CYBER-RESILIENCE
DANS LE SECTEUR BANCAIRE
DE DEMAIN

Bharathi KICHENAMOURTY

Frédéric GUILLARD

Moussa TIMERA

Saida MEDJDOUB

Sébastien CUVELIER

Février 2023

EGE Ecole de Guerre Economique

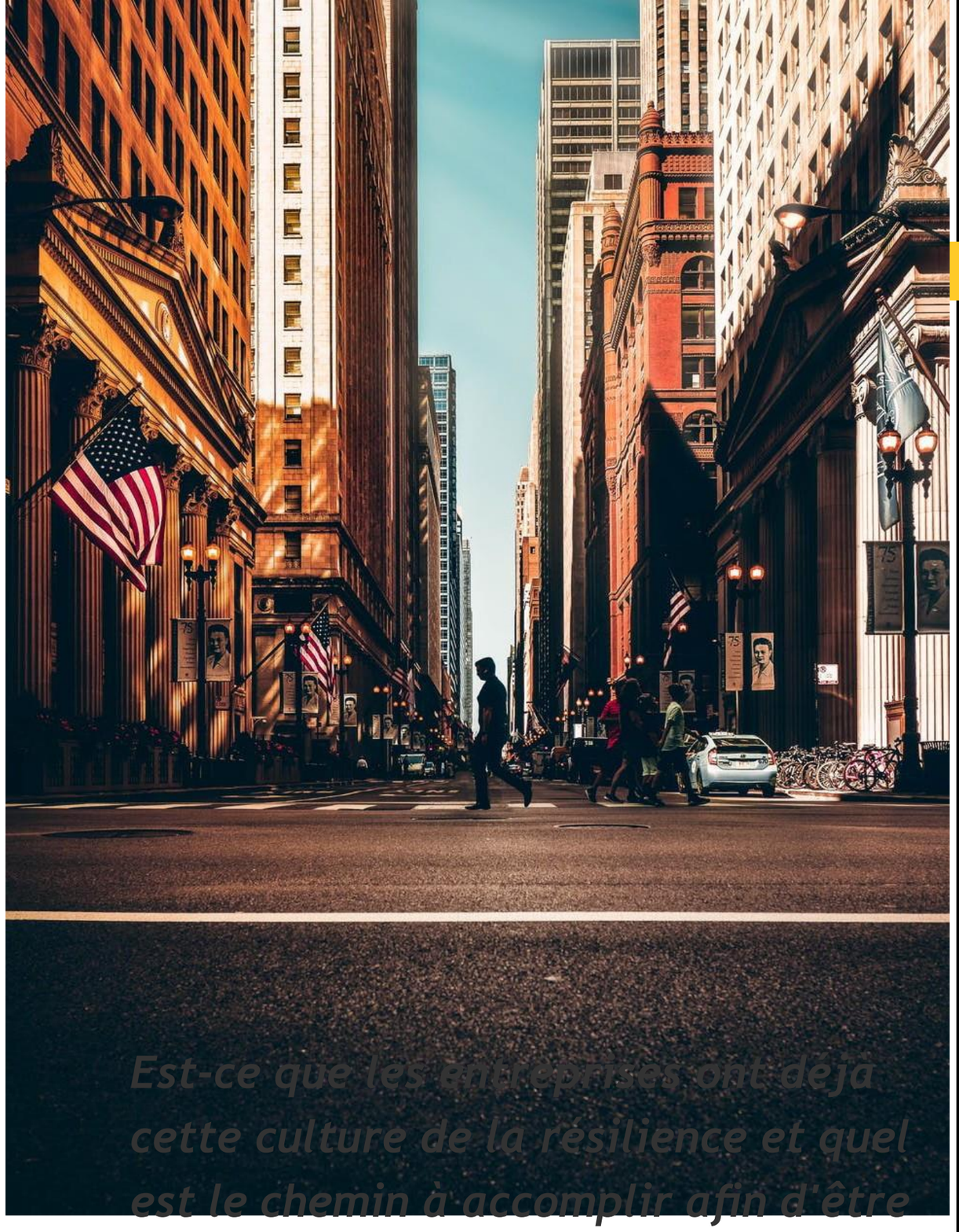
Sommaire

EGE Ecole de Guerre Economique

PARTIE 1

De la résilience du secteur bancaire à la cyber résilience

EGE Ecole de Guerre Economique



Est-ce que les entreprises ont déjà cette culture de la résilience et quel est le chemin à accomplir afin d'être pleinement engage dans une politique de Cyber résilience ?

DE LA RÉSILIENCE DU SECTEUR BANCAIRE À LA CYBER RÉSILIENCE

Si l'on se réfère à la définition du National Institute of Standards and Technology dépendant du Ministère du commerce US, la Cyber résilience est : La capacite à anticiper, à résister, à reconstruire à partir d'un point donné et à s'adapter à des conditions défavorables tel que des attaques, des compromissions sur des systèmes informatique.

La cyber-résilience est une approche plus large englobant la cybersécurité et la gestion de la continuité d'activité. Elle vise à se défendre contre les cyberattaques potentielles et à assurer la survie de l'entreprise à la suite d'une attaque.

Sans prétendre que cette définition prévaut sur une autre, elle a le mérite de résumer en une phrase les points importants à prendre en compte dans ce domaine : Protéger, Contenir, Relancer et Apprendre de nos expériences afin de s'améliorer continuellement et être en mesure d'augmenter la maturité d'une entreprise face aux Cyber attaques.

1.1 Résilience dans le secteur bancaire

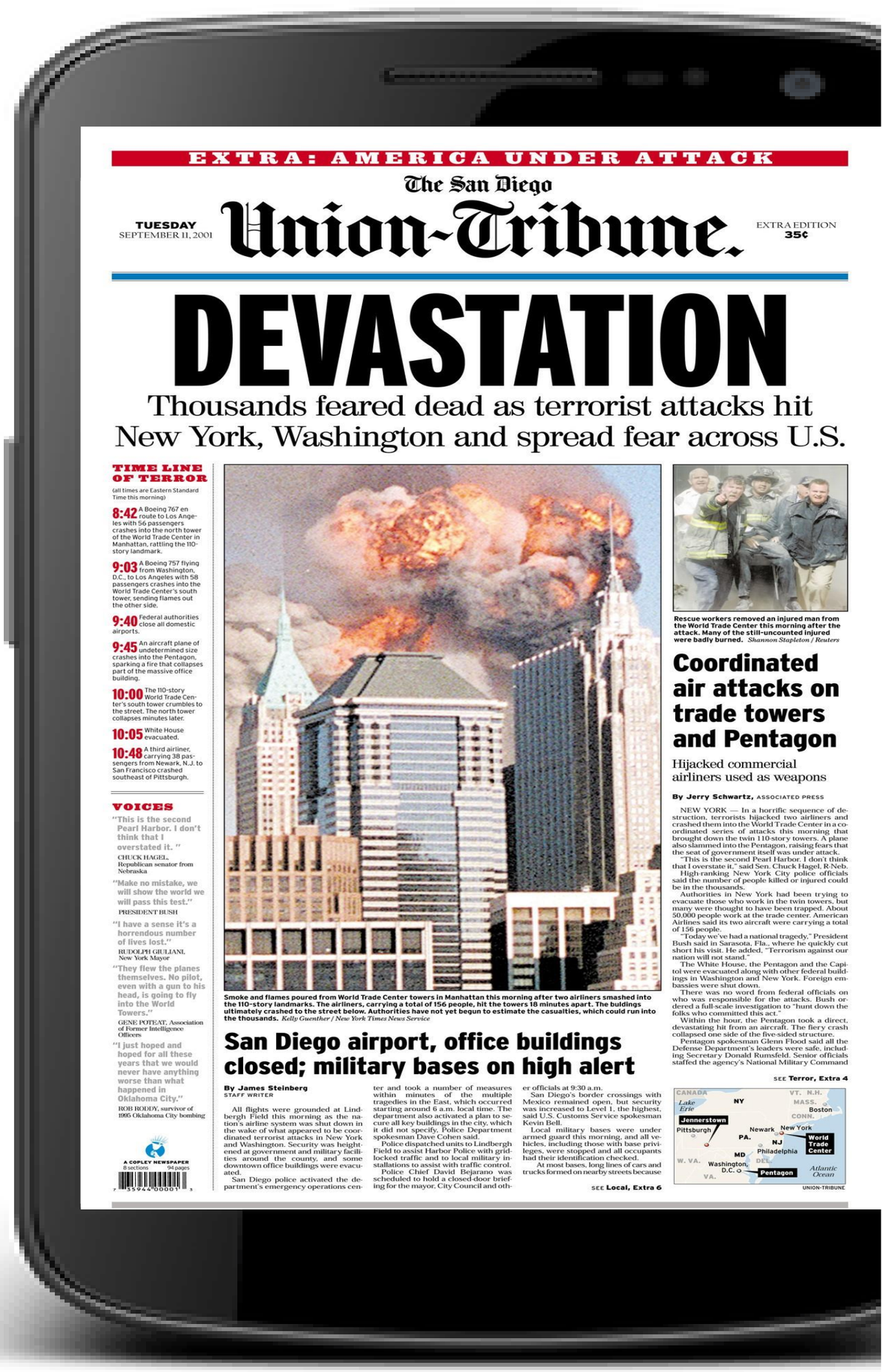
La résilience n'est pas une pratique récente dans le monde de la finance. Elle a pour objectif de s'assurer que les établissements financiers respectent leurs obligations règlementaires vis-à-vis des autorités de marché (AMF, SEC, ...) et contractuelles vis-à-vis de leurs clients.

Elle a pour objectif, à l'échelle du secteur, de contenir les effets d'un incident systémique et un risque d'emballement pouvant aboutir à une crise économique.

Les industries bancaires et financières font partie des secteurs vitaux pour l'économie d'un pays et l'augmentation des échanges entre pays/économies a accru le besoin de renforcer la résilience dans cette industrie.

Deux évènements majeurs aux Etats Unis illustrent parfaitement la prise de conscience collective sur l'importance de la résilience et ont réellement été un tournant dans l'amélioration des organisations à faire face à des événements extrêmes et à augmenter leur maturité dans ce domaine :

- Les attentats du 11 Septembre 2001,
- L'ouragan Sandy le 29 octobre 2012.



EXTRA: AMERICA UNDER ATTACK

The San Diego Union-Tribune.

TUESDAY SEPTEMBER 11, 2001 — EXTRA EDITION 35¢

DEVASTATION

Thousands feared dead as terrorist attacks hit New York, Washington and spread fear across U.S.

TIME LINE OF TERROR

(all times are Eastern Standard Time this morning)

8:42 A Boeing 767 en route to Los Angeles with 56 passengers crashes into the north tower of the World Trade Center in Manhattan, rattling the 110-story landmark.

9:03 A Boeing 757 flying from Washington, D.C., to Los Angeles with 58 passengers crashes into the World Trade Center's south tower, sending flames out the other side.

9:40 Federal authorities close all domestic airports.

9:45 An aircraft plane of undetermined size crashes into the Pentagon, sparking a fire that collapses part of the massive office building.

10:00 The 110-story World Trade Center's south tower crumbles to the street. The north tower collapses minutes later.

10:05 White House evacuated.

10:48 A third airliner, carrying 38 passengers from Newark, N.J. to San Francisco crashed southeast of Pittsburgh.

VOICES

"This is the second Pearl Harbor. I don't think that I overstated it."
CHUCK HAGEL, Republican senator from Nebraska

"Make no mistake, we will show the world we will pass this test."
PRESIDENT BUSH

"I have a sense it's a horrendous number of lives lost."
RUDOLPH GIULIANI, New York Mayor

"They flew the planes themselves. No pilot, even with a gun to his head, is going to fly into the World Towers."
GENE POTEAT, Association of Former Intelligence Officers

"I just hoped and hoped for all these years that we would never have anything worse than what happened in Oklahoma City."
ROB RODDY, survivor of 1995 Oklahoma City bombing

A COPLEY NEWSPAPER
8 sections 94 pages

Smoke and flames poured from World Trade Center towers in Manhattan this morning after two airliners smashed into the 110-story landmarks. The airliners, carrying a total of 156 people, hit the towers 18 minutes apart. The buildings ultimately crashed to the street below. Authorities have not yet begun to estimate the casualties, which could run into the thousands. *Kelly Guenther / New York Times News Service*

Rescue workers removed an injured man from the World Trade Center this morning after the attack. Many of the still-uncounted injured were badly burned. *Shannon Stapleton / Reuters*

Coordinated air attacks on trade towers and Pentagon

Hijacked commercial airliners used as weapons

By Jerry Schwartz, ASSOCIATED PRESS

NEW YORK — In a horrific sequence of destruction, terrorists hijacked two airliners and crashed them into the World Trade Center in a coordinated series of attacks this morning that brought down the twin 110-story towers. A plane also slammed into the Pentagon, raising fears that the seat of government itself was under attack.

"This is the second Pearl Harbor. I don't think that I overstate it," said Sen. Chuck Hagel, R-Neb.

High-ranking New York City police officials said the number of people killed or injured could be in the thousands.

Authorities in New York had been trying to evacuate those who work in the twin towers, but many were thought to have been trapped. About 50,000 people work at the trade center. American Airlines said its two aircraft were carrying a total of 156 people.

"Today we've had a national tragedy," President Bush said in Sarasota, Fla., where he quickly cut short his visit. He added, "Terrorism against our nation will not stand."

The White House, the Pentagon and the Capitol were evacuated along with other federal buildings in Washington and New York. Foreign embassies were shut down.

There was no word from federal officials on who was responsible for the attacks. Bush ordered a full-scale investigation to "hunt down the folks who committed this act."

Within the hour, the Pentagon took a direct, devastating hit from an aircraft. The fiery crash collapsed one side of the five-sided structure.

Pentagon spokesman Glenn Flood said all the Defense Department's leaders were safe, including Secretary Donald Rumsfeld. Senior officials staffed the agency's National Military Command

SEE Terror, Extra 4

San Diego airport, office buildings closed; military bases on high alert

By James Steinberg
STAFF WRITER

All flights were grounded at Lindbergh Field this morning as the nation's airline system was shut down in the wake of what appeared to be coordinated terrorist attacks in New York and Washington. Security was heightened at government and military facilities around the county, and some downtown office buildings were evacuated.

San Diego police activated the department's emergency operations center and took a number of measures within minutes of the multiple tragedies in the East, which occurred starting around 6 a.m. local time. The department also activated a plan to secure all key buildings in the city, which it did not specify. Police Department spokesman Dave Cohen said.

Police dispatched units to Lindbergh Field to assist Harbor Police with gridlocked traffic and to local military installations to assist with traffic control.

Police Chief David Bejarano was scheduled to hold a closed-door briefing for the mayor, City Council and other officials at 9:30 a.m.

San Diego's border crossings with Mexico remained open, but security was increased to Level 1, the highest, said U.S. Customs Service spokesman Kevin Bell.

Local military bases were under armed guard this morning, and all vehicles, including those with base privileges, were stopped and all occupants had their identification checked.

At most bases, long lines of cars and trucks formed on nearby streets because

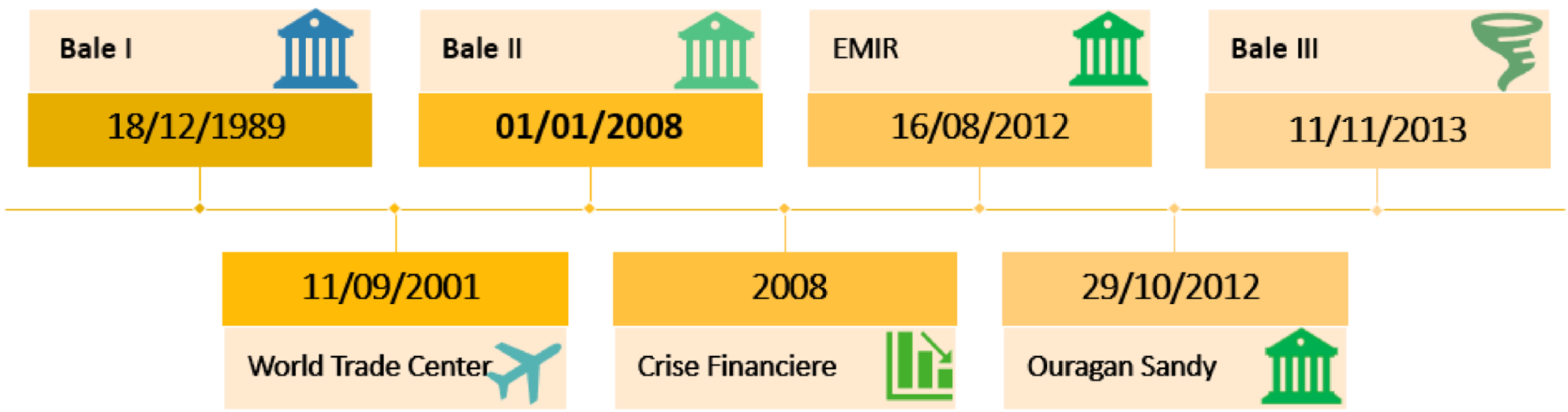
SEE Local, Extra 6

UNION-TRIBUNE

Ces deux évènements qui ont entrainé la fermeture de Wall Street pendant quelques jours (du jamais vu depuis 1929), ont eu une forte résonnance dans l'industrie et ont conduit les entreprises a :

- Renforcer la réponse à un incident via la mise en place d'un plan de gestion de crise au sein des entreprises,
- Prévoir les moyens matériels nécessaires afin de gérer une reprise d'activité graduellement. Exemple : Immeuble de replis pour le staff à distance requise de l'immeuble principal tel que préconisé par la FFIEC (Federal Financial Institutions Examination Council),
- Réaliser des tests de résilience avec les acteurs de marché (tests de place),
- Améliorer les plans de continuité d'activité des entreprises, Business Continuity Management, et dans ce cadre réaliser des analyses de risques sur les activités métiers critique, BIA (Business Impact Analysis) et sur la façon dont elles sont opérées.

Chronologie des évènements marquant dans le secteur de la Finance



Il n'est pas possible de parler de résilience dans le domaine de la finance sans parler des accords de Bâle et de ses différentes évolutions au fil du temps.

Ces accords avaient et ont toujours pour objectif de renforcer la résilience de chaque établissement bancaire et, à l'échelle de l'ensemble du secteur financier, en les soumettant à une batterie de tests afin d'éviter tout effet collatéral majeur sur l'économie si un acteur majeur faisait défaut (le cas Lehman Brothers), en les obligeant à avoir en réserve un montant suffisant de fonds propres à même de se prémunir d'un emballement.

La crise financière de 2008 a montré les limites des premiers accords mais le cercle vertueux de l'autorégulation était enclenché dans ce secteur.

La mise en place de stress tests sur l'ensemble du secteur, afin de qualifier la résistance des banques à des changements macroéconomiques et microéconomiques a été une évolution importante et a permis aux banques non résilientes aux tests de définir des plans d'actions afin de renforcer leur capacité de défense via une augmentation des fonds propres ou à une restructuration de leurs activités.

Le dernier exemple à apporter dans le domaine de la résilience porte plutôt sur la capacité à innover et à s'adapter dans un secteur fortement règlementé.

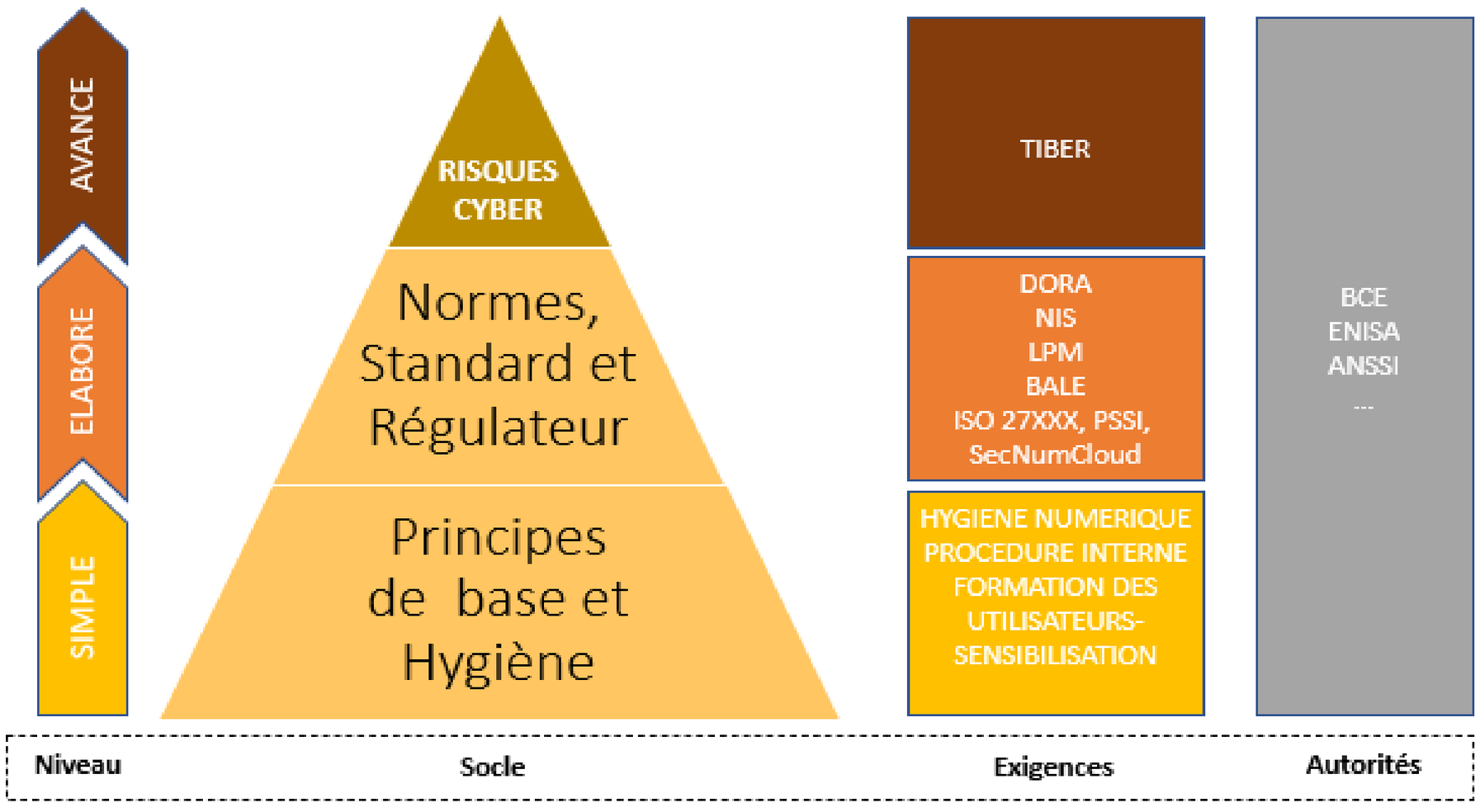
À la suite de la crise de 2008, la commission Européenne, via la directive EMIR, a imposé aux gestionnaires d'actifs ayant en portefeuille des produits OTC, de faire appel à des tiers afin de les contre valoriser. Ce surcoût opérationnel d'un côté a conduit l'industrie financière à créer de nouveaux services afin de répondre à ce nouveau besoin.

Une contrainte peut en définitive se transformer en opportunité pour le métier et être créatrice de valeur.

La digitalisation des marchés et de ces acteurs institutionnels a apporté des gains de productivité, une diminution des erreurs opérationnelles, de la transparence dans les échanges boursiers et bancaires mais a introduit de nouveaux risques liés aux failles de sécurité et aux erreurs humaines.

1.2 Cyber résilience dans le secteur bancaire

La cyber résilience est la continuité du tournant opéré dans la résilience dans le secteur bancaire et financier afin de faire face à des nouveaux type d'"attaques" dans le monde virtuel.



Comment les entreprises vont-elles s'adapter aux règlementations ?

Est-ce que la maturité actuelle des entreprises, qu'elles soient classées OIV et soumises à la LPM, ou identifiées comme OSE réglementées par la NIS, va permettre une transition rapide grâce aux solides fondations existantes ?

- Principe de base et hygiène,
- Cadre règlementaire et normatif,
- Appréciation des risques numériques.

Est-ce que ces contraintes vont amener des transformations structurelles dans l'industrie et des nouvelles opportunités business ?

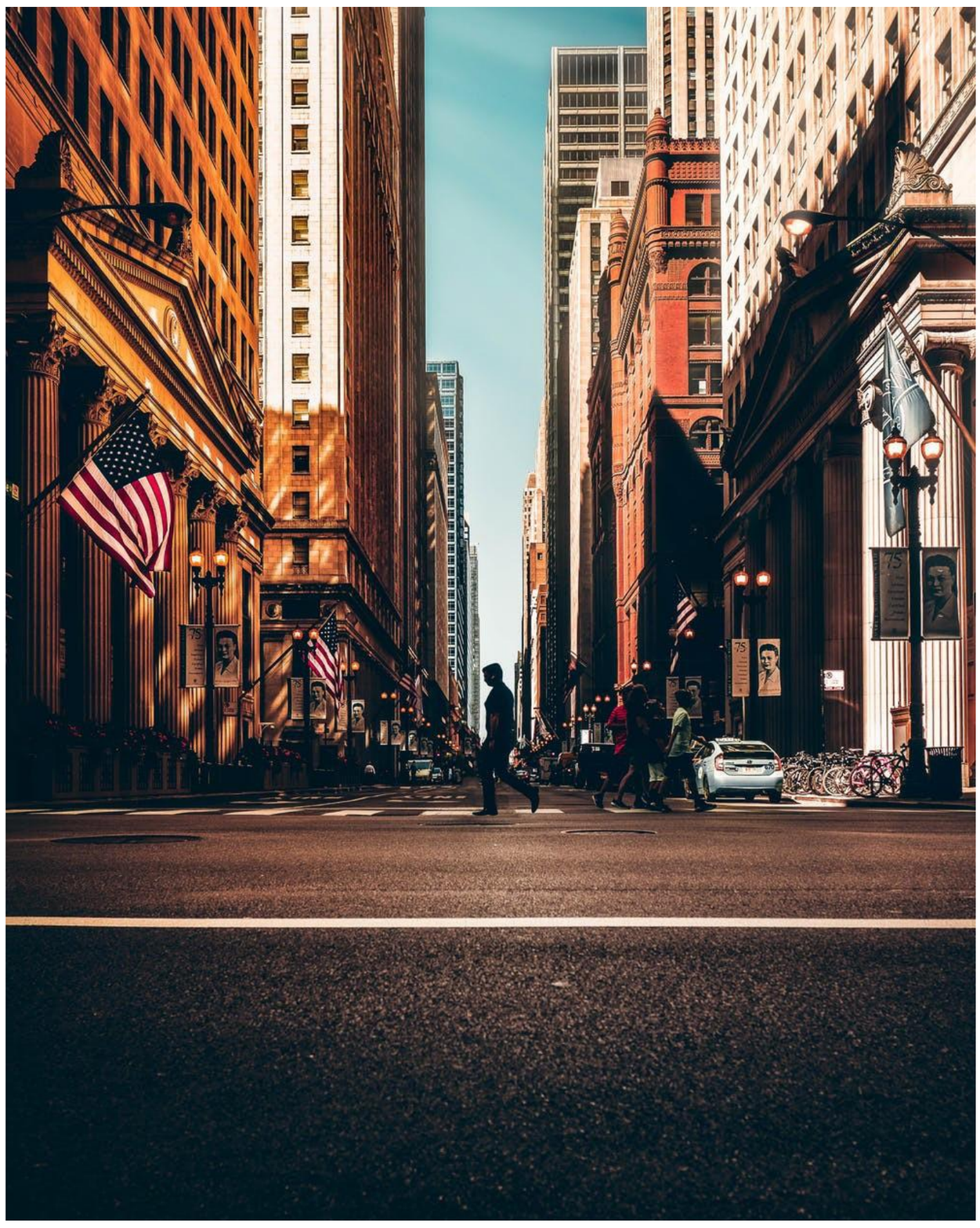
PARTIE 2

Le socle règlementaire de la résilience bancaire

EGE Ecole de Guerre Economique

2

Le socle règlementaire de la résilience bancaire



Comme à l'époque du far-west et des attaques de banques, le secteur financier a toujours été une cible pour les criminels de toutes sortes, et maintenant des cybercriminels.

Les évolutions technologiques et l'exposition importante aux cyberattaques a engendré une réelle volonté des Régulateurs d'encadrer les pratiques en matière de sécurité des SI et résilience en lien avec les technologies de l'information et des communications (TIC). Pour traiter efficacement les risques auxquels le secteur de la finance fait face, il est recommandé d'adopter une approche globale, incluant toutes les parties prenantes qui composent cette chaîne de traitement, car se protéger soi-même n'est pas suffisant : la dépendance à des tiers devenant de plus en plus manifeste.

La mise en conformité aux lois et règlements en vigueur constitue également le premier pas -et sûrement le plus important- vers une protection plus efficace.

2.1 Comité de Bâle

Au niveau international, le comité de Bâle a pour mandat de renforcer la règlementation, la supervision et les pratiques des banques afin d'assurer une stabilité financière. Il a reconnu que les principes publiés en 2011 ne couvrent pas certains aspects importants des risques opérationnels concernant les risques liés aux TIC (technologies de l'information et de la communication).

L'accélération des technologies et l'exposition croissante des systèmes bancaires aux cyberattaques ont amené le comité de Bâle à positionner la cyber résilience comme pratique vitale pour le secteur de la finance. En Mars 2021, le comité de Bâle (BAL IV) a publié les principes de la résilience opérationnelle.

Selon le comité de Bâle, les principes de résilience opérationnelle intégrale pour les banques comprennent la gouvernance, la planification et les tests de continuité des activités, la cartographie des interconnexions et des interdépendances, la gestion des dépendances vis-à-vis de tiers, la gestion des incidents et gestion des risques TIC, y compris la cyber sécurité :

Gouvernance

Les banques doivent utiliser leur structure de gouvernance existante pour superviser et mettre en œuvre une approche de résilience opérationnelle efficace. Cette dernière permet de réagir, de s'adapter et d'identifier les éventuels risques pour minimiser l'impact sur les opérations critiques. La résilience implique l'ensemble des couches managériales d'une organisation.

Planification et test de la continuité des activités

Les banques doivent mettre en place un plan de continuité des activités pour garantir leur capacité à fonctionner de manière continue et limiter les pertes en cas de perturbation

Gestion des incidents

Les banques doivent mettre en place des procédures de gestion d'incident (réponse aux incidents et retour à une situation nominale) et d'amélioration de réponse aux incidents. Elles doivent également définir une stratégie de communication et de partage d'information sur ces derniers, que ce soit en interne ou en externe (autorité de régulation).

Cartographie des interconnexions et des interdépendances

Les banques doivent cartographier les interconnexions et les interdépendances internes et externes liées aux opérations critiques. Cette cartographie permet d'identifier le niveau de vulnérabilité du système ainsi que la capacité de maintenir les opérations critiques.

La gestion du risque cyber devient donc un enjeu majeur pour le secteur financier. Pour y faire face, tous les régulateurs européens et internationaux renforce le cadre législatif pour la gestion des risques cyber et la résilience opérationnelle. Que ce soit à l'échelle européenne ou à l'échelle internationale, les régulateurs partagent les mêmes principes de base :

- Harmoniser le cadre législatif à l'échelle européenne et internationale pour la gestion des risques,
- Gérer les risques liés au TIC,
- Gérer et répondre aux incidents,
- Renforcer les tests de résilience opérationnelle,
- Focus sur les tiers (fournisseurs critiques),
- Définir une stratégie de communication et de partage d'information entre les établissements.

Les règles législatives ne précisent pas les aspects techniques de l'implémentation des règles législatives. Elles précisent surtout les objectifs à attendre. Les professionnels IT/sécurité se basent sur les standards techniques et bonnes pratiques pour rendre opérationnels les objectifs fixés par la réglementation. Parmi les standards, le framework NIST a été adopté par une grande partie des institutions financières.

Gestion de dépendance vis-à-vis de tiers

Les banques doivent faire une analyse de risque des prestataires tiers avant tout accord. Elles doivent également vérifier si le tiers dispose d'un niveau de résilience opérationnelle équivalent à celui de la banque pour protéger les opérations critiques. Le cas échéant, il faut prévoir une alternative pour maintenir l'activité.

Gestion des risques TIC en cybersécurité

Les banques doivent mettre en œuvre un solide programme de gestion des risques TIC pour faire face au risque cyber. La gestion des risques liés aux TIC comprend :

- L'identification et l'évaluation des risques liés aux TIC,
- La mise en place des procédures de réduction des risques liés au TIC,
- La mise en place des processus de gestion des incidents TIC et partage d'information,
- La mise en place des tests de suivi des mesures de réduction des risque TIC.

2.2. Directive NIS

Adoptée en juillet 2016, la directive NIS (Network and Information Security) a pour objectif de proposer des mesures destinées à assurer un niveau commun élevé de sécurité des réseaux et des systèmes d'information pour tous les pays de l'Union.

La directive prévoit de renforcer les capacités nationales de cyber sécurité. Elle repose sur une gouvernance pour chaque état membre et sur une coopération entre les pays européens tant au niveau opérationnel que pour les aspects politiques.
Les états membres de l'UE ont ainsi créés des autorités nationales compétentes en matière de cyber sécurité. En France, l'ANSSI (Agence Nationale de la Sécurité des Systèmes d'Information) répond à cette mission de défense des systèmes d'information de l'autorité nationale depuis sa création le 07 juillet 2009 par le décret n° 2009-834 et accompagne les entreprises nationales dans la mise en place des mécanismes de protection de leur patrimoine informationnel. Avec son Programme d'incubation, l'ANSSI tisse également des liens dans les régions depuis 2022 avec l'InterCERT-FR et la mise en place des CSIRT (Computer Security Incident Response Team) régionaux.

La France est le premier pays de l'Union Européenne à être passé par une loi pour élever le niveau de sécurité numérique du pays. La loi de programmation militaire (LPM) de 2013 a intégré des obligations à l'attention des organisations publiques et privées, dès lors que leurs activités sont jugées indispensables à la survie de la Nation, ce sont les Opérateurs d'Importance Vitale (OIV). La LPM exige la mise en application de règles fortement contraignantes et d'un contrôle régulier de l'Agence Nationale de la Sécurité des Systèmes d'Information (ANSSI). La directive NIS s'est inspirée de la loi de programmation militaire (LPM) et a défini deux nouveaux types d'acteur à encadrer :

- Les opérateurs de services essentiels (OSE) des secteurs de l'énergie, des transports, les banques et marchés financiers, la santé, la fourniture et distribution d'eau potable,
- Les fournisseurs de services numériques (FSN), ainsi que les moteurs de recherche, les places de marché (Marketplace) ou encore les services en nuage (cloud).

En France, les OSE et les FSN sont désignés par l'ANSSI (Agence Nationale de la Sécurité des Systèmes d'Information).

Source : Riskinsight Wavestone

La directive NIS laisse le soin à chaque état membre de définir les exigences de sécurité qui s'appliqueront aux opérateurs de services essentiels (OSE), Pour cette raison, les règles peuvent être différentes selon le pays.

La directive a mis en place un groupe de travail qui réunit depuis février 2017 les représentants des Etats membres, de la Commission Européenne et de l'agence européenne chargée de la sécurité des réseaux et de l'information l'ENISA (European Network and Information Security Agency). En France, c'est l'ANSSI qui participe à ces échanges. Les travaux menés ont permis d'accompagner les Etats membres pour la transposition de la directive en élaborant des méthodologies communes tel que les règles de sécurité. Ces règles sont réparties en quatre grands axes :

Source : Orange Cyberdéfense

La France précise le contenu de ses règles dans l'arrêté des règles de sécurité s'appliquant aux opérateurs de services essentiels publié dans le journal officiel de 28 septembre 2018. Par conséquent, la transposition de la directive NIS en droit français est achevée. Celui-ci reprend le découpage en quatre axes du groupe de travail et définit 23 règles couvrant un panel de mesures allant de l'analyse de risques à la gestion de crise.

En octobre 2021, le Parlement européen a approuvé une nouvelle version de la directive NIS (NIS2) qui fixe des exigences plus strictes en matière de sécurité informatique pour les entreprises, les administrations et les Etats.

L'élargissement de champ d'application en ajoutant de nouveaux secteurs tels que la gestion des déchets, les services postaux, les grands distributeurs alimentaires ou encore les fournisseurs d'accès à internet et les datacenters.

L'abandon de la distinction entre OSE et FSN, la désignation des OSE par la directive et non par les Etats

L'abandon de la distinction entre OSE et FSN, la désignation des OSE par la directive et non par les Etats

Le contrôle par les Etats des mesures techniques et organisationnelles mises en place (notamment pour l'analyse de risques et la gestion de crise).

Le framework NIS a une forte influence auprès des différentes industries, y compris auprès des superviseurs et régulateurs pour la rédaction des guidances en matière de cyber résilience dans le secteur bancaire.

2.3. DORA - Résilience numérique

En septembre 2020, la commission européenne a publié une proposition de règlement sur la résilience opérationnelle numérique du secteur financier : le DORA (Digital Operational Resilience Act).

L'objectif principal de la règlementation DORA est de mettre en place un cadre détaillé et complet sur la résilience opérationnelle numérique pour les institutions financières de l'UE. Le DORA a pour vocation de renforcer la cyber sécurité de l'ensemble du secteur financier. La place centrale et stratégique des systèmes d'information expose l'ensemble des institutions à un risque informatique pouvant affaiblir leur résilience opérationnelle. Cela intervient dans un contexte marqué par une multiplication des cyberattaques de plus en plus sophistiquées.

Pour la première fois, le DORA rassemblera les règles relatives à la gestion des risques liés aux TIC dans le secteur financier dans un seul texte législatif. Les règles sont destinées à couvrir un très large éventail d'entités fournissant des services financiers (établissements de crédit, entreprises d'investissement, établissements de paiement, de monnaie électronique, prestataires de services sur actifs numériques, sociétés de gestion, entreprises d'assurance et de réassurance, etc.), étant précisé que les exigences seront appliquées de manière proportionnelle en fonction de la taille et de la nature des activités de l'entreprise considérée.

Le recours de plus en plus courant aux prestataires externes dans les systèmes bancaires augmentant le niveau d'exposition aux risques cyber, l'union européenne exige de faire entrer dans le périmètre réglementaire les tiers « prestataires TIC critiques ». Le DORA constitue dès lors le premier cadre de surveillance au niveau de l'UE permettant d'identifier et de superviser les prestataires de service TIC jugés « critiques » pour les institutions financières. Cette identification est basée sur des critères spécifiques tel que l'impact systémique d'une défaillance opérationnelle du prestataire (cloud computing, logiciel, ...) sur le système bancaire. Après identification, ces prestataires sont soumis à la surveillance des autorités européennes (AES). Une des trois autorités européennes de surveillance (soit l'EBA, soit l'ESMA ou soit l'EIOPA) sera affectée à cette tâche de contrôle. L'autorité de surveillance choisie veillera à s'assurer que le prestataire de services a mis en place les dispositifs adéquats pour maîtriser les risques liés aux TIC pouvant impacter le système bancaire.

Les 5 piliers de la règlementation DORA listés ci-dessous permettent d'atteindre les objectifs suivants :

-De limiter les perturbations causées par les incidents via un dispositif adapté de gestion et de surveillance des risques,

-Avoir la capacité de réagir efficacement aux menaces via un dispositif de gestion des incidents TIC (gestion, classification et notification des incidents),

-De minimiser l'impact de cyberattaques via des tests de résilience opérationnelle grâce au déploiement d'un programme complet d'audit (test technique et test d'intrusion),

-D'identifier les risques liés aux tiers prestataires critiques et essentiels, D'avoir une stratégie de communication entre les différents établissements pour favoriser l'échange et le partage d'information sur les cyber-menaces.

Une vue générale et détaillées de DORA avec les numéros d'article est présentée en annexe 1.

Gestion des risques liés aux TIC

Exigences clés : La règlementation DORA pose un principe fondamental de la pleine responsabilité de l'organe de direction de l'entreprise dans la gestion des risques liés aux TIC.

Impact opérationnel : Le DORA introduit une formation obligatoire en matière de résilience opérationnelle numérique pour l'organe de gestion mais aussi pour l'ensemble du personnel, dans le cadre de son plan de formation. L'objectif est de maintenir à jour les compétences clés afin de mieux appréhender les risques informatiques et les impacts métiers associés.

Gestion des incidents liés au TIC

Exigences clés : Le DORA met en place un dispositif de signalement harmonisé des incidents selon une méthodologie standard de classification des incidents avec un ensemble de critères spécifiques :

Impact opérationnel : Les banques doivent adapter leur méthode de classification des incidents afin de se conformer aux exigences. Elles doivent également mettre en place les processus et les canaux de communication appropriés pour informer rapidement l'autorité de régulation en cas d'incident majeur.

Test de résilience opérationnelle numérique

Exigences clés : Le DORA impose de mettre en place un programme complet d'audits, comprenant une série d'évaluations, de tests, de méthodologies, de pratiques et d'outils, en mettant l'accent sur les tests techniques. Les organisations les plus critiques (l'autorité bancaire européenne, l'autorité européenne des marchés financiers et l'autorité européenne des assurances et des pensions professionnelles) doivent réaliser tous les trois ans un test d'intrusion en mode Red Team par des prestataires qualifiés indépendants. Ces tests couvrent les fonctions et services critiques et impliquant des tiers du secteur des TIC basés dans l'UE. Le scénario de test doit être approuvé à l'avance par l'autorité de régulation et les banques reçoivent, par la suite, un certificat de conformité à l'issue du test.

Impact opérationnel : L'organisation de ce type de test d'intrusion fondé sur la menace nécessite beaucoup de préparation. Notamment en impliquant l'ensemble des parties prenantes identifiées critiques qui doivent participer à la préparation de ces tests.

Partage d'informations et de renseignement

Exigences clés : Le DORA définit une stratégie de communication pour promouvoir l'échange d'informations sur les cyber-menaces entre entités financières. Elle introduit également des lignes directrices pour mettre en place des accords de partage d'informations en incluant des exigences de confidentialité et l'obligation d'informer l'autorité de régulation.

Impact opérationnel : Mise en place d'une stratégie de communication et appliquer les lignes directrices introduites par le DORA sur les modalités de partage d'information.

Gestion des risques liés aux tiers dans le domaine des TIC

Exigences clés : Avec le DORA, l'UE introduit des exigences à la fois pour les organisations financières, mais également pour les fournisseurs critiques de TIC. Le DORA impose aux organismes financiers de disposer d'une stratégie et d'une politique définies en matière de risque de tiers pour les TIC multifournisseurs. Elle exige d'établir un registre standard d'informations contenant la cartographie complète de tous leurs fournisseurs de TIC et leurs services. Il faut également informer annuellement le régulateur de toute modification apportée sur ce registre. Les organismes doivent définir une stratégie de substitution/continuité en cas de défaillance de fournisseur.

Avant de conclure un contrat, les entreprises doivent évaluer les fournisseurs de services TIC en fonction de certains critères (par exemple, le niveau de sécurité, le risque de concentration, les risques de sous-traitance). Ils doivent également prévoir une stratégie de sortie en cas de défaillance d'un fournisseur. Le DORA définit certaines modalités de contrat.

Les organismes financiers doivent disposer d'un niveau de contrôle suffisant et de surveillance de leurs prestataires. Les fournisseurs essentiels sont évalués chaque année au regard des exigences de résilience telles que la disponibilité, la continuité, l'intégrité des données, la sécurité physique, les processus de gestion des risques, la gouvernance, les rapports, la portabilité, les tests... Ces évaluations sont effectuées directement par le régulateur et donnent lieu à des sanctions en cas de non-conformité.

Impact opérationnel : La DSI et le service achat doivent partager une cartographie de l'écosystème TIC à jour et le service juridique doit intégrer la composante cyber résilience dans le cadre de la contractualisation avec leurs fournisseurs.

Le troisième pilier de la réglementation DORA, "Test de résilience opérationnelle numérique", peut s'appuyer sur le cadre TIBER-EU afin de répondre à cette exigence.

2.4. TIBER EU

En mai 2018, la Banque centrale européenne (BCE) a annoncé la mise en place d'un nouveau cadre européen (European framework for Threat Intelligence-based Ethical Redteaming ou TIBER-EU) pour tester la résilience de l'ensemble du secteur financier européen face à des cyberattaques « sophistiquées ».

Dans le cadre du TIBER-EU, il existe trois acteurs principaux :

- L'organisation : responsable de la gestion des risques, du cadrage et de la préparation des tests du début à la fin pour faciliter leur déroulement,
- Les autorités nationales : qui supervisent les tests et s'assurent qu'ils respectent bien le framework TIBER-EU,
- Le fournisseur de TI/RT : qui conduit les tests d'intrusion et Red Team.

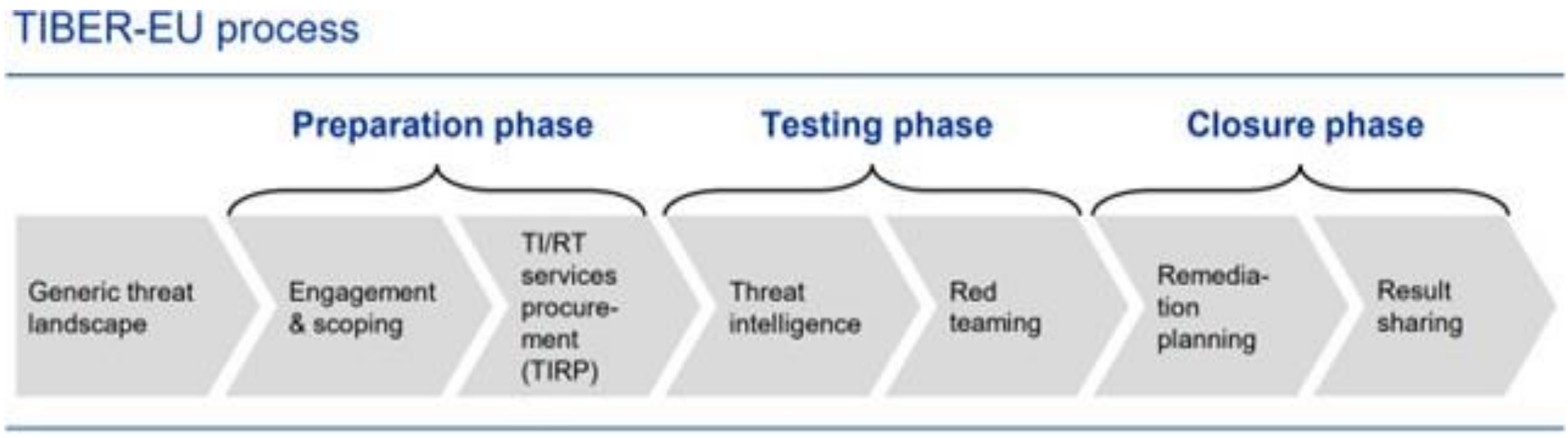
TIBER-EU nécessite que les tests Red Team ainsi que les attaquants mandatés, soient conduits par des entités extérieures à l'organisation commanditaire sans que la Blue Team, CSIRT de la société, ne soit informée des modalités de l'attaque qui sera réalisée en production afin d'être au plus près d'une situation réelle.

TIBER-EU est un cadre harmonisé pour la réalisation des tests d'intrusion de type Red Team ayant comme objectifs :

- D'améliorer la résilience des entités financières et du secteur en général,
- De standardiser et d'harmoniser les tests Red Team en Europe avant que des frameworks incompatibles n'émergent,
- Fournir des orientations sur la manière dont les entreprises peuvent planifier, exécuter et gérer ces tests au niveau national ou européen,
- Centraliser et analyser les résultats de test pour partager les conclusions aux entreprises du secteur concerné (géré par TIBER-EU Knowledge Center : TKC),
- Permettre aux multinationales d'opérer des tests Red Team au-delà des frontières internes à l'UE,
- Permettre une reconnaissance des tests effectués via ce framework au niveau européen.

Vue générale de TIBER

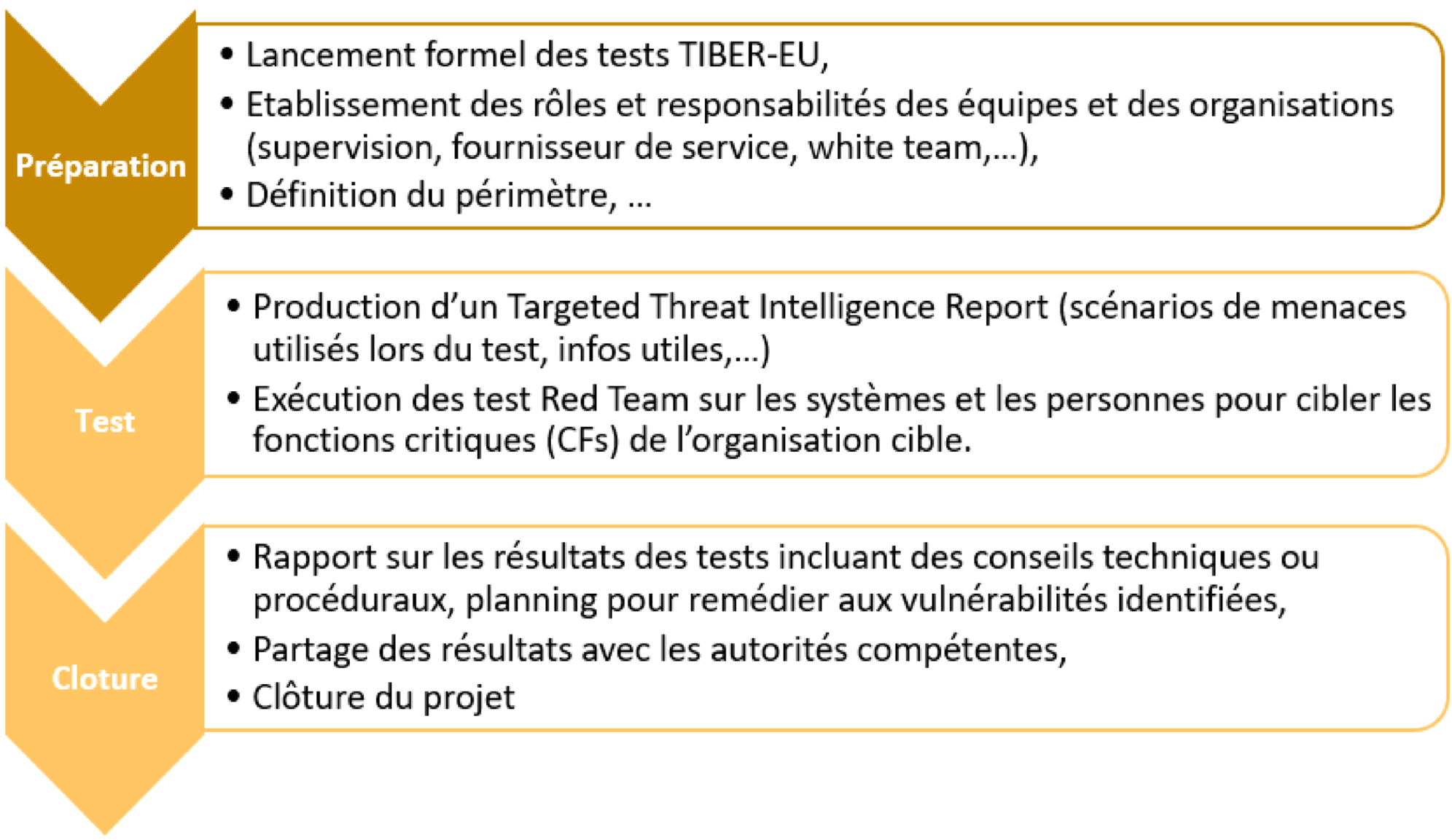
Le Framework TIBER se repose sur quatre processus :



Source : BCE

PROCESSUS TIBER

Le processus TIBER se décompose en trois phases obligatoires qui sont matérialisées dans le schéma suivant :



PARTIE 3

3. L'organisation de la cyber résilience opérationnelle bancaire

EGE Ecole de Guerre Economique

3.1. La continuité d’activité

Le Business Continuity Management doit être vu comme une réponse réactive à l'interruption ou l'indisponibilité d'une fonction critique métier entrainant des impacts juridiques, financiers, d'images ou de réputations.

3.1.1 BIA (Business Impact Analysis)

Une démarche au sein du monde bancaire a été renforcée ces dernières années, en premier lieu aux Etats-Unis pour les raisons évoquées en introduction, par le Business Impact Analysis (ou BIA) qui est un pilier du BCM.

Ce processus met autour de la table les différents acteurs de l'entreprise : le métier, le département informatique, les opérationnels en charge de l'activité au quotidien, du maintien en conformité de l'activité vis-à-vis du régulateur et des niveaux de service signés avec chaque client afin d'identifier les activités critiques d'un service.

Le BIA soulève une question essentielle :

Comment la société va-t-elle répondre à une interruption de service en s'appuyant sur ces ressources : humaines, technologiques, matérielles et organisationnelles pouvant intégrer des partenaires ou tiers délivrant un service … ?

EXEMPLE

Le trading de matières première nécessite d'une part d'accéder à une fonction de trading et ensuite à une fonction de règlement livraison, qui matérialise l'échange de valeur, supportés par un ou des outil(s) en interne ou en externe.

L'architecture, l'infrastructure et tous les composants IT indispensables pour délivrer un service doivent répondre au niveau de criticité des process business afin de garantir, dans le cadre de la politique de continuité d'activité mise en place au sein de l'entreprise, une reprise d'activité suite à un incident en respectant les deux contraintes suivantes : le Recovery Time Objective (R.T.O.) et le Recovery Point Objective (R.P.O.).

Si la reprise de service se fait dans le respect des conditions validées dans le cadre du plan de continuité d'activité, il n'est pas nécessaire de déclencher une cellule de crise et le plan de reprise d'activité.

Si la démarche est intéressante et permet d'adresser aussi bien la résilience grâce à la définition du plan de remédiation englobant les systèmes d'information, les ressources humaines et les capacités fournies par des tiers, elle n'en reste pas moins perfectible par son manque de vision holistique des enjeux métiers et des outils informatiques les supportant.

Cette approche métier dans les grandes entreprises, à défaut d'une approche à 360 degrés et “top down”, renforce les silos : gouvernance complexe et angle mort dans l'analyse de risques.

Une autre faiblesse de cette méthode est aussi un manque de visibilité sur les infras critiques utilisés par plusieurs métiers.

La dernière faiblesse de cette méthode est le couple produit/application. Les éléments sortants de cette dualité ne sont pas forcément discutés dans le cadre de cette analyse.

Les aspects de montée en charge dans le cadre de la reprise d'activité : localisation et nombre de personnels requis pour le redémarrage d'une activité sont bien décrits et testés.

Les autres éléments : postes de travail, le réseau, la conformité du site secondaire au besoin opérationnel ne font clairement pas parti de cet exercice.

Si le BIA est un exercice essentiel dans le cadre de la continuité et de la reprise d'activité, l'exercice reste perfectible par son approche en silos métiers et ne participe pas à pousser des sujets techniques et transversaux aux membres du comité de direction du fait du manque d'appui des métiers et fait fi des attaquants et de leur stratégie d'attaque.

Prenons l'exemple d'une attaque de type Ransomware

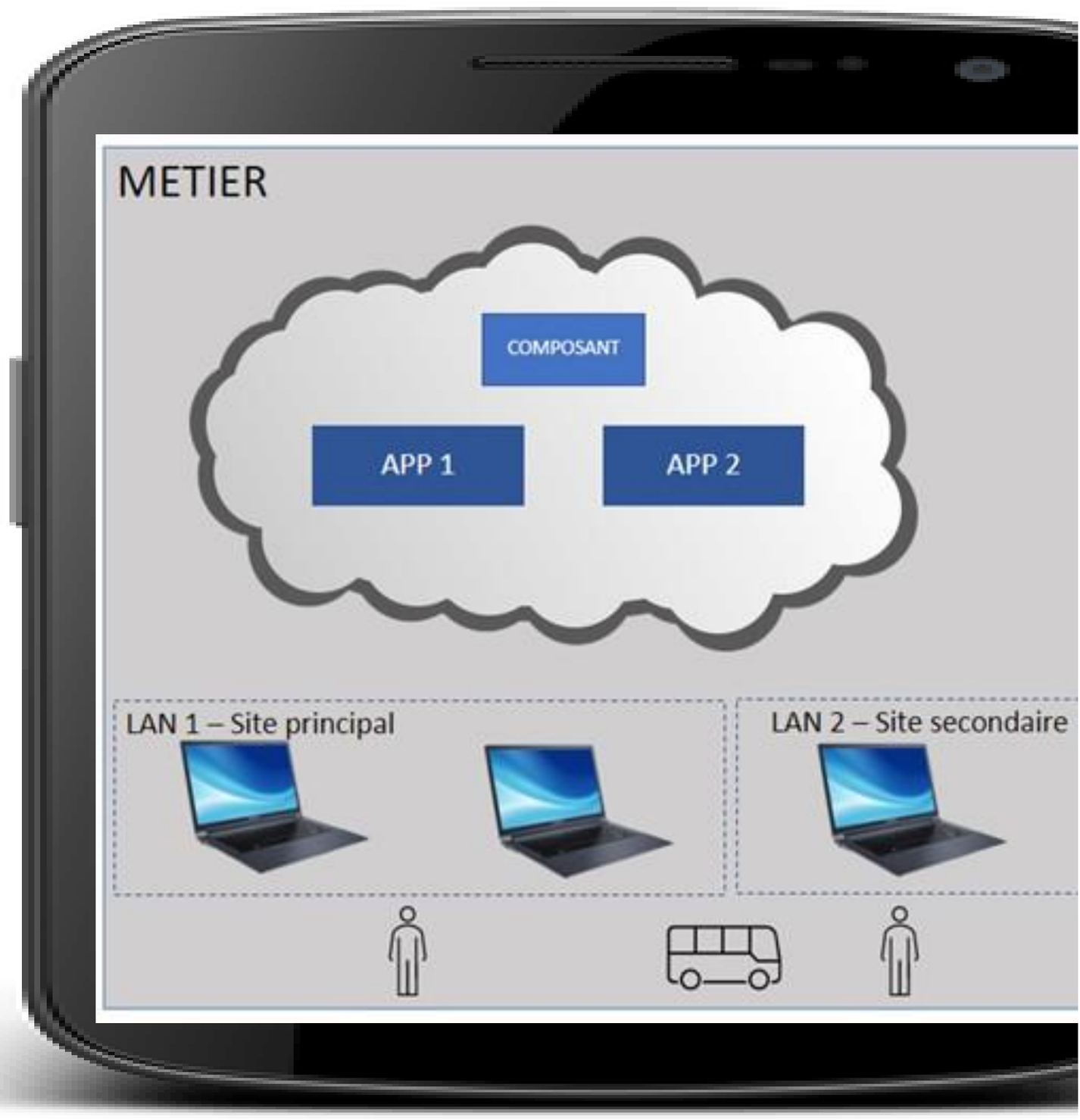
Le chiffrement des postes de travail sur le site principal va entrainer une impossibilité d'opérer une activité pour le compte d'un métier.

Ce scenario d'attaque n'aura pas été vu dans le cadre du BCM et du BIA d'une activité métier ce qui pose quelques questions :

-Est-ce que la DSI a défini en amont une stratégie de protection des postes de travail sur le site secondaire ?

-Est-ce que le DG et les membres du comité de direction ont le bon niveau de visibilité ?

-Est-ce que la DSI a le budget requis pour isoler les deux réseaux ?



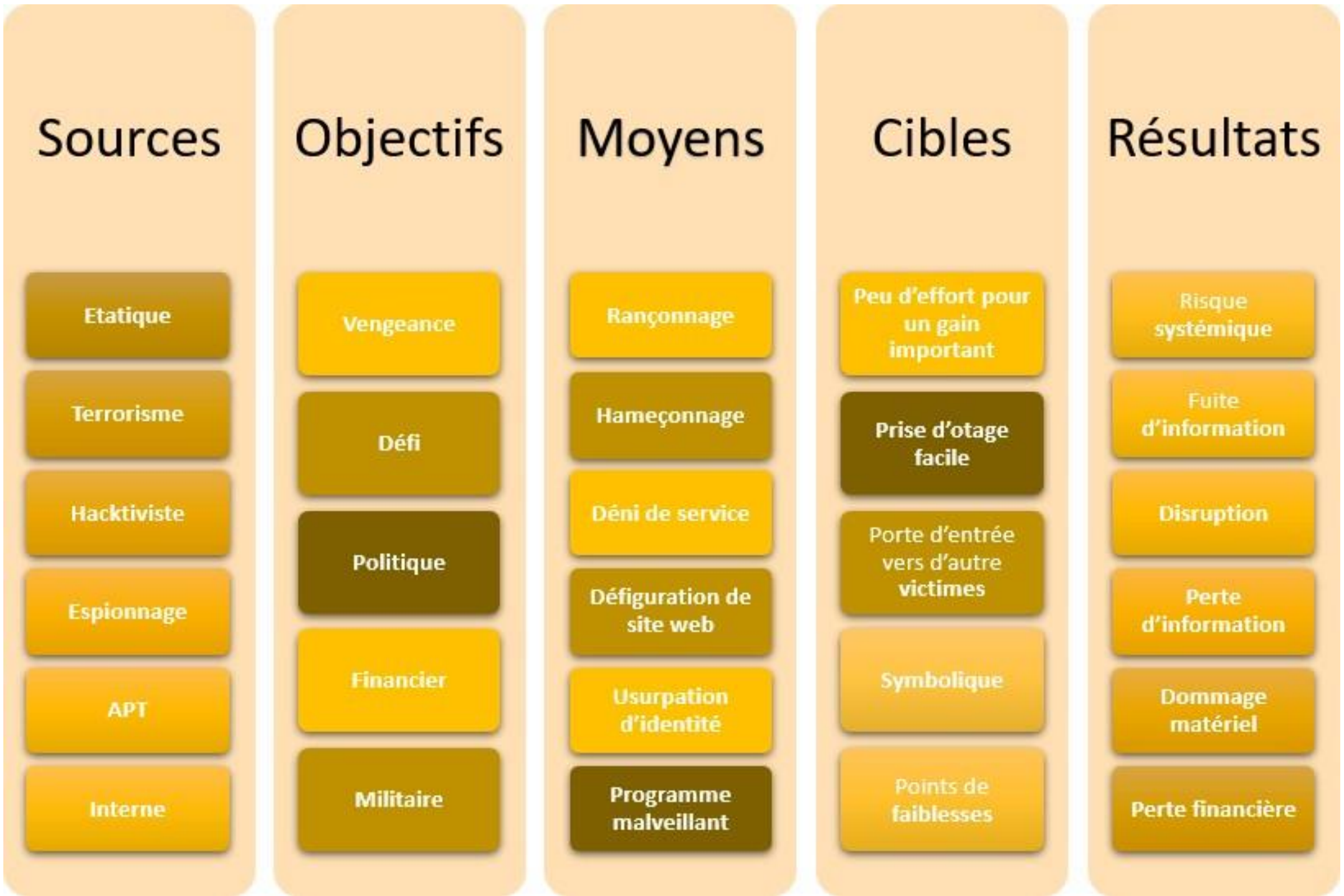
PARTIE 4

Adaptation de la gouvernance à la cyber résilience

EGE Ecole de Guerre Economique

4.1 Les surfaces d'exposition

Etat des menaces dans le secteur bancaire



Le risque le plus redouté d'une cyberattaque dans le secteur bancaire est le risque systémique pouvant paralyser l'économie à l'échelle nationale.

En cas d'incident cyber, les impacts potentiels pour le secteur bancaire s'échelonnent de « très élevé » à « critique » : les enjeux sont considérables pour les victimes avec des impacts directs sur le grand public mais également pour les attaquants du fait du risque de fraude et de détournement de fonds.

Le secteur financier reste la première cible des hackers dans le monde à cause de leurs rôles clés sur l'économie nationale et internationale et des flux critiques transitant à travers ces acteurs.

Les Advanced Persistent Threat (APT) sont des attaques sophistiquées et prolongées sur un système ciblé par les hackers dont l'objectif est de garder l'accès non autorisé le plus longtemps possible sans être remarqué afin d'exfiltrer un maximum d'informations. La différence entre une attaque classique et les APT se situe dans le fait que ces dernières sont planifiées avec une bonne connaissance de la cible afin de personnaliser un scénario d'attaque de haut niveau. Il s'agit de combiner plusieurs méthodes et/ou techniques grâce à des outils dédiés.
Les APT fonctionnent en trois grandes étapes et la plupart ont le même cycle de vie. Par conséquent il est important de reconnaitre leurs caractéristiques :

- Etape 1 : Infiltration,
- Etape 2 : Escalade et mouvement latéral,
- Etape 3 : Exfiltration.

« Le concept le plus essentiel en cyber-sécurité aujourd'hui est la vitesse. Pour vous défendre, vous devez être plus rapide que votre adversaire ».

Crowdstrike

APT27 (PANDA GOBELIN)

Découverte en septembre 2013. Cet adversaire basé en Chine cibles principalement les secteurs de la défense, de l'énergie et du gouvernement en Asie du Sud-Est, en particulier au Vietnam.

Opérant depuis au moins 2008, cet attaquant basé en Russie a ciblé des organisations politiques américaines, des organisations militaires européennes et des victimes dans de multiples secteurs à travers le monde.

APT28 (OURS DE FANTAISIE)

APT 34 (HELIX KITTEN)

Actif depuis au moins la fin de 2015 et est probablement basé en Iran. Il cible les organisations de l'aérospatiale, de l'énergie, de la finance, du gouvernement, de l'hôtellerie et des télécommunications.

De nombreux outils sont utilisés par les industries pour couvrir l'ensemble du cycle en partant du point de détection, puis mettre fin aux intrusions non autorisé, réduire les menaces et enquêter sur l'incident.

Purple Team Exercise Framework (PTEF) - SCYTHE et les experts de l'industrie ont créé le Purple Team Exercise Framework (PTEF) pour faciliter l'exécution d'émulations d'adversaires en tant qu'exercices d'équipe purple et / ou opérations d'équipe purple continues.

MITRE ATT&CK - la norme et le langage de l'industrie pour les tactiques, les techniques et les connaissances communes de l'adversaire.

Unified Cyber Kill Chain - Paul Pols - article universitaire rassemblant un certain nombre de Cyber Kill Chains par divers contributeurs de l'industrie tels que Laliberte, Nachreiner, Bryant, Malone, Lockheed et MITRE.

Cyber Kill Chain – Lockheed Martin – permet d'éduqué de nombreux consommateurs non techniques sur le fonctionnement des adversaires et les étapes qu'ils effectuent lors d'une violation.

Source : scythe.io

4.2. AppSec - Security by Design

Les grandes entreprises du monde bancaire et de la finance ont lancé cette transformation stratégique, intégration des risques cyber il y a quelques années afin de réduire leurs expositions aux risques d'attaques ou de fraudes et leurs conséquences afférentes.

Les deux principaux chantiers lancés ont eu pour objectif de réduire deux principales surfaces d'attaques importantes :

- Les utilisateurs via les courriers électroniques d'hameçonnage,
- Les applications exposant des services aux clients de l'établissement, application de type web dans un premier temps et mobile dans un second temps via leurs vulnérabilités logicielles.

Sur le premier chantier, l'acculturation aux risques d'hameçonnage pour les collaborateurs par des formations ludiques ou bien via de fausses campagnes d'hameçonnage organisées en interne ou via un prestataire externe a permis de réduire cette exposition sans la supprimer totalement. L'erreur reste alors du fait de l'humain. Ce type d'attaques reste en progression constante.

L'hameçonnage (phishing en anglais) est en progression sous toutes ses formes (1,3 millions de recherches d'informations et d'assistance), notamment par SMS.

Sur le deuxième chantier, l'effort requis et les impacts sur l'organisation, la gouvernance et les processus sont nettement plus conséquents et continuellement adaptés à la menace afin de réduire la surface d'exposition aux vulnérabilités.

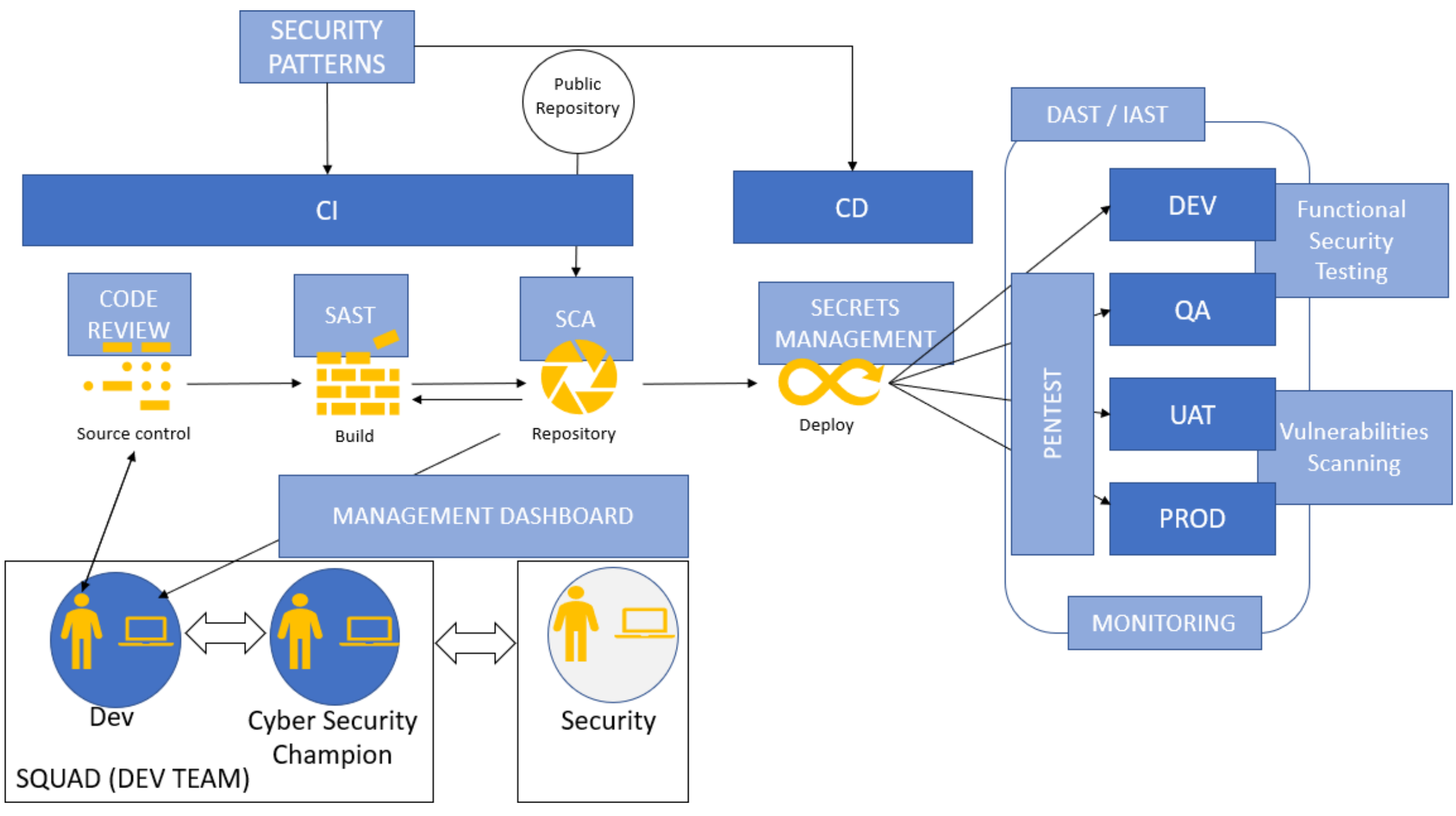
Sur le deuxième chantier, l'effort requis et les impacts sur l'organisation, la gouvernance et les processus sont nettement plus conséquents et continuellement adaptés à la menace afin de réduire la surface d'exposition aux vulnérabilités.

À la suite de l'entretien avec Felix A., AppSec, Banque privée le 22 avril 2022.

Le passage en production d'applications doit répondre dorénavant à un certain nombre d'exigences, en fonction de la criticité du métier et du niveau de confidentialité des données, dans le monde bancaire listées ci-dessous :

- D'architecture logicielle,
- D'infrastructure,
- Du niveau de confidentialité des données,
- De la directive RGPD,
- Du développement logiciel,
- De la conformité à la résistance aux tests de pénétration exécuté par une société tierce,
- De la méthode d'identification et d'authentification d'un utilisateur,
- Du chiffrement des données aussi bien en transit que sur le support de stockage,

Le schéma suivant illustre les évolutions qui ont été menées lors du cycle de vie du développement logiciel en termes d'outils afin de transformer le modèle devops, en intégrant la sécurité dès la conception du logicielle, en modèle devSecops d'une part, mais aussi du point de vue organisationnelle en nommant dans chaque équipe de développement une personne en charge des aspects sécurité : le Cyber Security Champion.



L'enjeu est considérable, et la vulnérabilité Log4J en fin d'année 2021 l'a parfaitement matérialisée, car la remédiation doit être réalisée au plus vite, les vulnérabilités logicielles étant la deuxième porte d'entrée dans le SI des entreprises.

Le temps de réponse des équipes IT est un enjeu majeur lors de ce type de crise, cette vulnérabilité impactant un nombre important d'applications, a permis de valider la pertinence du modèle SCA mais a aussi mis en relief un point d'amélioration important au niveau de la gestion d'un parc informatique : avoir une vision exhaustive de son parc applicatif et de ses composants logiciels dans le temps court.

Dans le cadre du développement du logiciel en intégrant la sécurité en amont, deux approches sont complémentaires mais on des avantages/inconvénients différents :

- L'approche STATIC APPLICATION SECURITY TESTING (SAST) considérée comme plus mature mais qui a pour inconvénient un manque de flexibilité en termes d'intégration,

- La tendance s'oriente vers des approches plus dynamiques : DYNAMIC APPLICATION SECURITY TESTING (DAST) et INTERACTIVE APPLICATION SECURITY TESTING (IAST) qui sont moins matures à ce stade mais permettent une analyse plus poussée, car exécutée lorsque l'application tourne et non plus uniquement sur une analyse statique de code.

L'outil SOFTWARE COMPOSITION ANALYSIS (SCA) permet de reporter les vulnérabilités existantes dans les packages utilisés par les développeurs durant le cycle de vie du développement logiciel afin d'éviter d'introduire de nouvelles vulnérabilités en production, mais surtout d'identifier au plus tôt des vulnérabilités déjà existantes en production devant faire l'objet d'un correctif.

FA - APPSEC OFFICER - 26/04/2022

FELIX.A

« L'utilisation d'application en mode SAAS est une des possibilités pour réduire le temps de remédiation d'une vulnérabilité en déportant la correction chez le fournisseur ayant une meilleure maîtrise de ce composant technologique ».

« Le modèle DAST, s'il reste performant dans une architecture web classique montre clairement ses limites sur une architecture orientée API ».

« Le modèle IAST peut pallier la limitation du DAST et est plus performant dans la recherche, du fait de son architecture où un agent est directement déployé au sein de l'application ».

Ces changements profonds au sein des entreprises permettent de réduire les risques face aux attaques mais ne les suppriment pas.

4.3. Organisation d'un SOC

Dans le cadre de cette étude du secteur financier et de la cyber résilience, la compréhension opérationnelle est nécessaire pour illustrer l'écosystème numérique d'une cellule de détection des intrusions. Pierre-Hervé G. est chargé de la sécurité opérationnelle d'une Mutuelle française de renom. Après quelques années dans le domaine des systèmes informatiques, il a choisi par passion de travailler dans le domaine de la cyber-sécurité.

Définition d'un S.O.C. selon Pierre-Hervé G.

L'interview accordée apporte une présentation détaillée d'un S.O.C.

Pierre-Hervé estime que le grand public a du mal à définir le rôle du S.O.C. Littéralement, cette terminologie, abrège l'expression anglaise Security Operationnal Center. Pour Pierre-Hervé, le S.O.C. est un centre de services dont le rôle est de protéger le système d'information. Les équipements utilisés dans le S.O.C. émettent des alertes dès lors que le système d'information fait l'objet d'une potentielle attaque.

Entre processus techniques et interventions humaines, cette cellule est un premier rempart dans les DSI afin de réduire la surface des attaquants et l'accès au S.I. (système d'information) :

- La mission des collaborateurs du S.O.C. est de détecter grâce aux équipements E.D.R., S.I.E.M., des sondes et des firewalls,
- La seconde mission du S.O.C. est un rôle de courroie de transmission dans la remontée des incidents ou des tentatives d'intrusion vers le C.E.R.T. et auprès de l'A.N.S.S.I. si nécessaire.

•

C.E.R.T. ou Fournisseur Externe de gestion des incidents Niveau 3

Les équipes du S.O.C. et celles du C.E.R.T. travaillent quotidiennement main dans la main. Les premiers analystes seront affectés dans le traitement des alertes émises en investiguant sur la cause. Quant aux équipes C.E.R.T, elles vont investiguer de manière plus poussée afin de résoudre les typologies d'attaques du S.I. : D-DOS, failles des éditeurs de logiciels, provenance géographique de l'attaque… En bref, les équipes S.O.C. et C.E.R.T. sont d'un excellent niveau de compétences techniques et de savoir être face à la menace des cyberattaques.

La profession est normée. A titre d'exemple, le site gouvernemental de la sécurité des S.I. décrit les missions du C.E.R.T. Dans cet écosystème présenté, il est intéressant de constater que le partage d'informations demeure le vecteur principal pour faire face efficacement sans grands moyens aux millions d'attaques.

Les Directions Générales des banques sont très sensibles aux préconisations des régulateurs bancaires, c'est pourquoi, les investissements dans le champ de la cyber-sécurité sont considérables :

- Achat des solutions logicielles,
- Gestion du cycle de vie des équipements,
- Licences d'exploitation,
- M.C.O. (maintien en condition opérationnelle),
- Formation des équipes,
- Certifications des compétences,
- Politique de rémunération motivante pour retenir les collaborateurs les plus compétents.

4.4. SOC R&D

La transformation est également opérée en aval dans le cadre de la réponse à un incident.

Le paradigme change complètement en intégrant la RSSI comme décisionnaire, via sa contribution lors de la gestion d'une crise ayant pour origine un incident cyber, de la reprise de l'activité.

Le métier a pour charge de prioriser les activités métiers qui doivent être relancées en fonction de leur criticité, mais la DSI, dans le cadre d'un incident cyber, est dépendante de l'analyse des CSIRT et donc du RSSI.

Sans l'assurance d'un redémarrage de l'activité sur une base saine, ce qui nécessite une investigation, recherche du patient 0, comprendre le mode opératoire de l'attaquant, par où il est passé, ou a minima l'assurance de redémarrer dans un environnement sous contrôle.

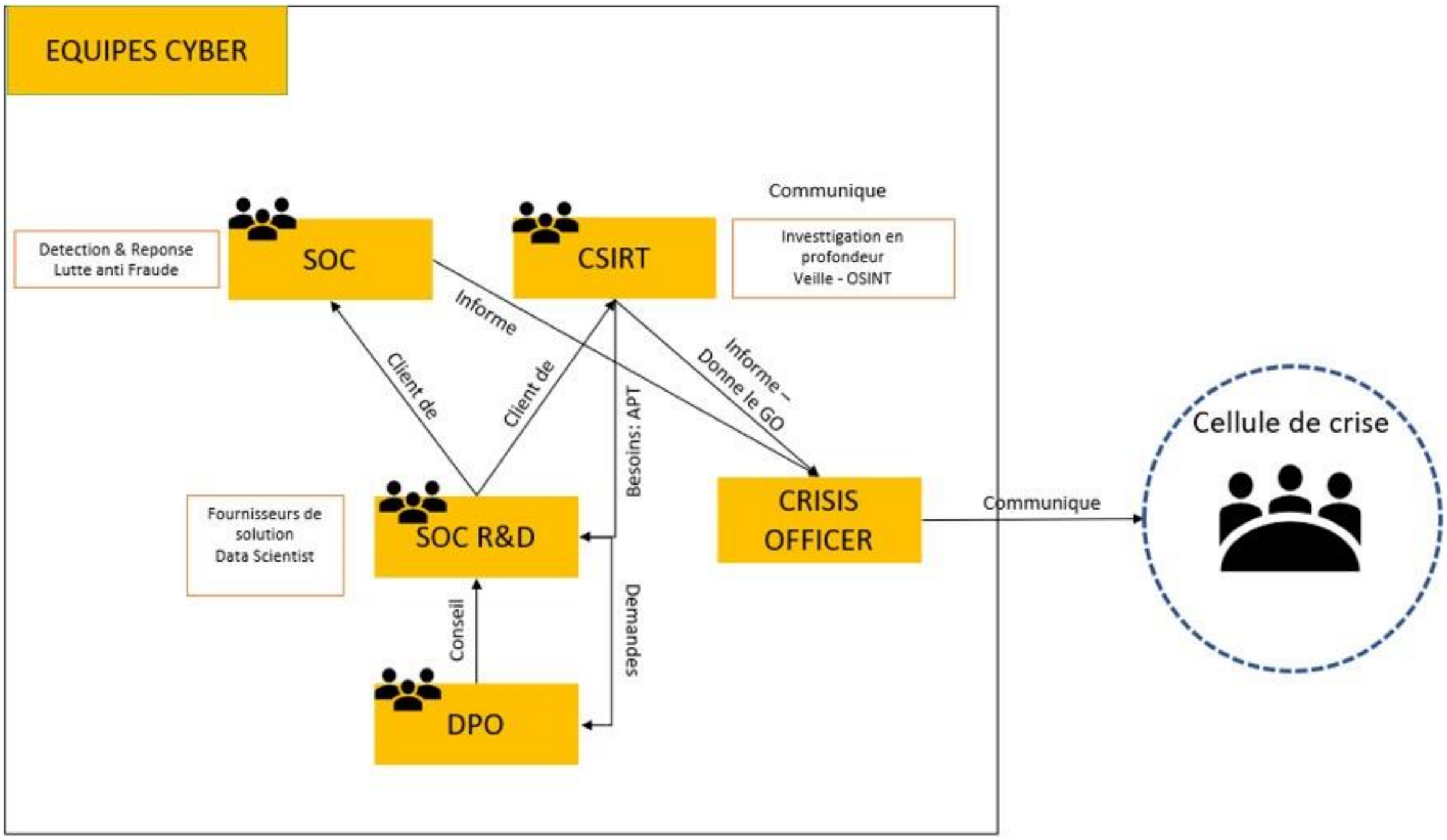
Le risque est de potentiellement accroître le problème au sein du SI et démotiver les équipes opérationnelles qui vont devoir repartir de zéro dans un contexte de crise anxiogène.

À la suite de l'entretien avec Amandine D., SOC R&D Manager, Banque privée le 22 avril 2022 :

Amandine D

« La gestion d'une crise cyber et la maîtrise du processus afférent est l'élément clef afin que les membres de l'équipe cyber puisse travailler de façon sereine lors de la crise en connaissant parfaitement leur rôle dans l'organisation ».

« La réévaluation continuelle du processus ainsi que sa répétition permettent d'atteindre un objectif et valider que le RACI correspond toujours à la réalité ».



Le SOC, en intégrant la composante CSIRT, a pour principal objectif de répondre à un incident cyber mais son organisation, dans les entreprises atteignant une taille critique, devient de plus en plus mature.

La composante SOC se découpe en trois parties :

- L'équipe SOC,
- L'équipe CSIRT,
- Et parfois une équipe SOC R&D.

Amandine D

« La capacité à gérer un volume de données important, captation, agrégation, analyse, en temps réel est un élément critique dans le cadre d'une réponse à un incident efficient ».
« Le machine learning permet de détecter des signaux faibles qui passaient ultérieurement sous les radars et d'adapter continuellement les stratégies de défense ».

Le traitement de la donnée est devenu un élément critique dans le cadre de la cyber résilience et de la réponse à un incident.

Le rôle de DPO devient un élément central dans les équipes SOC afin d'une part :

- D’apporter sa connaissance de la donnée en phase de design,
- De s'assurer que le traitement des données est conforme à la directive RGPD.

Du fait de la richesse des données traitées, un DPO dédié à l'équipe SOC est fortement encouragé.

Le choix d'un fournisseur de solution permettant de couvrir les besoins d'analyse, de big data, d'adaptation de modèle est aussi un élément central, les solutions proposées par Elastic dans le domaine de la cyber, SIEM, Endpoint, sont de plus en plus répandues sur le marché.

Le SOC devient une ville dans la ville avec son propre écosystème et ses propres contraintes liées à la résilience. Ainsi toute défaillance d'un système de protection peut avoir des conséquences sur la stratégie défensive.

Le SOC R&D est dédié à la recherche et au développement afin d'améliorer continuellement les stratégies défensives et s'adapter aux nouvelles attaques ou fraudes.

Les solutions embarquant de l'intelligence artificielle et plus spécifiquement du machine learning prennent une place de plus en plus prépondérante dans les stratégies défensives des entreprises.

L'analyse comportementale d'un utilisateur, “user behavior analysis”, ou d'un élément technique du système d'information, réseau, firewall, … se révèle de plus en plus efficace et permet d'identifier toute déviance par rapport à un comportement standard afin d'alerter les équipes de réponse à incidents pour une première investigation.

Le SOC R&D devient de facto un fournisseur de solution logicielle à ses deux uniques clients : le SOC et le CSIRT ont pour objectif la mise à jour de modèles prédictifs afin de prendre en compte de nouveau type d'attaques, APT, d'enrichir les bases d'informations existantes au sein de l'entreprise avec : adresses IP malicieuses, lutter plus efficacement contre les campagnes d'hameçonnage mais aussi lutter contre la fraude interne des lors que l'impact est financier.

Cela nécessite un ensemble de compétences, très recherchés sur le marché de l'emploi, au sein de ce service :

- Data Scientist,
- IA et langage naturel,
- Big data (à titre d'exemple, un proxy génère 1 million d'enregistrements par heure),
- Architecture logicielle répondant à des besoins de haute fréquence,
- Intégrateur de solution logicielle.

PARTIE 5

Écosystème numérique de la cyber résilience

EGE Ecole de Guerre Economique

5.1 Éditeurs

Les fournisseurs informatiques dans l'organisation bancaire sont considérés comme stratégiques dans la continuité des activités commerciales. A l'instar de Swift par exemple, qui très récemment a défrayé la chronique dans le conflit russo-ukrainien.

L'organisation bancaire repose sur deux jambes : elle est à la fois productrice de produits & services financiers et distributrice, soit directement par le biais de son réseau bancaire, soit par des tiers au statut de partenaires. Par ailleurs, la digitalisation a accéléré cette capacité de servir ses clients 24/24 et ce partout dans le monde. Tout s'accélère et des milliards de transactions se croisent par seconde dans le monde entier.

C'est pourquoi, la ligne directrice de la stratégie bancaire s'appuie sur l'intégration de ses fournisseurs dans la continuité et la pérennité de son activité commerciale. Nous distinguons différents niveaux de fournisseurs que nous allons présenter par la suite :

Les éditeurs de logiciels

ce sont des acteurs numériques en capacité de concevoir un produit logiciel au service de plusieurs clients, par exemple Microsoft avec sa fameuse offre 365 ou des acteurs plus spécialisés comme Secure hub ou Dili trust. Avec notamment OnPremise ou Saas, le secteur bancaire est friand de solutions logicielles innovantes afin de supporter sa croissance.

Les infogérants

les prestataires informatiques internationaux offrent leurs services d'infogérance aux banques depuis des décennies : IBM a même signé une joint-venture avec BNP Paribas appelée BP2I. Tata consulting services délivrent des prestations de maintien en condition opérationnelle ou d'exploitation (le RUN versus BUILD) depuis Bangalore en Inde. Accenture est un spécialiste sur l'infogérance SAP. Bien entendu, Atos et Cap Gemini occupent également dans le monde une place de leaders. Les enjeux sont colossaux, ces contrats de plusieurs centaines de millions d'euros signés entre les clients bancaires et ces géants de l'informatique pèsent très lourds dans les services financiers.

Les hébergeurs

Cette troisième activité se révèle depuis ces dix dernières années comme stratégique et l'externalisation des infrastructures vers les plus puissantes sociétés d'hébergement s'accélèrent. Le cloud pour être plus précis consiste à externaliser dans un nuage son infrastructure informatique en profitant d'une mutualisation des infrastructures du tiers tout en cloisonnant son système d'information. Les leaders du domaine sont outre Atlantique : Azure de Microsoft, AWS d'Amazon, GCP de Google ou Bluemix pour IBM. Notre fleuron national OVH est encore loin derrière et peu intégré dans le domaine bancaire.

Le contrat d'affaire reste la clé de voûte entre les banques et leurs fournisseurs. Les juristes veillent à inclure des clauses sur la sécurité opérationnelle : cet aspect est fondamental pour assurer une continuité des services. Il est arrivé que des clients comme BNP Paribas, interviennent dans le rachat d'éditeurs stratégiques comme Callatay Wouters par des fournisseurs plus établis et pérenne comme SOPRA STERIA.

Dans le cadre de la réglementation DORA, il a été cité plus haut que les fournisseurs engagés comme tiers devaient tous se mettre en conformité et renforcer leur PSSI pour se prémunir du risque et garantir la résilience des opérations bancaires, c'est une lourde responsabilité pour ces fournisseurs.

« ***Le marché des logiciels de système bancaire devrait connaître une croissance exceptionnelle en 2018-2026*** ». *Androidfun.fr*

Le marché du logiciel est un énorme marché que se partage des acteurs essentiellement européens et nord-américain.
Les populations dans le monde s'équipent de smartphones, de tablettes et de laptops, avec une forte accélération dans les pays en voie de développement. Ce phénomène profite également aux banques : les clients souhaitent utiliser les services bancaires 24/24 en se connectant à leurs espaces privés.

Le secteur bancaire est en recherche perpétuelle de solutions logicielles en mesure d'améliorer son efficacité opérationnelle, ou en quête de solutions OAD (outil d'aide à la décision) ou tout simplement en choisissant des solutions permettant la collaboration transfrontalière. Par ailleurs, le régulateur impose parfois des traitements spécifiques qu'il est préférable d'investir dans des solutions logicielles telles que les core banking. A titre d'exemple, nous pouvons citer Sab, Temenos.

Dans le volet des marchés financiers, les progiciels sont très répandus : passage d'ordre, calcul de rentabilité, gestion de portefeuille… Blackrock, Mysis, Calypso, Arpson, Sungard sont les softwares leader de la Banque Finance Investissement (B.F.I.).

Les banques sont toutes dotées d'un service achat dit « **procurement** », composé d'experts, de juristes, d'analystes et de négociateurs dont le rôle est d'analyser le risque fournisseur et de filtrer les brebis galeuses.
Ce filtre est une parade contre le risque opérationnel de tiers. Nos grandes banques françaises souhaitent généralement s'engager avec des fournisseurs pérennes disposant d'une feuille de route, produit impulsé par une cellule R&D en phase avec les exigences du secteur. Néanmoins, comme nous avons pu le voir précédemment, les grands groupes bancaires s'engagent dans ce nouveau siècle, dans deux défis majeurs, à savoir : la numérisation de l'économie et la lutte contre le réchauffement climatique (décarbonisation). Le secteur bancaire intègre des produits logiciels innovants en phase avec sa stratégie RSE. Nous ne pouvons-nous intéresser aux éditeurs de logiciels, sans nous intéresser aux start-ups. La plateformisation de l'économie génère de nouvelles sources de partenaires pour les banques. Afin de sécuriser leurs engagements et leur pérennité, les banques investissent par le biais de leur département private equity dans ces fintechs.

« ***En 2020, les fintechs françaises ont prouvé leur résilience en levant près de 830 millions d'euros, selon le baromètre annuel France Fintech. Pour cause, les évolutions technologiques et réglementaires récentes ont généré de profonds bouleversements dans l'écosystème des services financiers*** ». *Fintech : 100 millions d'euros dédiés aux startups de la finance (bpifrance.fr)*

5.2 Infogérants

L'infogérance est la délégation de la gestion totale ou partielle de son SI ou de son infrastructure informatique à un prestataire externe.

Les grandes banques commerciales françaises sont quasiment toutes organisées de la même façon. Soit une organisation matricielle, composée de business lines spécialisées (banque de détail, asset management, gestion privée, BFI, assurance, affacturage, leasing, crédits consommation, private equity…). Chaque business line est filialisée et organisée avec un comex comprenant une DSI en charge des études.
Le SI infrastructure en charge de l'exploitation du business est mutualisé : un serveur de production est en mesure d'accueillir N applications quel que soit leur provenance. En informatique tout est une question d'architecture technique et de configuration machines.

A titre exemple, BP2I est une joint-venture entre BNP Paribas et IBM, BPCE IT est la filiale infogérance de BPCE. SILCA quant à elle, est celle du Crédit Agricole SA et enfin GTS, sera l'infogérant interne du groupe Société Générale.

Chez ces infogérants internes, nous retrouvons tout ce qui permet à la banque de fonctionner : poste de travail, réseaux, run, build, cloud, datacenters, téléphonie… Selon trois niveaux de service selon la norme ITIL, avec une expertise N3 sur Paris et un N1 & N2 en outsourcing France ou offshore.

« ***SILCA entend développer la mutualisation de ses infrastructures, la massification de la sous-traitance ainsi que l'industrialisation des processus et la modernisation des outils. Ce programme doit permettre de réduire significativement les coûts de la production informatique et de favoriser par l'innovation la digitalisation des métiers du groupe Crédit Agricole*** » *SILCA, filiale de Crédit Agricole S.A., modernise la gestion de ses infrastructures avec l'aide de Capgemini – Capgemini France.*

Afin de réduire considérablement les couts d'exploitation et de se dédouaner d'une gestion des compétences complexes dans un contexte de pénurie, caractérisé par une évolution continue des savoir-faire, ces mêmes acteurs bancaires, sont en mesure de signer des contrats d'infogérance totalement externalisée avec des géants comme Accenture, Cap, Atos ou des champions nationaux comme ITS Groupe ou Neurone. Dans la cyber-sécurité, OBS reste le pionnier.
C'est justement dans ce cadre que la réglementation DORA s'inscrira en prévoyant une évaluation des tiers impliqués dans la gestion des opérations bancaires.

« ***En France comme dans le reste du monde, le marché de l'externalisation des SI ne suit pas une évolution linéaire. On constate toutefois une croissance globale du nombre de contrats signés et de leur valeur depuis les années 90. Par exemple, des études menées par le cabinet Pierre Audoin Consultants montrent que le marché représentait moins de 2 milliards d'euros avant 1997, pour passer à plus de 5,6 milliards d'euros en 2007. En 2020, le marché s'élève à plus de 13 milliards d'euros en France (source : Statista)*** ». *Les chiffres clés du marché de l'infogérance en France (freelance.com)*

Les DSI des groupes bancaires signent des contrats de plusieurs millions d'euros sur une année avec des infogérants sur des niveaux de services différents.

5.3 Hébergeurs

Alors que les institutions financières cherchent à améliorer leur efficience et l'expérience client, dans un environnement de plus en plus concurrentiel, la transformation technologique reste une priorité.

Dans le même temps, la réglementation et la gestion des risques liés à la transformation technologique nécessitent d'être bien comprises, atténuées et gérées. Les règles dictées par les régulateurs doivent être continuellement respectées. Ces deux points sont de la plus haute importance pour le secteur de la finance.

Selon une étude de Gartner réalisée en 2021, la sécurisation du cloud est le segment de la sécurité qui aura le plus de croissance en 2022 : +41%.

De plus les investissements dans les solutions clouds publics sont de plus en plus importants +23%. Les projections de Gartner nous montrent bien que la cyber résilience est un domaine qui va fortement orienter les choix des entreprises et des DSI dans les années à venir, surtout dans le domaine de la finance. Amazon, Microsoft, Google, Alibaba et IBM ont mis la main sur plus de 70% du marché.
Si les parts de marche d'IBM sont en constante baisse, sur le segment le plus important du cloud public, il faut noter que la société reste leader sur la construction d'une offre cloud privé souvent en partenariat avec leurs clients sur des modèles Multi-zone Région (cloud MZR).

Ce positionnement pourrait s'avérer payant pour IBM avec le renforcement des exigences liées à la directive Dora et pour des acteurs de niche qui déjà arrivent à tirer leur épingle du jeu en Europe : le Français OVH et l'américain Rackspace (*).

(*) IBM est leader sur ce segment marché

Comme mentionné précédemment, le volet technologique introduit de nouveaux risques pour les entreprises et le choix d'un fournisseur Cloud nécessite d'avoir une bonne vision de ces potentiels risques.

L'ENISA a publié un document permettant d'accompagner les entreprises lors de la sélection d'un fournisseur cloud en partageant une vision exhaustive des risques encourus.

Le fournisseur Cloud qui sera en position d'être leader dans le secteur de la finance est celui qui répondra au mieux aux points suivants : dans le cadre de la construction de solution cloud privé, le projet de cloud MZR co-construit par IBM et BNP PARIBAS SA et qui sera opéré par des équipes BNP PARIBAS SA, est un pari très intéressant car il allie une expertise technologique sur les solutions cloud fournies par IBM et une expertise métier et de la régulation fournie par BNP PARIBAS SA et devrait permettre non seulement de gérer en totale autonomie son SI, mais aussi de proposer aux acteurs du monde de la finance une solution d'hébergement conforme aux exigences réglementaires.

Les risques principaux

La majorité de ces risques sont inhérents à un SI mais doivent faire l'objet d'une analyse de risques orientés fournisseur. Mais le choix d'un modèle privé permet au client de réduire l'exposition à ces risques.

Gouvernance

Une attention particulière doit être portée lors de la rédaction du contrat liant les deux parties sur le niveau de service attendu et clarifier le modèle de gouvernance en identifiant les zones de responsabilités entre le client et le fournisseur en fonction du type de service souscrit : IAAS, PAAS, SAAS.... et du type de cloud choisi : public, privé ou hybride même si le modèle public avec une infrastructure partagée avec d'autres clients et ne prenant pas en compte les contraintes et obligations du secteur financier n'est clairement pas adaptée à ce secteur.

Données

La directive RGPD implique implicitement de choisir un fournisseur de solution cloud (C.P.) qui est localisé en Europe plutôt qu'aux Etats Unis afin d'éviter toute fuite intempestive de données même si cela ne le garantit pas. Les discussions entre les GAFAM et les instances Européennes suivent leurs cours.

Confidentialité

Même hébergé en Europe, la confidentialité des données doit être garantie par le CP en proposant un système de clef de chiffrement et de déchiffrement, pouvant être gérée directement par le client avec une délégation (si nécessaire encadrée par le contrat et validé par le service juridique du client).

Réversibilité

Au-delà des aspects financiers, les particularités des fournisseurs de cloud sont à regarder dans le détail, surtout dans le cadre de la réversibilité, lorsque le client souhaite changer de fournisseur.

A titre d'exemple, les CP proposent peu ou prou les mêmes services mais avec des particularités propres à leur stack technologique ou à leurs processus interne.

Chaque CP propose une solution propre pour gérer le déploiement d'applications et autres services au sein de leur cloud, le modèle devops indispensable et permettant de supporter le modèle Agile et l'innovation des entreprises.

Une entreprise qui souhaiterait, dans le cadre de la résilience, être client de deux fournisseurs de cloud devra adapter son Target Operating Model (T.O.M.) et payer un coût supplémentaire pour cette adaptation. Une contrainte que le projet GAIA-X adresse dans le cadre de la portabilité.

PARTIE 6

Panorama de la cyber résilience à l'échelle mondiale

EGE Ecole de Guerre Economique

6.1 Influence des superviseurs et régulateurs sur la cyber-résilience mondiale

Afin de maintenir un haut niveau de cyber résilience dans le système financier britannique et garantir la stabilité financière du pays, la Banque Centrale britannique a développé plusieurs outils et a été précurseur en matière de framework dédié pour l'analyse des menaces ou Threat Intelligence.

Parmi ces outils, deux sont impactant

CBEST **&** **CQUEST**

CBEST

Il s'agit d'un cadre développé en 2014 pour effectuer des tests à chaud basés sur des scénarios de threat intelligence utilisés par des hackers sur les systèmes critiques en production. Il s'agit aujourd'hui de la première méthode utilisée dans le secteur financier britannique pour tester volontairement leur capacité de défense.

Le framework CBEST pour une institution financière apporte les avantages suivants :

- Accès à des compétentes, savoir-faire issu du cyber threat intelligence,
- Des tests d'intrusion réalistes qui reproduisent des attaques sophistiquées à jour,
- Des indicateurs clés pour évaluer la maturité et la capacité de l'institution à détecter les cyberattaques et à y réagir,
- Accès à des informations de référence qui peuvent être utilisées pour évaluer d'autres parties du secteur financier.

« ***La mise en œuvre de CBEST aidera les conseils d'administration des sociétés financières, les fournisseurs d'infrastructures et les régulateurs à mieux comprendre les types de cyberattaques qui pourraient nuire à la stabilité financière au Royaume-Uni, la mesure dans laquelle le secteur financier britannique est vulnérable à ces attaques et l'efficacité des processus de détection et de recouvrement*** », *a déclaré la Banque Centrale d'Angleterre.*

CQUEST

Ce questionnaire sert à évaluer le niveau de maturité en matière de cyber résilience d'une institution financière sous forme d'auto-évaluation.

Les questions peuvent être par exemple :

- Les fonctions métiers sont-elles comprises ?

- Un inventaire actuel des actifs informationnels avec les systèmes de support est-il maintenu ?

- Comprenez-vous qui sont vos fournisseurs tiers et les services qu'ils fournissent ?

Le résultat est une carte synthétique de la capacité de cyber-résilience de la structure qui met en évidence tous les domaines d'amélioration.

Le template CQUEST de 48 questions est accessible via le site de la Bank Of England.

Le directeur général adjoint des opérations règlementaire de la banque centrale d'Angleterre Lyndon Nelson a présenté, lors du 8ème sommet sur la résilience opérationnelle et la cyber-sécurité de City & Financial, le cyber risque de 2015 à 2027.

Dans son discours, Lyndon Nelson parle des mesures prises par la Banque Centrale d'Angleterre : dans une première partie, un retour d'expérience sur le voyage parcouru de 2015 à 2021. Le travail réalisé jusqu'à ce jour se focalise sur les trois points essentiels suivants :

- des exercices de simulation
- des tests d'intrusion
- une collaboration internationale

La Banque Centrale d'Angleterre a récemment travaillé avec la Banque Centrale Européenne (BCE) et d'autres autorités européennes pour mener des CBEST sur une base intergouvernementale et ainsi s'aligner sur des cadres similaires tels que TIBER-EU.

L' Angleterre devient un leader mondial via son programme d'exercice, renforcé par la création du Cross Market Operational Resilience Group (CMORG) dont la fonction est de promouvoir la résilience du secteur financier. Les exercices vont au-delà des frontières avec un premier exercice de coordination au sein du G7 (auquel ont participé 23 autorités financières).

Les exercices de tests et l'expérience du déploiement de CBEST démontre que 80% des attaques proviennent d'une insuffisance en matière d'hygiène informatique. L'ensemble des entreprises petites et grandes sont concernées.

Sur la deuxième partie de son discours sur « ***le voyage à venir 2021-2027 et au-delà*** », Lyndon Nelson compare les cyber-risques au dessin Escher « ***les marches de Penrose où l'on monte constamment les escaliers et n'atteint pas le sommet*** ».

Les cyber-attaquants arrivent à dépasser constamment les limites, qu'elles soient techniques ou géographiques. A titre d'exemple, l'attaque au cours de laquelle les cybercriminels se sont coordonnés sur l'utilisation sur des guichets automatiques dans vingt-trois pays différents et neuf fuseaux horaires en deux fenêtres de 45 minutes : « ***si l'adversaire peut coordonner au-delà des frontières, alors nous devons en faire autant*** ».

Il met l'accent sur la nécessité de poursuivre les actions en relevant la nécessité de la collaboration à l'échelle internationale pour atteindre le sommet, notamment en s'appuyant sur la publication récente des principes du Comité de Bâle sur la résilience opérationnelle.

Les attentes de la Banque Centrale Britannique pour le forum 2027 sur la cyber résilience sont les suivantes :

- Que toutes les entreprises traitent la cyber-sécurité comme un risque commercial pour lequel leur conseil d'administration est pleinement engagé,
- Les entreprises visent à être une cible difficile pour les cyberattaques, mais partant du principe qu'une défaillance se produira, elles sont prêtes et ont testé leur capacité à récupérer leurs services critiques dans des délais raisonnables,
- La gestion des cyber risques est bien établie en tant que processus collectif. Cela comprend le partage actif de l'information ainsi que le renforcement de capacités communes,
- Que les entreprises reconnaissent pleinement leur cyber défiance et travaillent avec leurs fournisseurs pour identifier, évaluer et atténuer les vulnérabilités qu'elles apportent,
- Que la confiance entre les organismes de réglementation et les entreprises réglementées demeure forte pour contribuer à une réponse aux incidents solides et agiles ;

Enfin, la Banque Centrale du Royaume-Uni, à travers sa collaboration à l'échelle internationale ainsi que sa participation à l'élaboration de TIBER-EU auprès de la BCE, affirme sa volonté de devenir d'ici 2030 une référence pour le secteur des services financiers.

A l’échelle
Internationale

A l’échelle internationale une minorité de pays ont également élaboré leurs propres socles règlementaires dédiés à la cyber résilience pour leurs secteurs financiers. Ci-dessous un panorama de l’ensemble des standards qui évoluent dans le monde.

Etats-Unis

La résilience opérationnelle fait partie des priorités pour les régulateurs financiers américains. Deux acteurs travaillent activement sur le sujet :
•*La Federal Reserve*
•*L’Office of the Controller of the Currency*

En 2019 l’OCC a inclus dans leur plan de supervision pour la résilience opérationnelle la partie cyber-sécurité comme action clé avec un accent sur le maintien de la sécurité des systèmes IT et la résolution des problèmes identifiés dessus. Le Framework NIST a inspiré les standards américains existants pour la cyber résilience opérationnelle dans le secteur bancaire.
Le framework NIST est un cadre avec un ensemble de ligne directrice pour atténuer les risques cyber qui s’applique pour tous les organismes.

Le Federal Reserve Framework est utilisé pour la supervision des processus IT. La mise en place d’un plan de continuité d’activité est également à disposition des institutions financières pour améliorer leurs cyber résilience.

L’OCC publie et mets à jour des normes et règles pour sécuriser les systèmes IT du secteur financier.

Le Financial Service Sector Coordinating Council publie des directives à destination des institutions financières afin qu’elles puissent assurer leurs résiliences et la restauration de leurs services métiers.

Le Federal Financial Institution Examination Council (FFIEC) publie des directives pour renforcer la résilience des services de prestations.

HONG-KONG

A Hong Kong le secteur financier utilise le Framework Intelligence-led Cyber Attack Simulation Testing (iCAST) de l'HKMA (Hong Kong Monetary Authority) afin d'assurer leur cyber résilience.

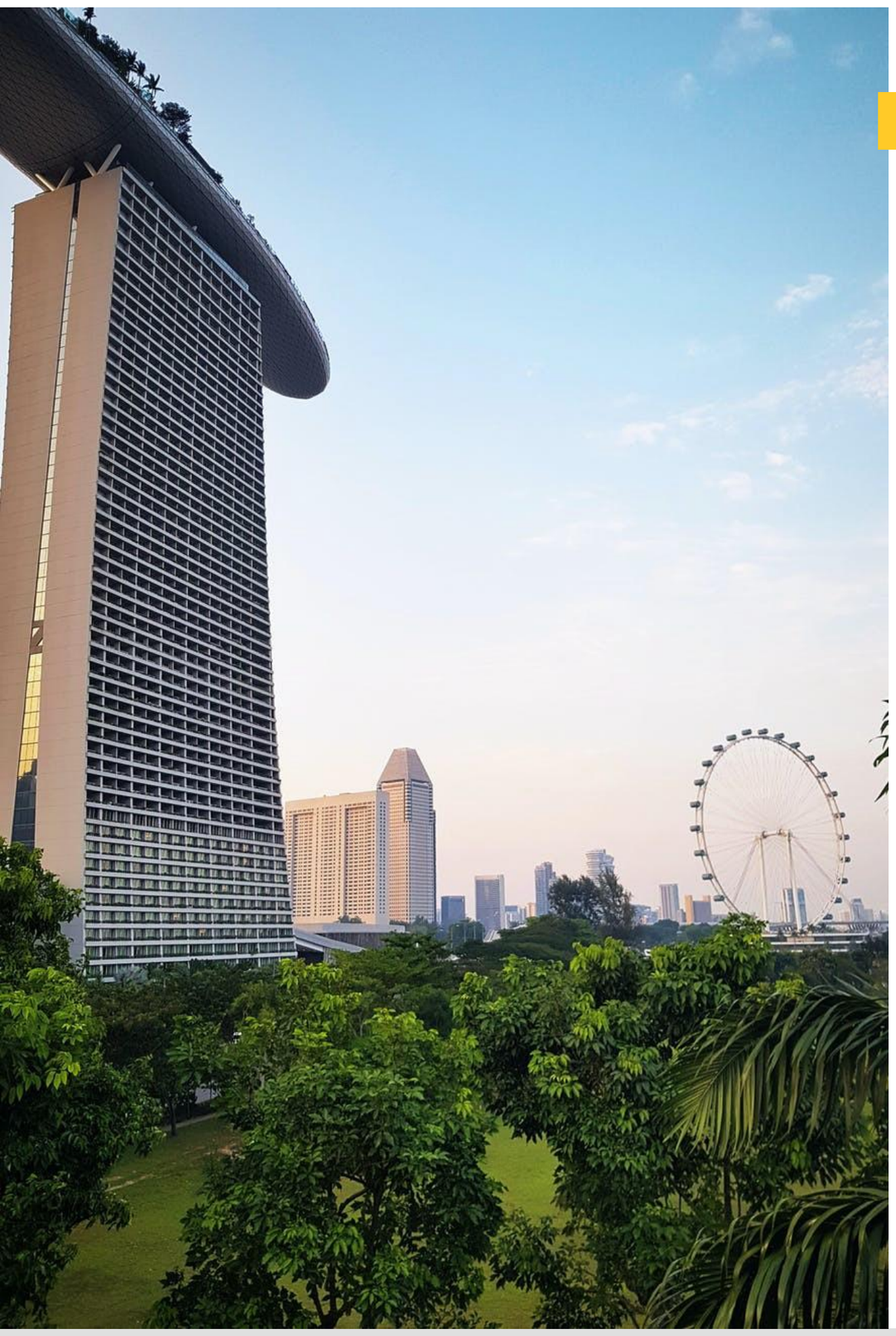
SAUDI ARABIE

Le Financial Entities Ethical Red-Teaming de la Saudi Arabian Monetary Authority est un framework désigné à destination des institutions financière en Arabie Saoudite.

AUSTRALIE

Les institutions financières australiennes utilisent quant à elles le Framwork Cyber Operational Resilience Intelligence-led Exercises (CORIE) pour faire leurs tests de résilience.

L'Australian Prudential Regulation Authority (APRA), en qualité de régulateur, propose des standards pour traiter les risques dans chaque domaine : les risques opérationnels, la sécurité IT, les plans de continuité et les risques externes.



SINGAPOUR

Les organismes bancaires à Singapour ont pour Framework Red Team : l'Adversarial Attack Simulation Exercises proposé par ABS (Association of Banks of Singapore) pour que les organismes renforcent leurs exercices de résilience.

Le Monitary Autority Of Singapore publie régulièrement plusieurs normes en matière de risque IT et cyber-sécurité ainsi que des guides pour la mise en place d'un plan de continuité d'activité.

EUROPE

TIBER Framework est le premier framework européen commun, un cadre qui peut être exploité par n'importe quel pays de l'Union européenne et offre une reconnaissance mutuelle et inter-juridictionnelle des engagements de l'équipe rouge pour les exercices de résilience.

ECB guidance pour le management des parties tiers et ECB guidance Cyber resilience oversight expectations (CROE) pour les infrastructures des marchés financiers (FMI).

Dans la majeure partie des pays dans le monde, les différents acteurs du secteur financier superviseurs, régulateurs, FMI ont la même approche en termes de gouvernance et de framework pour la cyber résilience opérationnelle.

Mais nous pouvons constater des écarts en termes de choix dans les domaines d'applications et sur les détails des règles à appliquer selon le framework utilisé.
A ce jour les normes de la cyber résilience sont abordées à l'échelle internationale uniquement sur des déclarations de principes de haut niveau.
Cet écart se justifie notamment à cause du manque d'un accord commun en matière de standard international unique qui puisse s'appliquer pour l'ensemble des acteurs financiers de façon transfrontalière.

Le défi à venir d'ici 2030 sera essentiellement de faire émerger les différents standards existant dans le monde du secteur financier afin de fournir un standard de cyber résilience internationale applicable de façon transfrontalière.

Les avantages d'un standard unique pour tous consistent à tirer parti de quelques cadres afin d'avoir une approche fondée sur les bonnes pratiques qui ont été testées et approuvées par un très grand nombre d'institutions, ce qui permet d'avoir une cohérence entre les processus et les systèmes qui s'étendent à plusieurs organismes de façon transfontalière avec moins de contrainte juridictionnelle.

Stantard international dans le secteur financière

G-7 Éléments fondamentaux pour les tests d'intrusion axés sur les menaces - le Groupe des 7 pays a fourni des conseils sur la réalisation de tests d'intrusion axés sur les menaces.

En juin 2016 The Committee on Payments and Market Infrastructures (C.P.M.I.) et le Board of the International Organization of Securities Commissions (I.O.S.C.O.) ont publié leur guide sur la cyber résilience pour les FMI ("Cyber Guidance"). Il s'agit d'une première orientation cyber approuvée à l'échelle internationale pour l'industrie financière.

Dans le cadre de l'utilisation réglementaire des tests d'intrusion et du red teaming dans le secteur des services financiers -Global Financial Markets Association (G.F.M.A.) et compte tenu de toutes les exigences réglementaires imposées par le pays, la Global Financial Markets Association a entrepris de créer un cadre mondial qui répondrait aux exigences réglementaires de plusieurs pays.

D'autres pays sont plus susceptibles de suivre l'approche émergente du Royaume-Uni CBEST ou celle de la BCE TIBER-EU, par exemple, une fois que les normes internationales auront évoluées dans cette direction.
Les entreprises devront donc continuer à ce stade à maintenir une conformité à des exigences règlementaires multiples.

A l'échelle internationale, la majorité des guides, frameworks développés pour la cyber résilience dans le secteur financier se sont inspirés des différents cadres et méthodologies exploités par plusieurs industries.

COBIT 5

ISO/IEC 27002

NIST cybersecurity Framework

FFIEC

PFMI

PARTIE 7

Focus sur l’influence des superviseurs Européen et Français

EGE Ecole de Guerre Economique

7.1. Résilience et sécurité Européenne

Le secteur financier est particulièrement exposé avec le développement soutenu de la dématérialisation : les évolutions technologiques ont permis de réduire certains risques opérationnels (notamment d'exécution) mais avec l'expansion des technologies dont le cloud pour l'avenir, l'ouverture des systèmes d'informations aux échanges extérieurs. Le secteur financier devient un terrain de jeux pour les cybercriminels et leurs attaques qui sont de plus en plus sophistiquées.

En partant de la sécurité vers la résilience, il est devenu un enjeu majeur pour les infrastructures de marché européens d'assurer la stabilité financière. La sécurité et la stabilité financière qui en découle font partie de la mission principale de la Banque Centrale Européenne, les Banques Centrales nationales et les régulateurs.

Depuis 2016, la cyber résilience devient un sujet d'attention, les trois acteurs de l'Euro système travaillent ensemble à l'élaboration d'un cadre européen afin d'assurer la résilience des infrastructures de marché. Ils ont ajusté au fil des années leurs gouvernances et programmes de travail pour relever le défi de la disponibilité, de la sécurité et de la continuité de ses activités.

Leurs interventions s'articulent autour de plusieurs volets : réglementaires, introduction de frameworks, et publication de guides.

Un projet d'envergure de renforcement de la cyber-résilience a été également mis en œuvre, il s'agit du Cyber Resilience Enhancements, connu avec l'acronyme CRE.

Au sein du MIB (Market Infrastructure Board), organe décisionnel rattaché au Conseil des Gouverneurs, la BCE et les 4CB (Banque de France, Banque d'Italie, Banque d'Espagne et Deutsche Bundesbank) ont intégré cette dimension « Cyber résilience » pour l'ensemble des services de paiements comme TARGET. Les 4CB ont présenté 4CR visant dans ce cadre qui couvre quatre volets du cyber résilience :

- CRE Security testing
- CRE Security services
- CRE Recovery
- CRE Software integrity

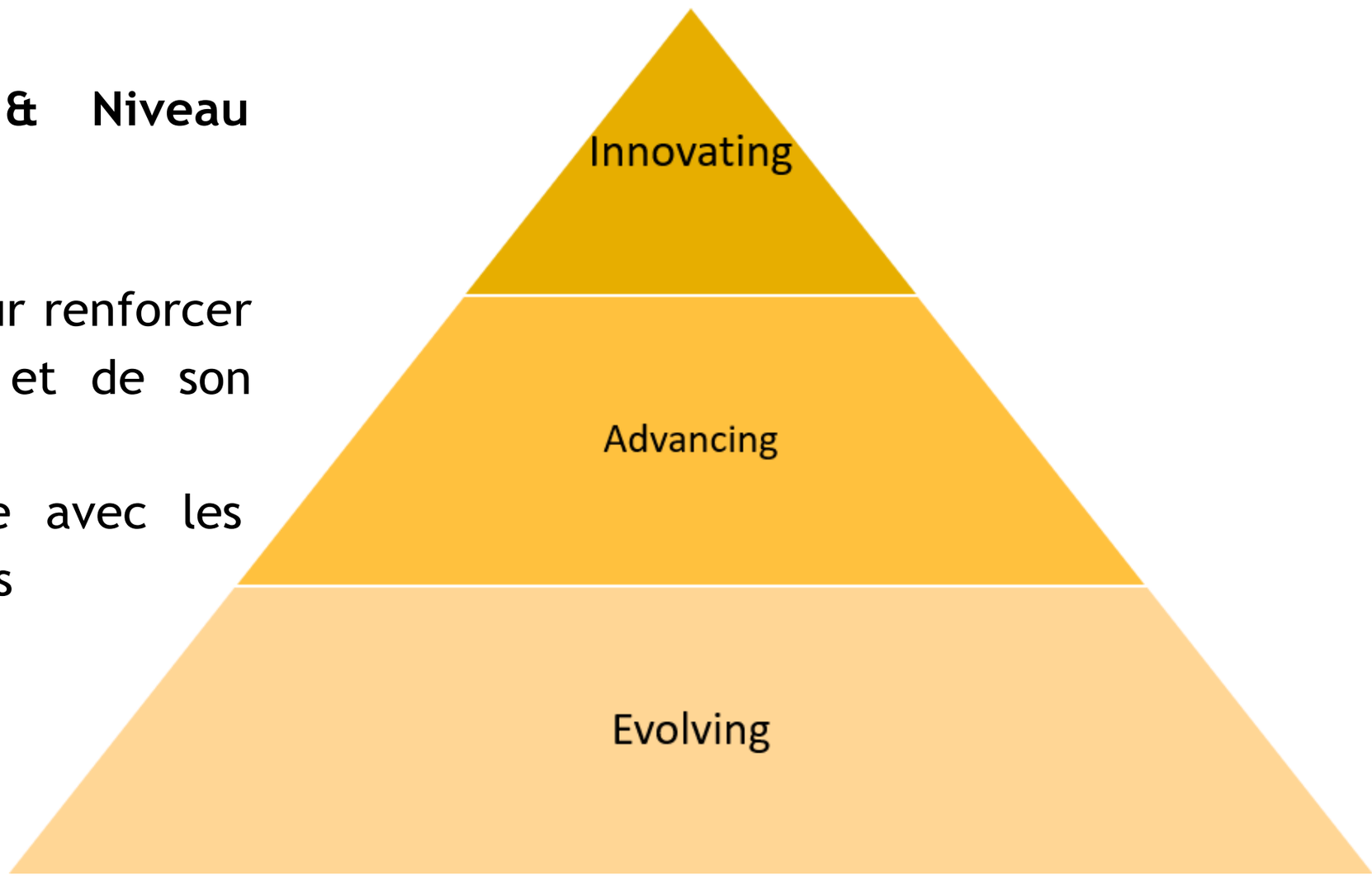
En juin 2020, dans le but de renforcer la gestion du risque opérationnel, le MIB a opté pour le modèle international « directive en 3 lignes », aussi utilisées par la Banque de France, définissant l'organisation des fonctions de gestion du risque opérationnel et de la sécurité pour l'ensemble des TARGET Services. Publié par l'Institute of International Auditor (I.I.A.), le modèle des trois lignes de défense a pour objectif de fournir la gouvernance afin de clarifier les rôles et les responsabilités en matière d'activités dans l'entreprise.

À l'horizon 2023 il sera complété par un nouveau cadre de référence pour la cyber-sécurité et la sécurité de l'information ECRIS framework (Eurosystem Cyber Resilience and information Security) qui a pour objectif de couvrir l'ensemble des exigences exprimés par les régulateurs (règlement SIPS), par la fonction de surveillance à travers la cyber résilience « oversight expectation 'CROE' », et doit intégrer le CRE (Cyber Resilience Enhancements).

L'objectif de CROE n'est pas la conformité, mais de protéger l'écosystème financier. Le guide permet aux FMI de mettre en œuvre et aux surveillants d'évaluer le degré de conformité des FMI, grâce à un ensemble de bonnes pratiques qui servent de référence. La particularité de CROE est de donner la possibilité pour chaque institution d'auto-évaluer sa progression de niveau de maturité de la cyber résilience et de gouvernance. Il s'agit d'une approche à trois niveaux de maturité.

Niveau Évolutif plus & Niveau Avancé Plus

- Capacités évolutives pour renforcer la résilience de la FMI et de son écosystème
- Collaboration proactive avec les parties prenantes externes



Niveau Évolutif Plus

- Pratiques évaluées et optimisées
- Application des éléments de sécurité harmonisée pour gérer les risques cyber dans l'entreprise
- Stratégie de cyber résilience et cadre approuvés
- Eléments essentiels présents et maintenus en condition
- Performance et pratiques surveillées et gérée

En matière de gouvernance, le CROE propose

5 risk management categories:

Governance
Identification
Protection
Detection
Response and recovery

3 overarching components

Testing
Situational Awareness
Learning and evolving

La Banque de France en qualité de banque centrale et garant de la stabilité financière ajoute à cette première série d'exigences européenne l'élaboration de nouvelles exigences en matière de cyber-sécurité dont les principales sont les suivantes :

- Le renforcement de la maîtrise des risques, à travers une stratégie cyber dédiée. Celle-ci doit encadrer une analyse régulière du panorama des menaces cyber ainsi qu'une gouvernance associant tous les acteurs (business, finance, gestion des risques, IT, etc.),
- Des obligations de tests renforcés, sur la base de scénarios constamment réactualisés de menaces cyber et de simulations d'attaques (red team tests).
- Une forte innovation, à travers une évolution permanente des technologies utilisées et le maintien en condition de sécurité de l'ensemble des composants des systèmes d'information,
- La protection de l'intégrité des données transitant par les plateformes (dans le respect du règlement général de protection des données (RGPD).

7.2. CONTRIBUTION DE LA BANQUE DE FRANCE

La banque de France à travers son plan « **construire ensemble 2024** » met un accent particulier sur la cyber-sécurité et la résilience avec une ligne d'objectif dédié à atteindre par la banque :

« **Renforcer et renouveler notre résilience collective** ».

Les actions qui y sont principalement couvertes sont :

- ***Préparer les unités à faire face à des chocs dont l'expérience montre que leur nature, leur intensité et leur durée sont difficilement prévisibles,***
- ***Gérer les crises lorsqu'elles surviennent,***
- ***Créer les conditions de retour à un mode de fonctionnement nominal une fois les crises terminées.***

Le responsable de la continuité des activités de la Banque de France supervise les travaux conduits par l'ensemble des unités de la Banque pour renforcer la résilience interne.

Dans le discours de clôture sur « ***les enjeux de la résilience opérationnelle pour le système financier*** »

Le sous-gouverneur Denis Beau soulève l'enjeu de la dimension « **cyber** » pour la résilience opérationnelle de demain du secteur bancaire. L'ensemble de l'écosystème financier est l'objet d'attaque cyber, c'est pourquoi depuis déjà plusieurs années la cyber résilience est discutée à l'échèle internationale et européenne comme avec le projet réglementaire DORA.

« ***Toutes ces évolutions réglementaires sont bienvenues, car elles permettront aux institutions financières de mieux identifier les menaces… Il est primordial que les superviseurs échangent sur leurs meilleurs pratiques, partagent leurs expériences*** ».

Entrevue avec un expert de la cyber résilience de la Banque de France au sein de l'Eurosytème : M. L.

Quelle sont les actions de la Banque de France en termes de cyber résilience jusqu'à ce jour ?

Le trajet a commencé en juin 2016 avec un document fondamental (CPMI-IOSCO) avec leur publication de Guidance cyber pour les FMI afin que celui-ci soit appliqué immédiatement auprès de l'ensemble des acteurs financiers.

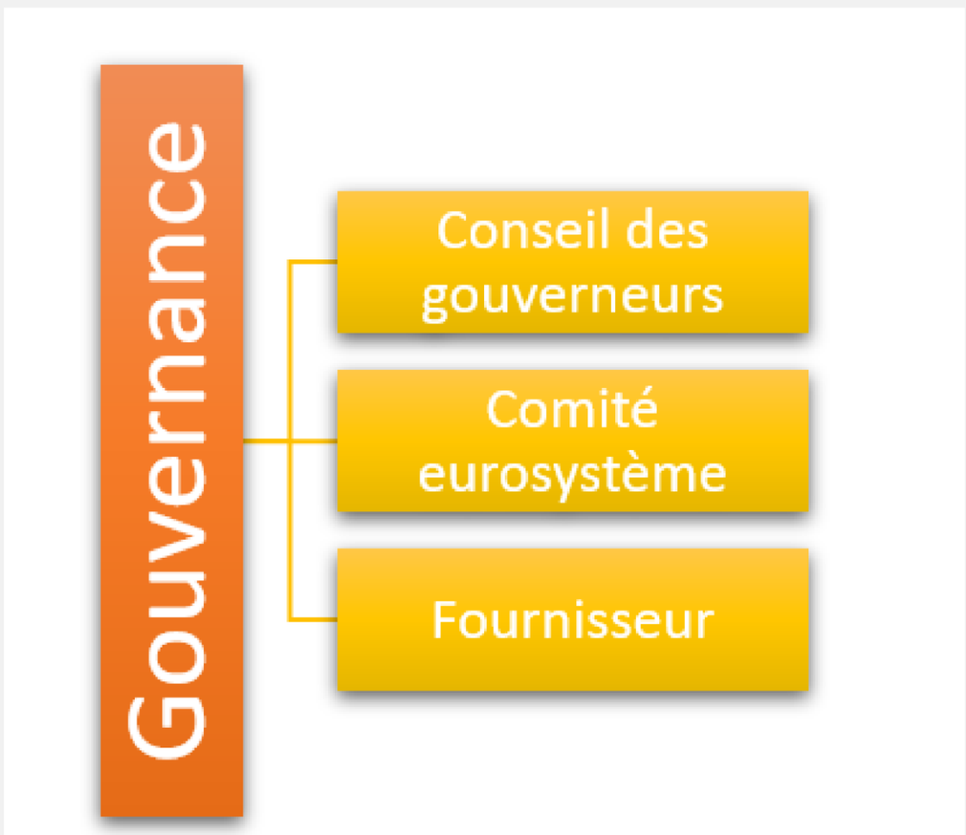
En juin 2017 la BCE et les 4CB ont proposé leur plan de réponse au CMPI-IOSCO et en 2018 un budget de plusieurs millions d'euros a été débloqué pour mettre en place la cyber résilience. La BCE a poursuivi ses travaux sur le CROE « Cyber Resilience Oversight Expectations », dont l'objectif est de mettre en œuvre la guidance de CMPI-IOSCO qui a été publié en 2018.

La Banque de France en décembre 2018, à la suite de la publication de CROE, aurait dû atteindre le niveau « Advancing » qui a finalement été atteint sur TARGET en 2021 et les travaux se poursuivent dans le cadre de T2S en 2022.

Quelles sont les interventions de la Banque de France à l'échelle européenne ?

Et en termes de gouvernance la Banque de France a opté pour le modèle en trois lignes de défenses : une première ligne pour l'opérationnel, une deuxième pour la gestion des risques et une troisième pour l'audit. Et justement « j'interviens au niveau de cette deuxième ligne au sein du Risk Management Coordination Group ».

Gouvernance au sein de l'Eurosystème



Nous intervenons en tant que banque centrale en qualité de client au sein du comité de l'Eurosystème et également en qualité de fournisseur faisant parti du 4CB.

Depuis 2020 ERCB est composé de plus grandes institutions financières d'Europe, qui se sont unis dans le cadre du dispositif appelé Initiative pour le partage des cyber-informations et des cyber-renseignements (Cyber Information and Intelligence Sharing Initiative, CIISI-EU). La Banque de France fait partie du comité ECRB représenté par la directrice générale de la DGSO.

Quelles sont les projets à venir jusqu'en 2030 concernant le cyber résilience ?

> L'objectif en termes de cyber résilience est de poursuivre les travaux afin que la Banque de France puisse atteindre le niveau « Evolving » de CROE d'ici 2030. La poursuite des travaux concernant ECRIS Framework d'ici 2023, puis sa mise en place dans les années à venir.

Et le Framework TIBER, où en est la Banque de France ?

> Pour avoir le niveau « Advancing » de CROE il est obligatoire d'appliquer le Framework TIBER et faire appel à une société tierce pour la partie Threat intelligence.
> Par rapport au framework TIBER-EU, la banque de France n'a pas déployé encore le TIBER-FR. Il faut savoir que la difficulté de TIBER est de couvrir l'ensemble de l'écosystème afin de faire des tests de bout en bout. Aujourd'hui les tests TIBER ciblent des systèmes spécifiques. Nous pouvons bien sûr d'ici 2030 s'attendre à des évolutions et un déploiement TIBER-FR n'est pas à exclure.

CONCLUSION

La Cyber résilience du secteur bancaire et du secteur de la finance reste une préoccupation majeure de l'institution européenne et des gouvernements des Etats membres afin d'assurer la stabilité de l'économie européenne mais aussi mondiale du fait de la globalisation des échanges et des flux financiers.

Le monde financier a toujours suscité beaucoup d'interrogations quant à sa capacité à rebondir après une crise majeure. Très longtemps focalisée sur le risque de pertes financières, la cyber-sécurité devient une priorité dans le quotidien des acteurs bancaires et dans leur projection du fait des enjeux majeurs dans un monde allant toujours vers plus de digitalisation et entrainant mécaniquement une augmentation des surfaces d'attaques.

Les Britanniques ont compris très tôt l'importance de la cyber résilience, Londres étant la deuxième place financière mondiale en termes de volume de transactions.

Conserver l'attractivité de leur marché et potentiellement avoir un levier différenciant sur le plan commercial en comparaison d'autres places de marché et à minima s'assurer que la cyber résilience ne soit pas un facteur discriminant pour les acteurs institutionnels.

Le constat passé de l'UE sur la résilience opérationnelle est l'absence de proposition de règles détaillées et exhaustives dans ces guidances. Auxquelles s'ajoutent l'absence de coordination au niveau national pour une mise en pratique efficiente de ces règles européennes. Cette situation devient problématique pour le maintien d'un marché unique, complexifie la stabilité du secteur financier de l'UE et fragilise la sécurité des consommateurs et des investisseurs.

Au travers du discours d'Ursula von der Leyen sur l'état de l'Union en 2021, l'Union Européenne affirme sa volonté de pallier ces problématiques : « Si tout est connecté, tout peut être piraté. Les ressources étant rares, nous devons unir nos forces. [...] C'est pourquoi nous avons besoin d'une politique de cyber- défense européenne, notamment d'une législation établissant des normes communes dans le cadre d'une nouvelle loi européenne relative à la cyber- résilience. »

Lyndon Nelson dans son discours partage cette même vision pour le Royaume Unis lors du huitième sommet sur la résilience opérationnelle et la cyber- sécurité de City & Financial.

Nous pouvons relever que ces deux leaders au sein de l'Europe partagent les mêmes ambitions concernant la politique à mettre en place en Europe sur le sujet de la cyber-sécurité : « L'Europe doit devenir un leader en matière de cyber-sécurité »

Pour atteindre cette ambition, l'UE doit se doter d'une véritable doctrine en matière de cyber-défense. Et la résilience étant le point clé d'une cyber-défense, l'UE au cours de ces dernières années a mis en place des mesures drastiques à travers des directives et réglementations, en particulier avec le règlement Digital Operational Resilience Act (D.O.R.A).

La publication du DORA par l'UE à la suite de la directive NIS a pour objectifs de répondre à cette problématique en harmonisant les règles applicables à travers ses cinq piliers et de répondre également au manque de coordination au niveau national grâce aux implications des Autorités Européennes de Surveillance (AES) dans le respect des obligations énoncées dans le DORA.

Chaque Etat décide de l'autorité compétente pour la mission de surveillance et l'application des sanctions. Sachant qu'avec le DORA les exigences seront appliquées de manière proportionnelle en fonction de la taille et de la nature des activités de l'entreprise considérée.

En France, cette mission de surveillance est assurée par la Banque de France à travers l'Autorité de Contrôle Prudentiel et de Résolution (ACPR).

Les sanctions envisagées par le DORA en cas de non-conformité sont de deux types : sanctions administratives et mesures correctives. Les Etats membres peuvent également décider d'instaurer des sanctions pénales à condition que les mesures appropriées soient mises en place.
Les secteurs financiers ayant déjà implémenté le NIS pourront plus facilement adapter leurs programmes organisationnels et techniques selon le règlement du DORA.

La force de ce cadre législatif européen reste incontestablement la préparation des banques aux tests d'intrusions, dont l'objectif est de mettre en conditions réelles les hommes et les ressources techniques, d'éprouver leur résistance et de les confronter à la réalité d'une cyber résilience.

Les cadres règlementaires nationaux, supra nationaux et internationaux ont besoin de converger vers un socle commun, robuste, garantissant les intérêts des citoyens et la stabilité du système financier à l'échelle mondiale.

Ces cadres représentent un levier important pour les CISO afin d'obtenir des budgets auprès des membres du COMEX mais cette garantie de moyen ne doit pas les empêcher de partager régulièrement avec ces derniers des détections de fraudes par exemple afin de démontrer la pertinence des investissements technologiques. La technologie reste, sans conteste, un des piliers de la cyber résilience.

L'économie mondiale progresse à grands pas vers une humanité robotisée. L'intelligence artificielle contribue à la fois à l'essor de solutions défensives plus pertinentes en mesure de mieux contrer les attaquants mais également plus agiles dans l'adaptation continue à la complexité et la créativité des nouvelles attaques.

De l'autre côté du miroir, l'intelligence artificielle est également utilisée par les attaquants afin de faciliter les tentatives de piratage mais aussi afin de comprendre les modèles de défenses mises en place par les entreprises et ainsi les contourner.

La nature même des organisations de hackers, organisations transfrontalières, rend difficile la pénalisation de leur activité, une approche dans le domaine juridique à l'échelle internationale pourrait pallier ce problème mais reste peu probable sur le court et moyen terme du fait d'intérêt divergeant au sein de la communauté internationale.

Assureurs traditionnels et spécialisés sensibilisent leurs clients et façonnent des produits sur mesure, la cyber criminalité générant de plus en plus de revenus.
Notre échange avec un agent général (Axa Naïma KHROUSSA) nous confirme cette orientation du marché vers la protection des entrepreneurs mal informés des risques cyber. Son passé de DSI, lui permet de conseiller à la fois sur le plan prévoyance mais, également sur la protection des actifs de ses clients.
Un des éléments clef de la cyber résilience sera lié à l'hébergement des services financiers par les Cloud Provider.

La mise en adéquation des offres d'hébergements avec les exigences règlementaires sera un gage de confiance pour les clients mais sera également perçu comme un élément important pour le Time2Market pour les activités B2B et leurs services juridiques, achats, cyber...

L'éducation constitue le socle principal via la sensibilisation du grand publique face à ce fléau de cybercriminalité.
A ce titre, le plan d'investissement massif France 2030 a prévu 140 millions d'euros pour répondre aux besoins en formation.
Campus cyber est également un exemple de prise de conscience étatique, puisque initié par le président de la République et qui fait suite à l'initiative d'Israël et de leur cyber-campus de Beer Sheva. Sur un espace commun du quartier d'affaires de la défense, sont réunis progressivement les acteurs spécialisés du domaine : les services étatiques, les sociétés technologiques et les centres de formation.

La cyber résilience bancaire atteindra un niveau de maturité dans les dix années à venir, car les politiques de la banque centrale, les investissements des Etats et la prise de conscience de la société civile, apporteront non seulement les réflexes nécessaires au quotidien mais également l'intelligence attendue pour contourner les attaques en déjouant les stratégies lancées.

ANNEXE

EGE Ecole de Guerre Economique

Annexe

Les entités financières visées par DORA

Les entités financières visées par DORA		
Les établissements de crédit	Les plates-formes de négociation	les institutions de retraite professionnelle
Les établissements de paiement	Les référentiels centraux	les agences de notation de crédit
Les établissements de monnaie électronique	Les gestionnaires de fonds d'investissement alternatifs et	les contrôleurs légaux des comptes et les cabinets d'audit
Les entreprises d'investissement	les sociétés de gestion	les administrateurs d'indices de référence d'importance critique
Les prestataires de services sur crypto-actifs, les émetteurs de crypto-actifs, les émetteurs de jetons	Les prestataires de services de communication de données	les prestataires de services de financement participatif
Les dépositaires centraux de titres	Les entreprises d'assurance et de réassurance	les référentiels des titrisations
Les contreparties centrales	les intermédiaires d'assurance, les intermédiaires de réassurance et les intermédiaires d'assurance à titre accessoire	les tiers prestataires de services informatiques

Description détaillée des piliers de DORA

	Gestion des risques liés aux (TIC) (articles 4 à 14)	Gestion, classification et notification des incidents liés à l'informatique ; (articles 15 à 20)	Tests de résilience opérationnelle numérique (articles 21 à 24)	Gestion des risques liés aux tiers prestataires de services informatiques (articles 25 à 39)	Partage d'informations (article 40)
Objectifs visés par DORA à travers ces piliers	• mettre en place et maintenir des systèmes et des outils informatiques résilients afin de réduire au minimum l'incidence des risques informatiques, • identifier les sources de risques informatiques et adopter des mesures de protection et de prévention, • de détecter rapidement les activités anormales, • instaurer des politiques de continuité des activités et des plans de rétablissement après sinistre	• assurer une surveillance, un traitement et un suivi cohérents et intégrés des incidents liés à l'informatique, afin de déterminer et de supprimer les causes profondes pour éviter que de tels incidents ne se (re)produisent.	• évaluer l'état de préparation en cas d'incidents liés à l'informatique, recenser les faiblesses, les défaillances ou les lacunes en matière de résilience opérationnelle numérique afin d'être en mesure de mettre rapidement en œuvre des mesures correctives.	• permettre un suivi complet, par l'entité financière, du risque associé aux tiers prestataires de services informatiques tout au long des différentes étapes de leur relation, à savoir la conclusion du contrat, son exécution, sa résiliation et la phase post-contractuelle.	• Sensibiliser au risque informatique et renforcer les capacités défensives des entités financières et leurs techniques de détection des menaces grâce aux échanges des informations et des renseignements sur les cybermenaces.
Articles par pilier	• ***Art 4*** *: Gouvernance et organisation* • ***Art 5*** *: Cadre de gestion des risques informatiques* • ***Art 6*** *: Systèmes, protocoles et outils informatiques* • ***Art 7*** *: Identification* • ***Art 8*** *: Protection et prévention* • ***Art 9*** *: Détection* • ***Art 10*** *: Réponse et rétablissement* • ***Art 11*** *: Politiques de sauvegarde et méthodes de rétablissement* • ***Art 12*** *: Apprentissage et évolution* • ***Art 13*** *: Communication* • ***Art 14*** *: Harmonisation accrue des outils, méthodes, processus et politiques de gestion des risques informatiques*	• ***Art15*** *: Processus de gestion des incidents liés à l'informatique* • ***Art 16*** *: Classification des incidents liés à l'informatique* • ***Art 17*** *: Notification des incidents majeurs liés à l'informatique* • ***Art 18*** *: Harmonisation du contenu et des modèles des rapports de notification* • ***Art 19*** *: Centralisation des notifications d'incidents majeurs liés à l'informatique* • ***Art 20*** *: Retour d'information en matière de surveillance*	• ***Art 21*** *: Exigences générales applicables à la réalisation de tests de résilience opérationnelle numérique* • ***Art 22*** *: Test des outils et systèmes informatiques* • ***Art 23*** *: Tests avancés d'outils, de systèmes et de processus informatiques sur la base de tests de pénétration fondés sur la menace* • ***Art 24*** *: Exigences applicables aux testeurs*	❑ ***SECTION 1*** *: Principes clés pour une bonne gestion des risques lies aux tiers prestataires de services informatiques* • ***Art 25*** *: Principes généraux* • ***Art 26*** *: Évaluation préliminaire du risque de concentration informatique et autres accords de sous-traitance* • ***Art 27*** *: Principales dispositions contractuelles* ❑ ***SECTION 2*** *: Cadre de supervision des tiers prestataires critiques de services informatiques* • ***Art 28*** *: Désignation de tiers prestataires critiques de services informatiques* • ***Art 29*** *: Structure du cadre de supervision* • ***Art 30*** *: Tâches du superviseur principal* • ***Art 31*** *: Pouvoirs du superviseur principal* • ***Art 32*** *: Demande d'informations* • ***Art 33*** *: Enquêtes générales* • ***Art 34*** *: Inspections sur place* • ***Art 35*** *: Supervision continue* • ***Art 36*** *: Harmonisation des conditions permettant l'exercice de la supervision* • ***Art 37*** *: Suivi par les autorités compétentes* • ***Art 38*** *: Redevances de supervision* • ***Art 39*** *: Coopération internationale*	• ***Art 40*** *: Dispositifs de partage d'informations et de renseignements sur les cybermenaces*

Bibliographie

SOURCE

ANSSI, NIS : un cadre de coopération européen | Agence nationale de la sécurité des systèmes d'information (ssi.gouv.fr).

ANSSI. LES CERT FRANÇAIS. Disponible sur https: /www.ssi.gouv.fr/agence/cybersecurite/ssi-en-france/les-cert-francais/.

ASTIER, Stéphane et PAYEN, HUGUES, Projet de règlement DORA : renforcer la cybersécurité du secteur financier. Disponible sur Projet de règlement DORA : renforcer la cybersécurité du secteur financier (haas-avocats.com).

Bank for International Settlements, CPMI-IOSCO. "Guidance on cyber resilience for financial market infrastructures", disponible : https: /www.iosco.org/library/pubdocs/pdf/IOSCOPD535.pdf, Juin 2016.

Bank for international settlements. Basel Committee on Banking Supervision : Principles for operational resilience. Disponible sur Principles for operational resilience (bis.org), 31 mars 2021.

Bank of England " CBEST Intelligence-Led Testing CBEST Services Assessment Guide Version 2.0 ". Disponible : https: /www.bankofengland.co.uk/-/media/boe/files/financial-stability/financial-sector-continuity/cbest-services-assessment-guide, 2016.

Bank of England, bankofengland.co.uk. CQUEST - Cyber Resilience Questionnaire. https: /www.bankofengland.co.uk/-/media/boe/files/financial-stability/financial-sector-continuity/cyber-resilience-questionnaire.xlsx?la=en&hash=59AF930B27CB8A815C69B8A291AC80A1D2914A3F.

BEDOUCHA, Edouard. Directive NIS 1/2 : Quels enjeux juridiques ? Disponible sur Directive NIS 1/2 : Quels enjeux juridiques ? | Orange Cyberdefense, 7 mars 2019.

SOURCE

BEDOUCHA, Edouard. Directive NIS 2/2 : quels impacts pour les entreprises ? Disponible sur Directive NIS 2/2 : quels impacts pour les entreprises ? (orangecyberdefense.com), 8 mars 2019.

BOHIC, Clément. Cybersécurité : que pèse le marché en 2021 ? disponible sur Cybersécurité : que pèse le marché en 2021 ? | Silicon, 30 août 2021.

Bpifrance. 72 néo-banques ont vu le jour en 2020. Disponible sur 72 néo- banques ont vu le jour en 2020 (bpifrance.fr), 15 janvier 2021.

Bpifrance. Fintech : 100 millions d'euros dédiés aux startups de la finance. Disponible sur Fintech : 100 millions d'euros dédiés aux startups de la finance (bpifrance.fr), 21 janvier 2021.

Bpifrance. Fintech : DansNotreJargon : Fintech. Disponible sur #DansNotreJargon : Fintech (bpifrance.fr), 30 juillet 2018.

Capgemini. SILCA, filiale de Crédit Agricole S.A., modernise la gestion de ses infrastructures avec l'aide de Capgemini. Disponible sur SILCA, filiale de Crédit Agricole S.A., modernise la gestion de ses infrastructures avec l'aide de Capgemini – Capgemini France, 24 juin 2015.

CAPGRAS ETIENNE Etienne et VAN TIEGHEM Nicolas, Directive européenne NIS : quelle transposition dans le droit français et quel impact pour les entreprises ? https://www.riskinsight-wavestone.com/2018/09/bilan-directive-nis/.
Disponible sur Directive européenne NIS : quelle transposition dans le droit français et quel impact pour les entreprises ? - RiskInsight (riskinsight-wavestone.com), 2018.

SOURCE

COËFFE, Thomas. Infrastructures cloud : un marché en forte croissance, AWS domine, Azure progresse. Disponible sur Infrastructures cloud : un marché en forte croissance, AWS domine, Azure progresse (blogdumoderateur.com), 9 février 2022.

CROWDSTRIKE. WHAT IS AN ADVANCED PERSISTENT THREAT (APT)?. Disponible sur What is an Advanced Persistent Threat (APT)? | CrowdStrike, avril 2021.

CUVELLIEZ, Charles. Opinion | La résilience opérationnelle, nouveau cheval de bataille du comité Bâle. Disponible sur Opinion | La résilience opérationnelle, nouveau cheval de bataille du comité Bâle | Les Echos, 7 avril 2021.

Cybermalveillance.gouv.fr. Chiffres et tendances des cybermenaces : Cybermalveillance.gouv.fr dévoile son rapport d'activité 2021. Disponible sur Chiffres et tendances des cybermenaces : Cybermalveillance.gouv.fr dévoile son rapport d'activité 2021 - Assistance aux victimes de cybermalveillance, 08 mars 2022.

Denis BEAU, Banque de France, Réunion des superviseurs francophones "Les enjeux de la résilience opérationnelle pour le système financier". Disponible Les enjeux de la résilience opérationnelle pour le système financier | Banque de France (banque-france.fr), 09/12/2020,

DIAWARA, Amadou. Explorons DORA!, 22 mars 2021. Disponible sur Explorons DORA ! - Almond.

DUFOUR.T, VILEYN.M, FLICHE.O, DORLENCOURT.J, CLEMENT.G. Analyses et synthèses : La transformation numérique dans le secteur bancaire français N°131. Disponible sur Microsoft Word - 2021-EtudeNumBanque_VF3 (banque-france.fr).

DUPONCHEL, Matthieu et LUPONIS, David. Que retenir du projet de règlement DORA ? - Blog Mazars, 12 avril 2021. Disponible sur : https://www.mazars.fr/Accueil/Insights/Le-Blog/Que-retenir-du-projet-de-reglement-DORA.

SOURCE

Elastic. La recherche dans tous ses états. Disponible sur Recherche gratuite et ouverte : les créateurs d'Elasticsearch, de la Suite ELK et de Kibana | Elastic, 2022.

EUROPAEN CENTRAL BANK PUBLIC, EUROSYSTEM. Mandate of the Euro Cyber Resilience Board for pan-European Financial Infrastructures. Disponible : https://www.ecb.europa.eu/paym/groups/euro-cyber-board/shared/pdf/ECRB_mandate.pdf, 26 janvier 2018.

EUROPAEN CENTRAL BANK, EUROSYSTEM. Cyber resilience oversight expectations for financial market infrastructures. Disponible : https://www.ecb.europa.eu/paym/pdf/cons/cyberresilience/Cyber_resilience.pdf, Décembre 2018.

EUROPAGES. The B2B Sourcing Platform. Fabricant Producteur - éditeur de logiciels bancaires. Disponible sur Fabricant Producteur éditeur de logiciels bancaires | Europages.

EUROPEAN CENTRAL BANK. TIBER-EU FRAMEWORK : How to implement the European framework for Threat Intelligence-based Ethical Red Teaming. Disponible sur https://www.ecb.europa.eu/pub/pdf/other/ecb.tiber_eu_framework.en.pdf, mai 2018.

FEGHALI, Rami et TRAVERSES, Monique. Lettre d'actualité banque, Novembre 2020. Disponible sur : fr-france-pwc-newsletter-actualite-reglementaire- banque-22.pdf.

FLEURET, Nicolas. DORA, ou la résilience opérationnelle informatique. Disponible sur DORA, ou la résilience opérationnelle informatique - Le blog business (deloitte.fr), 19 octobre 2020 .

FranceFinTech. VUE DU SECTEUR. Disponible sur Barometres | France FinTech.

SOURCE

GAMELIN, Guillaume. A LA CONQUÊTE DE LA LOI SUR LA RÉSILIENCE OPÉRATIONNELLE NUMÉRIQUE DU SECTEUR FINANCIER. Disponible sur A la conquête de la loi sur la résilience opérationnelle numérique du secteur financier. Par Guillaume Gamelin, Directeur Général. (village-justice.com), 18 octobre 2021.

GAUDIAUT, Tristan. Cloud : les géants se partagent le marché. Disponible sur Graphique: Cloud : les géants se partagent le marché | Statista, 07 juillet 2021.

IBM. Présentation des régions multizones (MZR). Disponible sur Présentation des régions multizones (MZR) | Documentation IBM Cloud, 05 avril 2020.

JANIN, Samuel. PROTECTION DES INFRASTRUCTURES ET IMPLÉMENTATION DE TIBER-EU. Disponible sur PROTECTION DES INFRASTRUCTURES ET IMPLÉMENTATION DE TIBER-EU - PDF Téléchargement Gratuit (docplayer.fr), 05 juillet 2021.

JSMITH. Le marché des logiciels de système bancaire devrait connaître une croissance exceptionnelle en 2018-2026. Disponible sur Le marché des logiciels de système bancaire devrait connaître une croissance exceptionnelle en 2018-2026 – Androidfun.fr, 07 avril 2021.

KPMG, Operationel resilience in financial services. Disponible : Operational resilience in financial services (assets.kpmg), Juin 2019.

LOUKIL, RIDHA. Le français OVH est l'un des leaders du cloud privé en Europe, selon le cabinet Forrester. Disponible sur Le français OVH est l'un des leaders du cloud privé en Europe, selon le cabinet Forrester (usinenouvelle.com), 24 juin 2020.

SOURCE

SMITH, Roger. Le marché des logiciels de système bancaire connaîtra une croissance énorme d'ici 2029 |Automated Workflow Pvt. Ltd, TEMENOS Headquarters SA, SecurePaymentz. Disponible sur Le marché des logiciels de système bancaire connaîtra une croissance énorme d'ici 2029 |Automated Workflow Pvt. Ltd, TEMENOS Headquarters SA, SecurePaymentz – AFRIQUE QUI GAGNE, 23 avril 2022.

STAMFORD, Conn. Gartner Forecasts Worldwide Public Cloud End-User Spending to Grow 23% in 2021. Disponible sur Gartner Forecasts Worldwide Public Cloud End-User Spending to Grow 23% in 2021, 21 avril 2021.

Statista Research Department. IT-outsourcing services market revenue in France 2016-2021. Disponible sur IT-outsourcing market revenue in France 2016-2021 | Statista, 11 février 2022.

Trends-Tendances, Callataÿ & Wouters racheté par le français Sopra. Disponible sur Callataÿ & Wouters racheté par le français Sopra - Finance - Trends- Tendances (levif.be), 17/02/12.

VETRIAK, Nicolas et CHAPPOTTEAU, Georges. DORA, la nécessité d'une gouvernance encore plus efficace pour la Résilience Opérationnelle, PAROLES D'EXPERTS, 14 septembre 2021. Disponible DORA, la nécessité d'une gouvernance encore plus efficace pour la Résilience Opérationnelle - Magazine Decideurs (magazine-decideurs.com).

WAVESTONE, Décryptage de DORA - RiskInsight, 2021. Disponible sur https://www.riskinsight-wavestone.com/2021/01/decryptage-de-dora-quest-ce-que-cela-signifie-pour-la-resilience-des-organisations-financieres/.

YORGOS. TIBER-EU & The White Team (1)? Disponible TIBER-EU & The White Team (1) (cymension.eu) , 3 janvier 2021.

GLOSSAIRE

GLOSSAIRE

AES : Les trois AES, à savoir l'Autorité bancaire européenne (ABE) (« European Banking Authority » [EBA]), l'Autorité européenne des assurances et des pensions professionnelles (AEAPP) (« European Insurance and Occupational Pensions Authority [EIOPA] ») et l'Autorité européenne des marchés financiers (AEFM) (« European Securities and Markets Authority [ESMA] ») forment, avec les autorités de surveillance nationales des Etats membres, le pilier microprudentiel de la surveillance des marchés financiers de l'UE.

AMF : L'Autorité des marchés financiers (AMF) est une institution financière et une autorité publique indépendante française créée le 1er août 2003 par la loi de sécurité financière, dotée de la personnalité morale et disposant d'une autonomie financière, qui a pour missions de veiller à la protection de l'épargne investie dans les instruments financiers, à l'information des investisseurs et au bon fonctionnement des marchés d'instruments financiers.

ANSSI : L'Agence nationale de la sécurité des systèmes d'information (ANSSI) est un service français créé par décret en juillet 20091. Ce service à compétence nationale est rattaché au secrétariat général de la Défense et de la Sécurité nationale (SGDSN), autorité chargée d'assister le Premier ministre dans l'exercice de ses responsabilités en matière de défense et de sécurité nationale. L'ANSSI remplace la Direction centrale de la sécurité des systèmes d'information, créée par décret en juillet 2001.

API : Application Programming Interface, que l'on traduit en français par interface de programmation, est une solution informatique qui permet à des applications de communiquer entre elles et de s'échanger mutuellement des services ou des données.

APT / MPA : Une « Advanced Persistent Threat » (Anglais: traduction littérale, menace persistante avancée ; souvent abrégé APT) est un type de piratage informatique furtif et continu, ciblant une entité spécifique.
AWS : Amazon Web Services (AWS) est une division du groupe américain de commerce électronique Amazon, spécialisée dans les services de cloud computing à la demande pour les entreprises et particuliers.
politique monétaire de la zone euro et prend les décisions nécessaires à sa mise en œuvre

GLOSSAIRE

BCE : La Banque centrale européenne (BCE) est la principale institution monétaire de l'Union européenne. Elle est établie le 1er juin 1998 sur un modèle fédéral et son siège est à Francfort-sur-le-Main, en Allemagne. Elle bénéficie d'un monopole d'émission de l'euro en tant que monnaie commune et unique de l'Union économique et monétaire. Elle définit les grandes orientations de politique monétaire de la zone euro et prend les décisions nécessaires à sa mise en œuvre.

BCM : La « Business Continuity Management » est définie comme la planification et la préparation avancées d'une organisation pour maintenir les fonctions commerciales ou reprendre rapidement après une catastrophe. Cela implique également de définir les risques, notamment les incendies, les inondations ou les cyberattaques.

Bluemix : IBM Bluemix est une PaaS (plateforme en tant que service) Cloud lancée par IBM en 2014, avant d'être fusionnée avec IBM Cloud en 2017. Il permet d'utiliser plusieurs langages de programmation et services avec des outils de type DevOps.

BlueTeam : Blue Team est similaire à la Red Team dans le sens où elle identifie les vulnérabilités possibles. La différence se place dans sa stratégie d'amélioration des mécanismes de défense. De plus, contrairement à la Red Team, elle est au courant des défenses déjà en place. Elle est continuellement impliquée dans l'analyse d'activité suspicieuse.

BIA : Il s'agit d'un processus systématique comprenant un volet d'exploration et un volet de planification. Le volet exploratoire comprend l'identification des risques auxquels une entreprise est confrontée si ses activités commerciales sont perturbées. L'accent est mis ici sur les effets concrets que certains événements ont sur l'organisation et sur des domaines tels que la finance, la sécurité, le marketing ou l'assurance qualité. La composante de planification consiste en l'élaboration de stratégies visant à minimiser les risques. Le résultat de l'analyse est le rapport BIA. valeur, et qui dépassent en général les capacités d'une seule et unique machine et nécessitent des traitements parallélisés.

GLOSSAIRE

BFI : Banque de financement et d'investissement est un établissement financier dont la principale activité consiste à distribuer des services et des produits sophistiqués à des clients institutionnels, à des particuliers fortunés et à des grandes entreprises. Ses prestations s'articulent souvent autour des marchés financiers internationaux et nationaux, même si la banque d'investissement et de financement est également capable de fournir des services particuliers à la demande de ses clients. A la différence d'une banque commerciale, une BFI ne récolte pas l'épargne de ses clients et ne distribue pas de crédit, ni aux particuliers, ni aux entreprises.

Big Data : les mégadonnées ou les données massives, désigne les ressources d'informations dont les caractéristiques en termes de volume, de vélocité et de variété imposent l'utilisation de technologies et de méthodes analytiques particulières pour créer de la valeur, et qui dépassent en général les capacités d'une seule et unique machine et nécessitent des traitements parallélisés.
CBEST : CBEST fait partie de la boîte à outils de surveillance de la Banque d'Angleterre et de la « Prudential Regulation Authority » (PRA) pour évaluer la cyber-résilience des services commerciaux importants des entreprises. Cette évaluation hiérarchisée et ciblée nous permet, ainsi qu'aux entreprises, de mieux comprendre les faiblesses et les vulnérabilités et de prendre des mesures correctives, améliorant ainsi la résilience des entreprises d'importance systémique et, par extension, du système financier au sens large.

CERT / CSIRT : Un computer emergency response team (CERT) ou computer security incident response team (CSIRT) est un centre d'alerte et de réaction aux attaques informatiques, destiné aux entreprises ou aux administrations, mais dont les informations sont généralement accessibles à tous. L'appellation CSIRT est privilégiée en Europe, CERT étant une marque déposée aux États-Unis par l'université Carnegie-Mellon.

CIISI : Cyber Information and Intelligence Sharing Initiative est une initiative multilatérale de partage d'informations et de renseignements sur la cybersécurité entre les entités publiques et privée.

GLOSSAIRE

CIISI : Cyber Information and Intelligence Sharing Initiative est une initiative multilatérale de partage d'informations et de renseignements sur la cybersécurité entre les entités publiques et privée.

CMORG : Le « Cross Market Operational Resilience Group (CMORG) » mène une action collective sectorielle sur la résilience opérationnelle. Le groupe est composé d'environ 25 membres, des entreprises du commerce de détail, du commerce de gros, des IMF, des assurances, des autorités financières et du Centre national de cybersécurité. Il est coprésidé par des cadres supérieurs de la Prudential Regulation Authority (PRA) et de UK Finance. Le CMORG a trois objectifs principaux. Il s'agit d'identifier les risques pour la résilience du secteur financier, de développer des solutions pour améliorer la résilience opérationnelle du secteur et de partager le savoir

COBIT : Control Objectives for Information and Related Technology a été conçu par l'ISACA (Information Systems Audit and Control Association) il y a déjà une bonne dizaine d'années.

Il s'agit d'un cadre de référence ainsi que d'un ensemble d'outils jugés indispensables pour assurer la maîtrise et surtout le suivi (audit) de la gouvernance du SI dans la durée. COBIT est fondé sur un ensemble de bonnes pratiques collectées auprès d'experts SI de divers secteurs (industrie et services).

COMITE DE BÂLE : Le Comité de Bâle ou Comité de Bâle sur le contrôle bancaire (en anglais « Basel Committee on Banking Supervision, BCBS ») est un forum où sont traités de manière régulière (quatre fois par an) les sujets relatifs à la supervision bancaire. Il est hébergé par la Banque des règlements internationaux à Bâle.

GLOSSAIRE

CORIE : Cyber Operational Resilience Intelligence-led Exercises est un cadre réglementaire australien pour améliorer la résilience de la cybersécurité dans le système financier australien. L'objectif du programme CORIE est de tester et de renforcer la cyber-résilience des institutions financières contre les acteurs menaçants connus et, ainsi, de protéger les marchés financiers australiens.

CPMI-IOSCO : L'OICV et le Comité des paiements et des infrastructures de marché (CPMI) travaillent ensemble pour améliorer la coordination de l'élaboration et de la mise en œuvre des normes et des politiques concernant les accords de compensation, de règlement et de déclaration, y compris les infrastructures des marchés financiers (IMF) dans le monde entier. Les IMF, qui comprennent les contreparties centrales (CCP), les référentiels centraux (TR), les dépositaires centraux de titres (CSD), les systèmes de règlement de titres (SSS) et les systèmes de paiement (PS), jouent un rôle essentiel dans le système financier mondial.

CROE : Cyber resilience oversight expectations définissent les attentes de l'Eurosystème en matière de cyber-résilience sur la base des orientations mondiales existantes ;

CQUEST : Il s'agit d'un questionnaire d'auto-évaluation du niveau de maturité d'une entreprise en matière de cyber-résilience.

CrowdStrike : CrowdStrike est une entreprise étasunienne de cybersécurité fondée en 2011 et basée à Sunnyvale en Californie. L'entreprise fournit des outils de réponses numériques aux attaques informatiques, sécurise les nuages informatiques et les données de ses clients. L'entreprise a été impliquée dans les enquêtes sur les attaques concernant le studio Sony Pictures Entertainment en 2014, le Comité national démocrate de 2015 et les fuites de courriels concernant ce dernier congrès.

GLOSSAIRE

CTI : La Threat Intelligence, ou Cyber Threat Intelligence (CTI) est une discipline basée sur des techniques du renseignement, qui a pour but la collecte et l'organisation de toutes les informations liées aux menaces du cyber-espace (cyber-attaques), afin de brosser un portrait des attaquants ou de mettre en exergue des tendances (secteurs d'activités touchés, méthode utilisée, etc).

CyCLONe : Cyber Crisis Liaison Organisation Network est un nouveau réseau de coopération pour les États membres. L'objectif de CyCLONe est de contribuer à la mise en œuvre du plan d'action non contraignant de réponse en cas d'incident d'ampleur ou de crise informatique transfrontalière de la Commission européenne. Il vise également à compléter les structures de cybersécurité existantes au niveau de l'UE en reliant la coopération des niveaux technique (principalement le CSIRT Network) et politique (par exemple : Integrated Political Crisis Response - IPCR).

DAST : Le test dynamique de sécurité des applications (DAST) est le processus d'analyse d'une application Web via le front-end pour trouver des vulnérabilités par le biais d'attaques simulées. Ce type d'approche évalue l'application de « l'extérieur vers l'intérieur » en attaquant une application comme le ferait un utilisateur malveillant. Une fois qu'un analyseur DAST a effectué ces attaques, il recherche les résultats qui ne font pas partie de l'ensemble de résultats attendu et identifie les vulnérabilités de sécurité.

D-DOS : Distributed Denial of Service est une attaque qui vise à saturer les ressources d'un serveur informatique en le bombardant de requêtes émanant d'un grand nombre d'adresses IP différentes. Les adversaires qui procèdent à ce genre d'attaques contrôlent généralement un réseau de bots ou ordinateurs zombies, c'est à dire des ordinateurs qui ont été infectés et qui sont contrôlés silencieusement par l'attaquant.

DevSecOps : Mouvement devops incluant la sécurité informatique.

DGSO : Direction générale de la Stabilité financière et des Opérations Direction Générale de la Stabilité financière des Opérations (DGSO) est en charge de 1) la stabilité financière, 2) la mise en œuvre décentralisée en France de la politique monétaire de l'Eurosystème, 3) la gestion des réserves de change de la France et des activités de marché, 4) les opérations pour le compte de la clientèle institutionnelle.

GLOSSAIRE

DSI : Directeur des Services Informatiques est la personne chargée de gérer l'unité informatique au sein d'une entreprise.

DORA : Le projet de règlement de la Commission européenne « DORA » (« Digital Operational Resilience Act ») a pour objectif d'améliorer la résilience opérationnelle informatique des acteurs des services financiers en mettant en place un cadre de gouvernance et de contrôle interne spécifique (ICT risk management framework).

DPO : Data Protection Officer est personne en charge de la sécurité des données dans une entreprise, en particulier des données personnelles que celle-ci peut détenir. Elle est le point de liaison entre l'entreprise et la CNIL pour toutes les questions liées aux données personnelles.

EBA / ABE : L'Autorité bancaire européenne ou ABE (aussi connue sous le nom d'Autorité européenne de surveillance ; en anglais, « European Banking Authority ou EBA ») a été créée par le règlement (UE) no 1093/2010 du 24 novembre 20101 afin de renforcer le Système européen de supervision financière (SESF, en anglais « European System of Financial Supervision, ESFS »). Elle existe officiellement depuis le 1er janvier 2011 et succède au Comité européen des superviseurs bancaires (« Committee of European Banking Supervisors ou CEBS »).

EDR : Il désigne une catégorie d'outils et de solutions qui mettent l'accent sur la détection d'activités suspectes directement sur les hôtes du système d'information. Initialement dénommée « Endpoint Threat Detection & Response » (ETDR), en 2015 Gartner a réduit l'expression en « Endpoint Detection and Response » (EDR).

EIOPA / AEAPP : L'Autorité européenne des assurances et des pensions professionnelles (AEAPP), en anglais « European Insurance and Occupational Pensions Authority (EIOPA) », est la dénomination qui a remplacé le 24 novembre 2010 le CEIOPS.

GLOSSAIRE

EMIR : « L'European Market Infrastructure Regulation (EMIR) » est un règlement de l'Union européenne publié le 4 juillet 2012 afin de réguler les marchés des produits dérivés échangés de gré à gré, les contreparties centrales et les référentiels centraux (UE n°648/2012). Ce texte a pour objectif de réduire les risques liés aux produits dérivés de gré à gré (ou Over The Counter - OTC en anglais) en favorisant la transparence et la standardisation de ce type d'instruments financiers.

ENISA : l'Agence Européenne de cybersécurité, a été créée en 2004 et renforcée par l'adoption du "Cybersecurity Act" européen le 11 juin 2019. L'ENISA contribue à la création d'une culture interétatique en cybersécurité au niveau européen.

ESMA / AEMF : L'Autorité européenne des marchés financiers (AEMF ; en anglais « European Securities and Markets Authority (ESMA) ») est une autorité de surveillance européenne indépendante, installée à Paris.

FEDERAL RESERVE : Réserve fédérale est la banque centrale des États-Unis. Son appellation d'origine est Federal Reserve System, souvent abrégée en Fed. L'établissement, créé le 23 décembre 1913, contrôle la politique monétaire du pays en respectant trois objectifs fixés par le Congrès américain : le plein emploi, la stabilité des prix et le maintien de taux d'intérêt abordables. Au-delà de son rôle originel autour de la politique monétaire, la Réserve fédérale a aussi pour mission de contrôler les systèmes bancaire et financier des États-Unis.

FFIEC : Le Federal Financial Institutions Examination Council (FFIEC) est un organe officiel inter institutions du gouvernement américain composé de cinq régulateurs bancaires qui est habilité à prescrire des principes, des normes et des formulaires de rapport uniformes pour promouvoir l'uniformité dans la surveillance des institutions financières. Il supervise également l'évaluation immobilière aux États-Unis. Ses règlements sont contenus dans le titre 12 du Code of Federal Regulations.

FMI : Le Fonds monétaire international (FMI ; en anglais : International Monetary Fund, IMF) est une institution internationale regroupant 190 pays, dont le but est de « promouvoir la coopération monétaire internationale, garantir la stabilité financière, faciliter les échanges internationaux, contribuer à un niveau élevé d'emploi, à la stabilité économique et faire reculer la pauvreté ».

GLOSSAIRE

FinTech : La technologie financière (aussi dénommée fintech) désigne l'ensemble des nouvelles technologies dont l'objectif est d'améliorer l'accessibilité ou le fonctionnement des activités financières, mais aussi les entreprises dans ce domaine.

FSN : Fournisseurs de service numérique est une personne morale qui fournit tout service de la société de l'information, c'est-à-dire tout service presté normalement contre rémunération, à distance, par voie électronique et à la demande individuelle d'un destinataire de services.

G7 : Le Groupe des sept (G7) est un groupe de discussion et de partenariat économique de sept pays réputés en 1975 pour être les plus grandes puissances avancées du monde qui détiennent environ les 2/3 de la richesse nette mondiale puis 45 % en 2019 : Allemagne, Canada, États-Unis, France, Italie, Japon et Royaume- Uni.

GCP : Google Cloud Platform (GCP) est une plateforme de cloud computing fournie par Google, proposant un hébergement sur la même infrastructure que celle que Google utilise en interne pour des produits tels que son moteur de recherche1. Cloud Platform fournit aux développeurs des produits permettant de construire une gamme de programmes allant de simples sites web à des applications complexes.

IA : Intelligence artificielle (IA) est l'ensemble des théories et des techniques mises en œuvre en vue de réaliser des machines capables de simuler l'intelligence humaine.

IAAS : Infrastructure as a service est une forme de Cloud Computing offrant des ressources informatiques au sein d'un environnement virtualisé (le Cloud) par le biais d'internet ou d'une autre connexion. L'IaaS est l'une des quatre principales catégories de services Cloud Computing, au même titre que le Software as a Service (SaaS), le Desktop as a Service (DaaS), et la Platform as a Service (PaaS).

IAST : L'outil IAST (test de sécurité des applications interactives) analyse le code des vulnérabilités de sécurité pendant que l'application est exécutée par un test automatisé, un testeur humain ou toute activité « interagissant » avec la fonctionnalité de l'application. Cette technologie signale les vulnérabilités en temps réel, ce qui signifie qu'elle n'ajoute pas de temps supplémentaire à votre pipeline CI/CD.

GLOSSAIRE

IIA : Établi en 1941, l'Institute of Internal Auditors (IIA) ou Institut des Auditeurs Internes est un institut voué à l'établissement de standards professionnels d'audit interne. Il regroupe des membres de 165 pays, directement ou via des « chapitres » affiliés. L'IIA veut être la voix de la profession (l'audit interne), son principal représentant et le défenseur de ses intérêts, une autorité reconnue en la matière, jouant un rôle majeur de formation.

ISO : International Organization for Standardization est un organisme de normalisation international composé de représentants d'organisations nationales de normalisation de 167 pays, selon le principe d'un membre par pays. L'ISO est le plus grand organisme de normalisation au monde et demeure une organisation non gouvernementale.

ITIL : Information Technology Infrastructure Library est un ensemble d'ouvrages recensant les bonnes pratiques (« best practices ») du management du système d'information. Rédigée à l'origine par des experts de l'Office public britannique du Commerce (OGC), ITIL a fait intervenir à partir de sa version 3 des experts issus de plusieurs entreprises de services telles qu'Accenture, Ernst & Young, Hewlett-Packard, Deloitte, BearingPoint, CGI ou PriceWaterhouseCoopers.

LPM : Le projet de loi de programmation militaire pour 2014-2019 précise qu'il est de la responsabilité de l'État d'assurer une sécurité suffisante des systèmes critiques des opérateurs d'importance vitale. À travers quatre mesures principales, il vise à établir un socle minimum de sécurité pour les organisations.

MCO / MCS : Maintien en Conditions Opérationnelles / Maintien en Conditions de Sécurité

MIB : C'est l'organe de gouvernance qui a pour mission d'assister le conseil des gouverneurs en veillant à ce que les infrastructures et plates-formes de marché de l'Eurosystème, dans les domaines du règlement en espèces, du règlement des titres et de la gestion des garanties, soient maintenues et développées conformément aux les objectifs du Traité du Système européen de banques centrales (ESCB), les besoins opérationnels du ESCB, les avancées technologiques, ainsi que les exigences réglementaires et de surveillance, le cas échéant ;

GLOSSAIRE

NIS : En juillet 2016, le Parlement européen et le Conseil de l'Union européenne ont adopté la directive sur la sécurité des réseaux et des systèmes d'information connue sous l'appellation « directive NIS ». Cette directive prévoit le renforcement des capacités nationales de cybersécurité ; l'établissement d'un cadre de coopération volontaire entre États ; le renforcement par chaque État de la cybersécurité d'opérateurs dits de services essentiels (OSE) au fonctionnement de l'économie et de la société (élargissement de la notion d'opérateur d'importance vitale OIV) ; l'instauration de règles européennes communes en matière de cybersécurité des prestataires de services numériques dans les domaines de l'informatique en nuage, des moteurs de recherche et places de marché en ligne

NIST : Le NIST CyberSecurity Framework (CSF), est un cadre méthodologique de gestion de la cybersécurité.

OCC : L'Office of the Controller of the Currency (OCC) est une agence fédérale des États-Unis dont la responsabilité est de réglementer, affréter et superviser les banques nationales. Branche du département américain du Trésor, l'OCC a son siège à Washington, DC.

OIV : Un opérateur d'importance vitale (OIV) est, en France, une organisation identifiée par l'État comme ayant des activités indispensables à la survie de la nation ou dangereuses pour la population. Il y en a environ 250 dans 12 secteurs d'activité. Pour des raisons de sécurité nationale, la liste des OIV n'est pas publique et il est demandé aux entreprises désignées de ne pas communiquer sur leur implication au dispositif. Le dispositif est décrit par décret en 20063 avant d'être codifié au Code de la Défense4 en 2007.

OSE : Un opérateur de services essentiels (OSE) est, en France1, un statut caractérisant une entité publique ou privée qui fournit un service essentiel et qui est tributaire de réseaux informatiques ou de systèmes d'informations et dont l'arrêt aurait un impact significatif sur le fonctionnement de l'économie ou la société. la fin des années 2010, dans le cloud computing (informatique en nuage).

GLOSSAIRE

OTC : Lorsque deux parties, un acheteur et un vendeur, souhaitent conclure une transaction, elles peuvent le faire sur deux types de marchés : sur le marché organisé ou Bourse ou sur le marché de gré à gré, aussi appelé over-the-counter (OTC). Sur un marché de gré à gré, la transaction est conclue bilatéralement entre les deux parties, tandis que sur un marché organisé, les contreparties ne négocient pas bilatéralement mais placent des ordres d'achat et de vente, via une société de bourse du type NYSE Euronext ou London Stock Exchange.

OVH : Oles Van Hermann, devenu OVHcloud, est une entreprise française. Elle pratique initialement de l'hébergement de serveur, et est un fournisseur d'accès à Internet (FAI), puis opérateur de télécommunications pour les entreprises. Elle se développe, à la fin des années 2010, dans le cloud computing (informatique en nuage).

PAAS : Plateform as a service est un modèle d'informatique en Cloud dans lequel un fournisseur tiers fournit aux utilisateurs sur Internet des outils matériels et logiciels, généralement ceux nécessaires au développement d'applications. Un fournisseur PaaS héberge le matériel et les logiciels sur sa propre infrastructure. Ainsi, le PaaS libère les développeurs de l'obligation d'installer le matériel et les logiciels en interne pour développer ou exécuter une nouvelle application.

PENTEST : Un test d'intrusion (« penetration test » ou « pentest », en anglais) est une méthode d'évaluation (« audit », en anglais) de la sécurité d'un système d'information ou d'un réseau informatique ; il est réalisé par un testeur (« pentester
», en anglais).

PSSI : Politique de Sécurité des Systèmes d'Information est un document de référence listant un ensemble de règles et de politiques visant à assurer la sécurité d'un système d'informations et reflétant la stratégie de l'entreprise ou de l'organisation.

RACI : (Responsible, Accountable, Consulted et Informed) désigne dans le domaine du management une matrice des responsabilités. Elle indique les rôles et les responsabilités des intervenants au sein de chaque processus et activité.

GLOSSAIRE

REDTEAM : Une Red Team (« équipe rouge ») peut être un groupe externe de pentesters (testeurs d'intrusion) ou une équipe au sein de votre propre organisation. Dans les deux cas, son rôle est le même : émuler un acteur réellement malveillant et tenter de pénétrer dans vos systèmes.

RGPD : Le règlement UE 2016/679 du Parlement européen et du Conseil du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, et abrogeant la directive 95/46/CE dit règlement général sur la protection des données (RGPD, ou encore GDPR, de l'anglais « General Data Protection Regulation »), est un règlement de l'Union européenne qui constitue le texte de référence en matière de protection des données à caractère personnel. Il renforce et unifie la protection des données pour les individus au sein de l'Union européenne.

RPO / PDMA : La perte de données maximale admissible (PDMA ou parfois PDAM), en anglais « recovery point objective (RPO) » quantifie les données qu'un système d'information peut être amené à perdre par suite d'un incident. Usuellement, elle exprime une durée entre l'incident provoquant la perte de données et la date la plus récente des données qui seront utilisées en remplacement des données perdues. Cette durée est exprimée généralement en heures ou minutes.

RSSI : responsable sécurité des systèmes d'information (RSSI) a pour mission première de définir la politique de sécurité du SI (sécurité des systèmes et réseaux, sécurité des applications, stratégie de sauvegarde des données ou bien encore la mise en place d'un plan de continuité d'activité …), et se doit aussi de veiller scrupuleusement à sa mise en œuvre. Le RSSI peut exercer sa fonction en tant que salarié, ou en mission ponctuelle. On parle alors de RSSI de transition ou de RSSI externalisé.
RTO / DMIA : La durée maximale d'interruption admissible (DMIA) est l'expression de besoin de disponibilité des différents métiers ou services, dans une organisation. Elle est aussi appelée le DIMA pour délai d'indisponibilité maximal autorisé ou admissible.

SAAS : Software as a Service (SaaS), ou Logiciel en tant que Service en Français, est un modèle de distribution de logiciel au sein duquel un fournisseur tiers héberge les applications et les rend disponibles pour ses clients par l'intermédiaire d'internet.

GLOSSAIRE

SAST : Un outil « Static Application Security Testing (SAST) » est un outil de sécurité d'application (AppSec) fréquemment utilisé, qui analyse le code source, binaire ou d'octet d'une application. Outil de test en boîte blanche, il identifie la cause première des vulnérabilités et aide à corriger les failles de sécurité sous-jacentes. Les solutions SAST analysent une application de « l'intérieur vers l'extérieur ».

SCA : L'analyse de la composition logicielle (SCA) offre une visibilité sur les composants et les bibliothèques open source incorporés dans le logiciel créé par les équipes de développement. SCA peut aider à gérer les risques liés à la sécurité et aux licences. Cela peut aider à garantir que tout composant open source intégré dans les applications répond à certaines normes, afin d'éviter d'introduire des risques qui pourraient entraîner une violation de données, une atteinte à la propriété intellectuelle ou des litiges juridiques.

SEC : La U.S. Securities and Exchange Commission, communément appelée la Securities and Exchange Commission, souvent abrégée en « la SEC », est l'organisme fédéral américain de réglementation et de contrôle des marchés financiers. C'est en quelque sorte le « gendarme de la Bourse » américain, aux fonctions généralement similaires à celles de l'Autorité des marchés financiers que l'on rencontre dans d'autres États.

Security By Design : Un produit « secure by design » signifie que le risque et la sécurité sont intégrés lors de sa conception et tout au long de son cycle de vie. Son architecture est pensée pour être suffisamment robuste et garantir la sécurité et la confidentialité des systèmes logiciels.
SI : Le système d'information (SI) est un ensemble organisé de ressources qui permet de collecter, stocker, traiter et distribuer de l'information1, en général grâce à un réseau d'ordinateurs

SIEM / SEM / SIM : Appelés également SEM (« security event management », « Gestion des événements de sécurité ») ou SEIM (« security event information management », « Gestion de l'information des événements de sécurité ») ou encore SIEM (« security information and event management », « Gestion de l'information et des événements de sécurité »), ils permettent de gérer et corréler les journaux. On parle de corrélation car ces solutions sont munies de moteurs de corrélation qui permettent de relier plusieurs événements à une même cause racine.

GLOSSAIRE

SIPS : Systemically Important Payment System. Un système de paiement est dit « d'importance systémique » lorsqu'il est susceptible de provoquer des perturbations ou de transmettre des chocs dans le système financier au niveau domestique, voire international.

SOC : Un « Security Operations Center (SOC) », dans une entreprise, est une division qui assure la sécurité de l'organisation et surtout le volet sécurité de l'information.
SWIFTNET : Society for Worldwide Interbank Financial Telecommunication est une coopérative de banques créée en 1973 qui garantit la sécurité des transactions financières. SWIFTNet est le réseau privé mondial de communication bancaire créé par les banques et géré par SWIFT.

TARGET : Le système de transferts express automatisés transeuropéens à règlement brut en temps réel, surtout connu sous l'acronyme Target (« Trans-European Automated Real-time Gross settlement Express Transfer system ») est un système de paiement permettant aux banques de l'Union européenne de transférer des fonds en temps réel dans tout le territoire de l'Union. Le système de règlement des opérations dites de gros montants, Target 1, a été mis en place début 1999 avec l'introduction de l'euro. Target 1 ne fut qu'une étape de transition vers Target 2, véritable plate-forme commune.

TIBER : Le cadre TIBER-EU constitue le premier cadre pour des tests contrôlés et sur mesure contre les cyberattaques. Il vise plusieurs objectifs dont : créer un cadre européen pour le piratage informatique contrôlé afin de tester la résilience des entités sur les marchés financiers, faciliter les tests pour les entités transfrontalières sous la supervision ou le contrôle de plusieurs autorités et aider les institutions financières à mieux comprendre leurs capacités de protection, de détection et de réaction ainsi qu'à lutter contre les cyberattaques.

TIC : Les technologies de l'information et de la communication ou techniques de l'information et de la communication (TIC, transcription de l'anglais information and communication technologies, ICT) sont, principalement dans le monde universitaire, le domaine de la télématique, c'est-à-dire les techniques de l'informatique, de l'audiovisuel, des multimédias, d'Internet et des télécommunications qui permettent aux utilisateurs de communiquer, d'accéder aux sources d'information, de stocker, de manipuler, de produire et de transmettre l'information sous différentes formes.

GLOSSAIRE

TKC : TIBER-EU Knowledge Center gère, centralise et analyse les résultats de tests de résilience opérationnelle pour partager les conclusions aux entreprises du secteur concernées.

TOM : Target Operating Model (TOM) est un modèle d'organisation d'une entreprise alignée sur ses capacités de fonctionnement axé sur les fonctionnalités de cybersécurité ;

UE : L'Union européenne (UE) est une union politico-économique sui generis de vingt-sept États européens qui délèguent ou transmettent par traité l'exercice de certaines compétences à des organes communautaires.

UK : Le Royaume-Uni, (en anglais : United Kingdom), est un pays d'Europe de l'Ouest, ou selon d'autres définitions, du Nord, situé au nord-ouest de l'Europe continentale. Le Royaume-Uni est constitué de quatre pays constitutifs : l'Angleterre, l'Écosse, le pays de Galles et l'Irlande du Nord.

MOT DE L'EQUIPE

SE REUNIR EST UN DEBUT

RESTER ENSEMBLE EST UN PROGRES

TRAVAILLER ENSEMBLE EST LA

REUSSITE

HENRY FORD

BHARATHI KICHENAMOURTY

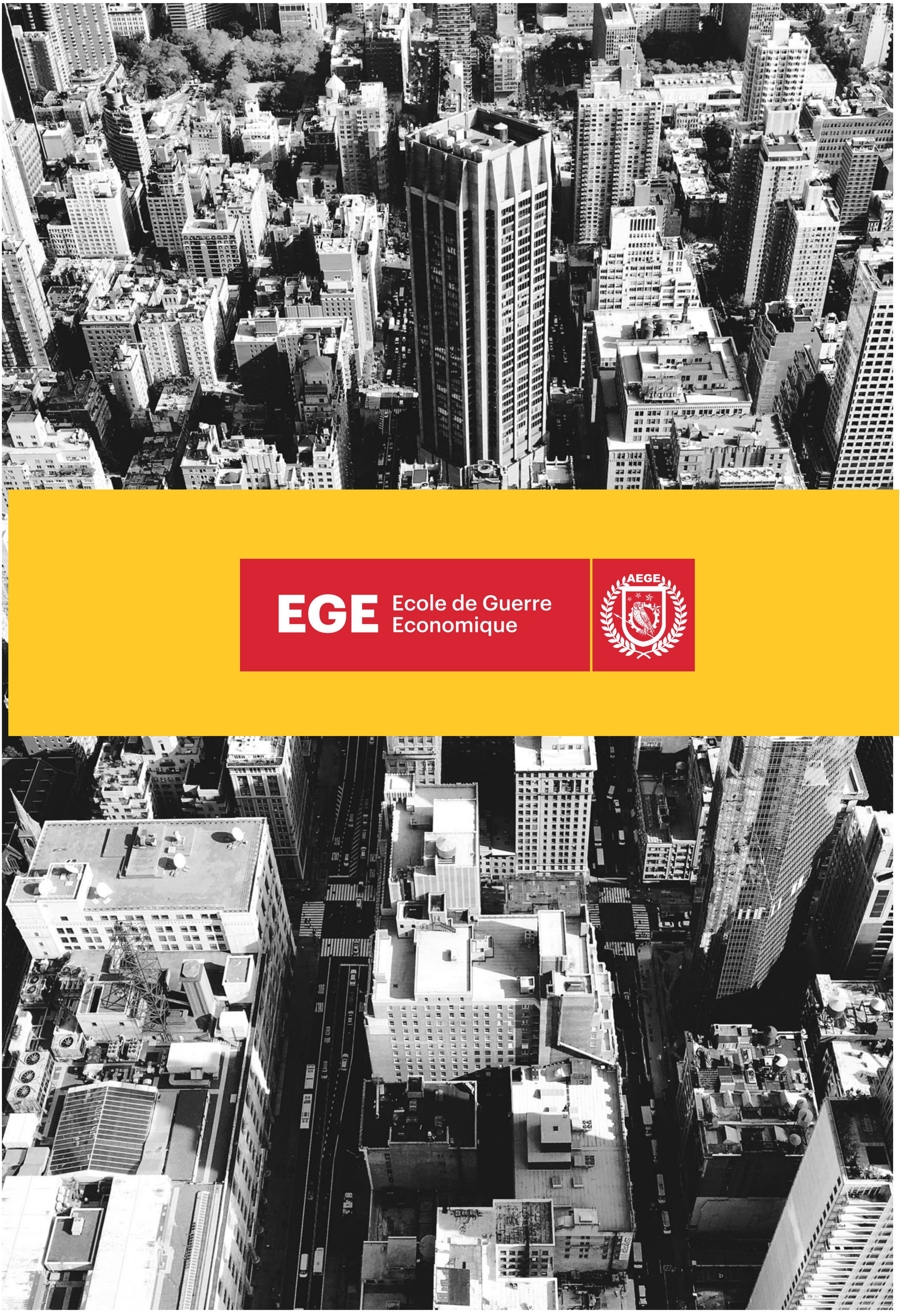
FREDERIC GUILLARD

MOUSSA TIMERA

SEBASTIEN CUVELIER

SAIDA MEDJDOUB

EGE Ecole de Guerre Economique



EGE Ecole de Guerre Economique

AEGE