber-Sécurité centrée sur la protection des données montre clairement ses limites, même si elle reste importante et représente un « minimum vital ». Trop restrictive, la Cyber-Sécurité doit être renforcée par une approche globale et totalement intégrée : la Cyber-Résilience.

La Cyber-Résilience se veut holistique et systémique, proactive et en auto-apprentissage, dans un monde digital qui devient de plus en plus complexe. Personnalisable, elle doit être intégrée aux enjeux organisationnels et business.

Il s'agit d'aller au-delà d'une stratégie de pure défense et de gérer les risques naturellement, « by design », dans un mode « business as usual », face à des menaces changeantes et adaptatives, tout comme le système immunitaire le fait pour protéger le corps humain.

> *Par rapport aux révolutions précédentes, la révolution digitale a ceci de plus pernicieux que la ressource n'est ni tangible ni a priori limitée, dès lors elle est plus difficile à appréhender et à maîtriser.*

VERS LA CYBER-IMMUNITÉ...

La Cyber-Résilience est une méthodologie qui doit devenir une culture ayant pour objectif de constamment pouvoir préparer, identifier, protéger, détecter, analyser, répondre et récupérer suite aux incidents et menaces, restaurer les systèmes et les processus pour garantir la continuité de l'activité, donc de récupérer même après un impact. Il s'agit de développer, pour chaque activité dépendant du numérique, un système immunitaire performant. Pour qu'il soit efficient, il faut que les différentes composantes de l'organisation interagissent de manière coordonnée, selon une approche systémique.

Il s'agit de s'inspirer de la nature et d'utiliser le biomimétisme pour concevoir un système de défense digital disposant des mêmes vertus.

Ce système de défense cyber-immunitaire protégera le cyberespace, communiquera et se mobilisera face aux menaces. Il devra apprendre de son environnement et donc évoluera et s'améliorera en permanence.

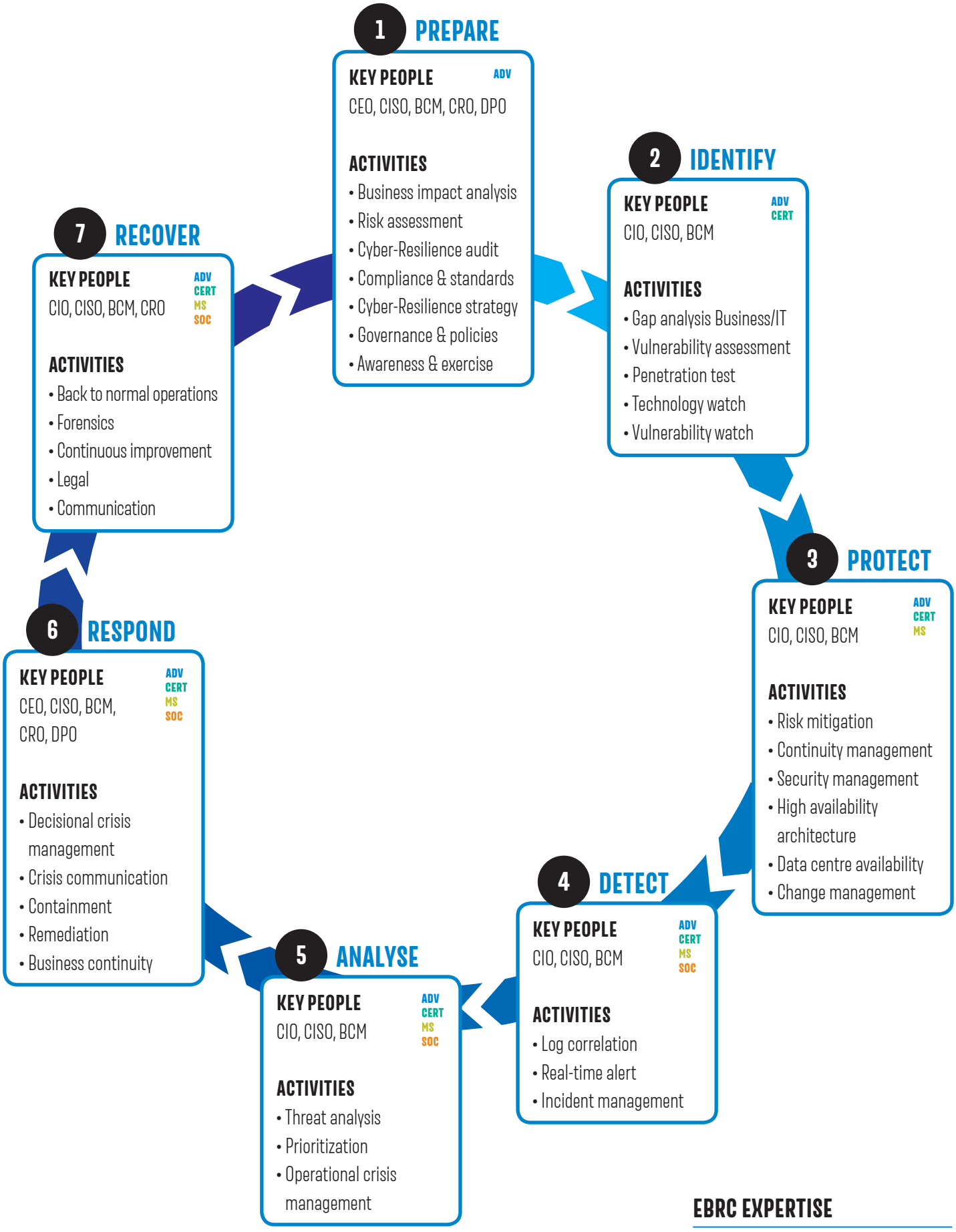
LA CYBER-RÉSILIENCE DANS VOTRE ORGANISATION

Assurer la continuité de votre business

LES POINTS CLES DE LA CYBER-RÉSILIENCE :

- Connaître et respecter le cadre règlementaire : RGPD, NIS, autorités de contrôle (finance, assurance, transport, santé…)
- Adopter les standards internationaux pour la gestion des risques et la résilience des activités : ISO 31000, ISO 27001, ISO 27018, ISO 27032, ISO 22301, ISO 22316
- Adopter et/ou imposer à ses fournisseurs de services le niveau de sécurité et de continuité approprié sur la base de certifications : Data Centre Tier IV, PCI DSS, HDS (Hébergeur de Données de Santé), ISO 27001, ISO 22301
- Concevoir ou transformer les infrastructures existantes en adoptant une conception intégrant la "Security and privacy by design" : Proxy, Firewall, Anti-virus, Anti-DDoS, Mail security, Sandboxing, IPS/IDS, WAF
- Sensibiliser, former et informer en continu l'ensemble des collaborateurs et les parties prenantes à la Cyber-Résilience
- Arbitrer sur la capacité de l'entreprise à déployer ces moyens ou opter pour un partenaire en mesure d'accompagner la mise en œuvre de la Cyber-Résilience : audit, conseil, risk management, continuité d'activités, data centres certifiés, gestion opérationnelle et intégrée de la sécurité (SOC/CERT), gestion des infrastructures IT, programmes de certification…

AMÉLIORATION CONTINUE



EBRC EXPERTISE

ADV – ADVISORY
CERT – COMPUTER EMERGENCY RESPONSE TEAM
MS – MANAGED SERVICES
SOC – SECURITY OPERATION CENTER

Un secteur financier **cyber-résilient**

LA BCE ÉMET UNE GUIDANCE EN FAVEUR DE LA CYBER-RÉSILIENCE

Parce qu'il est au cœur de l'économie, le secteur financier est un pilier indispensable de la croissance mondiale du monde moderne. Porteuse de la confiance entre les systèmes, les états, les entreprises et les individus, la finance se doit d'être résiliente par définition. Les règles internationales, notamment celles arrêtées par le Comité de Bâle, visent sans cesse à renforcer la stabilité du secteur.

Mais un nouveau type de risques s'est insinué au fil de l'adoption technologique, et la cyber-dépendance a forcé le secteur à garantir le fonctionnement d'un numérique devenu vital. Récemment, la Banque Centrale Européenne a émis une guidance portant sur la prise en compte de la Cyber-Résilience des infrastructures de marché. Celle-ci pose un nouveau jalon pour le secteur et va établir la norme de demain.

Au cœur du secteur financier, les infrastructures de marché (les FMI's) telles que les systèmes de paiement interbancaires, de contrepartie centrale ou de règlement-livraison de titres, ont un rôle systémique qui nécessite la capacité à pouvoir se détacher de risques vitaux, estime la BCE. Constatant également que le paysage des menaces cyber devient de plus en plus sombre, la BCE a préparé des recommandations à ces FMI's qui, après consultation publique, devront consacrer les efforts nécessaires à améliorer leur Cyber-Résilience.

Dans son rapport CROE (Cyber Resilience Oversight Expectations), l'autorité européenne donne trois niveaux de maturité à la Cyber-Résilience : de base, intermédiaire et avancé. Pour chacun de ces stades, la Banque Centrale établit un cadre de conformité et d'actions pluridisciplinaires. Car la Cyber-Résilience ne se borne pas à éclairer les risques liés au numérique, mais à mettre en abîme l'entreprise sur sa capacité à poursuivre ses activités contre les vents et marrées du digital. Les attentes de la BCE portent ainsi sur la capacité des FMI's à se doter de la gouvernance, des capacités d'identification, de mesures de protection, d'aptitudes de détection et de solutions de réponse et de recouvrement après cyber-crise. Le document détaille également les attentes en matière de simulation, de conscientisation, d'amélioration, de communication et d'apprentissage continus.

La Banque Centrale Européenne ne s'est pas arrêtée là, puisqu'elle a, dans la foulée, publié un cadre européen pour tester cette résilience après des cyber-attaques. Elargi à tout le secteur, le TIBER-EU (Threat Intelligence-based Ethical Red Teaming), dispose aussi d'implémentations nationales volontaires par les pays de la zone Euro.

Ces lectures très importantes pour les organes de direction des entreprises concernées préparent sans conteste le terrain pour demain : de la Cyber-Résilience à la Cyber-Reliance.

Sources : Cyber Resilience Oversight xpectations (CROE) For Financial Market Infrastructures", European Central Bank, avril 2018.
"TIBER-EU Framework : How to implement the European framework for Threat Intelligence-based Ethical Red Teaming", European Central Bank, mai 2018.

L'Europe active **dans la Cyber-Résilience**

Fin 2017, la Commission européenne a décidé de renforcer le mandat de l'ENISA (European Union Agency for Network and Information Security) afin d'en faire une véritable agence de Cyber-Sécurité de l'Union européenne. L'ENISA organise régulièrement des exercices de Cyber-Résilience appelés « Cyber Europe », à l'échelle du continent européen. En 2016 par exemple, elle a organisé un exercice portant sur les « Clouds providers » et les « Internet Service Providers ». En 2018, l'exercice « Cyber Europe 2018 » a ciblé le domaine de l'aviation et a touché directement les autorités de l'aviation civile, les fournisseurs de services du secteur (ANSPs, Air Navigation Service Providers), les sociétés aéroportuaires, ou encore les transporteurs aériens.

DES NORMES INTERNATIONALES CONVERGENTES

La Cyber-Résilience est une approche intégrée regroupant analyse des risques, Cyber-Sécurité, continuité d'activités, gestion de crise et organisation de la résilience.

Pour supporter les acteurs dans cette démarche visant à optimiser leur degré de protection, les organisations internationales et autorités publiques prônent le développement et le respect de normes toujours plus poussées telles que : ISO 27001 (gestion de la sécurité de l'information), 20000 (gestion des services informatiques), 27018 (protection des données à caractère personnel) ou 22301 (gestion de la continuité d'activités). Ainsi, la nouvelle norme française d'Hébergeur de Données de Santé à caractère personnel (HDS) mise en application depuis 2018 exige les normes ISO 27001, 20000 et 27018.

Par ailleurs, en mars 2017 a également été publié le nouveau standard « Organisation de la résilience », qui se définit comme « la capacité d'une organisation à absorber et à s'adapter à un environnement changeant ».

La Cyber-Résilience est couverte par les référentiels internationaux suivants :

ISO 31000, qui définit le cadre de la gestion des risques
ISO 27001, qui couvre le système de gestion de la sécurité de l'information (ISMS)
ISO 22301, qui couvre le système de gestion de la continuité (BCMS)
ISO 22316, le nouveau standard « organisation de la résilience »

Cyber-Résilience = ISO 31000 + ISO 27001 + ISO 22301 + ISO 22316

Les cyber-risques sont aujourd'hui multidimensionnels. Or, le niveau de protection des données est déterminé par le point le plus faible de la chaîne de protection. La Cyber-Résilience est une approche globale et systématique qui vise à assurer une protection équilibrée et homogène. Elle repose sur deux piliers majeurs : l'approche « Business Continuity Management » (ISO 22301) et « Information Security Management » (ISO 27001). D'autres normes, comme la norme PCI DSS portant sur les paiements, permettent encore de renforcer la Cyber-Résilience.

Les normes et certifications **trois normes clés**

BUSINESS CONTINUITY MANAGEMENT - 22301

Sécurité sociétale - Systèmes de management de la continuité d'activité - Exigences

ISO 22301 spécifie les exigences pour planifier, établir, mettre en place et en œuvre, contrôler, réviser, maintenir et améliorer de manière continue un système de management documenté afin de se protéger des incidents perturbateurs, réduire leur probabilité de survenance, s'y préparer, y répondre et de s'en rétablir lorsqu'ils surviennent. *Source : ISO.org*

MANAGEMENT DE LA SÉCURITÉ DE L'INFORMATION - 27001

Technologies de l'information - Techniques de sécurité - Systèmes de management de la sécurité de l'information – Exigences

ISO 27001 spécifie les exigences relatives à l'établissement, à la mise en œuvre, à la mise à jour et à l'amélioration continue d'un système de management de la sécurité de l'information dans le contexte d'une organisation. Elle comporte également des exigences sur l'appréciation et le traitement des risques de sécurité de l'information, adaptées aux besoins de l'organisation. *Source : ISO.org*

PCI DSS NORME DE SÉCURITÉ DES DONNÉES

La Norme de sécurité de l'industrie des cartes de paiement (PCI DSS) a été développée dans le but d'encourager et de renforcer la sécurité des données du titulaire ainsi que pour faciliter l'adoption de mesures de sécurité uniformes à l'échelle mondiale. La norme PCI DSS sert de référence aux conditions techniques et opérationnelles conçues pour protéger les données du titulaire. La norme PCI DSS s'applique à toutes les entités impliquées dans le traitement des cartes de paiement, notamment les commerçants, les entreprises de traitement, acquéreurs, émetteurs et prestataires de services, ainsi qu'à toutes les autres entités qui stockent, traitent ou transmettent des données du titulaire (CHD) et/ou des données d'identification sensibles (SAD). *Source : PCI Security Standards Council*

VERS LA CYBER-RELIANCE

LE DIGITAL REQUIERT LA CYBER-RÉSILIENCE

La troisième révolution industrielle en cours connait des mouvements similaires à ceux qui ont agité, en leur temps, les première et seconde révolutions industrielles, à savoir l'apparition de régulations qui visent à encadrer l'exploitation des ressources.

Fin du XVIII^{ème} et du XIX^{ème}, aux yeux des principaux acteurs des deux premières révolutions industrielles, les ressources de la planète étaient considérées comme publiques, à disposition et sans limites.

Début du XXI^{ème} siècle, l'Humanité doit faire face à l'un de ses plus grands défis : gérer les effets de bord de l'exploitation massive des ressources fossiles à la base de l'accélération de la civilisation humaine. Ces effets de bord non désirés étaient prévisibles et sont aujourd'hui concrets avec le réchauffement climatique accéléré.

L'enjeu est colossal pour notre civilisation et pourrait mettre en péril nos modèles économiques et modèles de sociétés, mais aussi menacer la survie de nombreuses espèces, dont celle de l'Homme et par conséquent de notre civilisation. Ce défi ne pourra être relevé que grâce à un programme de résilience global, planétaire.

La troisième révolution industrielle ainsi que la quatrième vont, courant du XXI^{ème} siècle, faire basculer la civilisation dans un nouveau monde virtuel. La dépendance de la civilisation humaine au digital sera très poussée.

Les acteurs socio-économiques qui se ruent aujourd'hui dans le cyberespace n'ont pas encore acquis les réflexes de protection élémentaires qu'ils appliquent pourtant naturellement dans le monde physique...

Il est aujourd'hui vital et urgent pour tous les acteurs de développer une approche de Cyber-Résilience afin de protéger la donnée, matière première du XXI^{ème} siècle. En effet, le risque est inhérent au cyberespace. Dans celui-ci, le risque est certain. Il nous concerne tous, les Etats, les associations, les communautés, les organisations, les entreprises, les citoyens.

Dans ce cyberespace, dans le monde digital en cours de construction, devenir capable en permanence de prévenir, d'identifier les menaces, de se préparer, d'identifier, de protéger, de détecter, d'analyser, de répondre et de récupérer, tel est notre challenge.

Par analogie avec le monde physique, l'enjeu consiste à concevoir pour le cyberespace un système immunitaire qui assure par nature et « by design » la couverture de l'ensemble des activités et opérations qu'il traite quotidiennement en mode « business as usual. »

La Cyber-Résilience dans le monde digital **constitue le second défi de l'Humanité, d'ici la moitié du XXI^{ème} siècle.**

POUR RELEVER CE DÉFI DE LA CYBER-RÉSILIENCE, NOS EXPERTS SONT À VOTRE ÉCOUTE

Contactez-nous :
www.ebrc.com/contact

Consultez notre page Cyber-Resilience
www.ebrc.com/fr/offre/cyber-resilience

CYBER-RESILIENCE
DIGITAL NEEDS TRUST

ebrc

TRUSTED DATACENTRE, CLOUD & MANAGED SERVICES

5, rue Eugène Ruppert
L-2453 Luxembourg

www.ebrc.com/contact