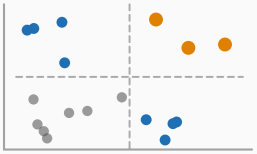
# Risque opérationnel et résilience

## Chapitre 9 : Étude de cas — cybermenaces et sécurité de l'information



Jaouad Madkour

Faculté d'Économie et de Gestion de Tanger · 30 août 2026

# Plan du chapitre

Avant de commencer

Une typologie du risque cyber

Référentiels du risque cyber

Étude de cas : Equifax

Synthèse

# Avant de commencer

# Pourquoi ce chapitre

**Pourquoi ce chapitre ?**

Le panorama des pratiques de cyber-résilience présenté au chapitre précédent se conclut naturellement par une étude de cas approfondie. Ce chapitre élargit d'abord le regard au-delà des seules cyberattaques — vers la notion plus large de sécurité de l'information — avant d'examiner en détail la défaillance la plus emblématique de la décennie 2010 : le piratage d'Equifax en 2017.

# Une typologie du risque cyber

# Au-delà du seul risque cyber

**L'information peut être volée, perdue ou divulguée par erreur**

La sécurité de l'information ne se réduit pas au risque cyber : un rapport d'audit oublié dans un train, une pièce jointe envoyée par erreur au mauvais destinataire, ou un document confidentiel jeté négligemment à la corbeille constituent tout autant des incidents de sécurité de l'information que le piratage d'un serveur. Une étude McAfee de 2017 estime que 43 % des fuites de données sont d'origine interne, la moitié d'entre elles étant non intentionnelles.

# Une matrice à quatre quadrants

## Causes internes/externes, vol/perte

Les risques de sécurité de l'information se répartissent selon deux axes : la cause (interne, y compris prestataires et consultants sur site ; ou externe, y compris les tiers) et la nature de l'incident (vol ou corruption intentionnelle des données ; perte ou divulgation involontaire). Ce croisement produit quatre quadrants — piratage et ingénierie sociale (externe/vol), catastrophes et défaillances de tiers (externe/perte), vol par un employé ou départ mal maîtrisé (interne/vol), et pertes de sauvegardes ou erreurs d'envoi (interne/perte) — chacun appelant des contrôles différents.

## Des cas emblématiques de fuites de données

Les Paradise Papers (2017), deuxième plus grande fuite de données de l'histoire après les Panama Papers, ont exposé 1,4 téraoctet de données confidentielles du cabinet Appleby, révélant des montages d'investissement offshore impliquant des personnalités, entreprises et gouvernements. Aux États-Unis, une fuite suspectée d'un employé de l'IRS a permis à ProPublica de publier les taux d'imposition effectifs de contribuables parmi les plus fortunés. Dans l'écosystème crypto, le vol de clés privées a coûté 55 millions de dollars à la plateforme bZx (2021) et 139,2 millions de dollars à l'échange BXH (2021), ce dernier cas illustrant une possible complicité interne.

# Référentiels du risque cyber

# Trois standards dominants

## NIST, CIS et ISO/IEC 27001

Trois référentiels structurent la protection en cybersécurité : le cadre du National Institute of Standards and Technology (NIST CSF), organisé autour de cinq fonctions — identifier, protéger, détecter, répondre, récupérer — dans une logique proche du cycle de gestion des risques opérationnels (chapitre 2) ; les contrôles critiques de sécurité du Center for Internet Security (CIS), une liste de 18 contrôles priorités régulièrement mise à jour par une coalition d'experts ; et la norme internationale ISO/IEC 27001, qui certifie l'existence d'un système de management de la sécurité de l'information (SMSI) fondé sur le cycle PDCA (chapitre 5).

## Des référentiels complémentaires, non concurrents

Ces trois référentiels ne s'excluent pas : le NIST CSF offre une structure conceptuelle de haut niveau, le CIS des contrôles techniques opérationnels détaillés, et l'ISO 27001 un chemin vers une certification externe reconnue. De nombreuses organisations combinent les trois, en s'appuyant par exemple sur le CIS pour la mise en œuvre technique tout en visant une certification ISO 27001.

**La confidentialité, l'intégrité et la disponibilité — le triptyque CIA**

La protection de l'information repose sur trois dimensions désignées par l'acronyme CIA : confidentialité (Confidentiality), intégrité (Integrity) et disponibilité (Availability) — les deux premières relevant de la sécurité de l'information proprement dite, la troisième de la continuité d'activité et donc de la résilience. Les contrôles se répartissent en deux familles : les contrôles **comportementaux** (campagnes de sensibilisation, tests de phishing simulés, règles de conduite, sanctions) et les contrôles **techniques** (architecture réseau, gestion des accès, pare-feux, chiffrement, détection de fuite de données, honeypots).

# Des indicateurs clés de risque dédiés

## Des KRI spécifiques à la sécurité de l'information

Prolongeant le chapitre 6 sur la communication des risques, la sécurité de l'information se prête à des indicateurs clés de risque spécifiques : retard de correctifs de vulnérabilité, retard des tests d'intrusion, taux de résultats aux tests de phishing simulés, nombre de « récidivistes » ayant échoué à plusieurs tests de phishing dans des zones sensibles, taux de vacance dans les équipes de cybersécurité, ou encore nombre d'appareils ou de cartes d'accès perdus ou volés — autant de signaux avancés d'une dégradation de la posture de sécurité, bien avant toute matérialisation en perte.

# Étude de cas : Equifax

# Le déroulement de l'attaque

## Trois mois d'intrusion non détectée

Le 10 mars 2017, des attaquants ont exploité une vulnérabilité connue du logiciel Apache Struts via le portail de contestation en ligne d'Equifax, l'une des plus grandes agences d'évaluation de crédit au monde. Pendant trois mois, ils sont restés non détectés au sein des systèmes d'Equifax, accédant à plusieurs bases de données et exfiltrant les noms, dates de naissance, numéros de sécurité sociale et informations de cartes bancaires de 147 millions de consommateurs américains. Equifax a perdu près de 5 milliards de dollars de capitalisation boursière dans la semaine suivant l'annonce publique, sur un total de 15,5 milliards.

# Cinq faiblesses structurelles identifiées

## Un cas d'école de défaillances multiples et interconnectées

L'analyse post-mortem d'Equifax a identifié cinq faiblesses majeures, illustrant qu'un événement de risque opérationnel majeur résulte rarement d'une cause unique. Premièrement, l'**absence d'inventaire exhaustif des actifs informatiques** a empêché les équipes de localiser et corriger Apache Struts dans le délai réglementaire de 48 heures suivant une alerte critique. Deuxièmement, l'**échec de mise en œuvre de la politique de gestion des correctifs** : le correctif de la vulnérabilité était disponible dès le 7 mars, trois jours avant l'attaque, et distribué en interne à 400 employés — sans jamais être appliqué. Troisièmement, une **communication interne défaillante** : un employé au fait de l'usage d'Apache Struts n'était pas sur la liste de diffusion de l'alerte, et son manager, qui l'avait reçue, ne l'a pas relayée. Quatrièmement, un **certificat SSL expiré** a empêché la surveillance du trafic chiffré pendant des mois, retardant la détection de l'intrusion jusqu'au 29 juillet — plus de trois mois après le début de l'attaque. Cinquièmement, une **communication de crise externe défaillante** : l'annonce publique n'est intervenue que six semaines après la découverte de la brèche.

## Un précédent ignoré

Dès 2015, un audit interne avait détecté un arriéré de 8 500 vulnérabilités non corrigées, révélant des faiblesses sévères du processus de gestion des correctifs — dont Equifax développait alors sa toute

# Les conséquences et les enseignements

## Un règlement de 700 millions de dollars

En juillet 2019, Equifax a accepté de payer jusqu'à 700 millions de dollars d'amendes et de compensations, dont 300 millions destinés aux consommateurs affectés. L'événement a entraîné la démission du directeur général, du RSSI et du directeur des systèmes d'information, ainsi que des enquêtes de plusieurs autorités fédérales américaines.

## Retour sur les 3R de la communication de crise

Le chapitre 5 avait présenté les « 3R » de la communication de crise destinés à limiter les dommages réputationnels lors d'un événement de risque opérationnel majeur. Le cas Equifax illustre a contrario les conséquences d'un défaut de leur application : une communication tardive et peu transparente a aggravé la perte de confiance déjà provoquée par la fuite elle-même, transformant un incident technique en crise de réputation durable.

# Synthèse

# Ce qu'il faut retenir

**Synthèse du chapitre**

La sécurité de l'information dépasse le seul risque cyber et se répartit selon une matrice à quatre quadrants croisant l'origine (interne/externe) et la nature (vol/perte) de l'incident. Trois référentiels — NIST, CIS, ISO/IEC 27001 — structurent sa gestion, combinant contrôles comportementaux et techniques, suivis par des indicateurs clés de risque dédiés. Le cas Equifax illustre, à travers cinq faiblesses interconnectées — inventaire défaillant, gestion des correctifs non appliquée, communication interne rompue, certificat expiré, communication de crise tardive — comment un événement de risque opérationnel majeur naît rarement d'une cause unique, mais de la conjonction de défaillances qui, prises isolément, auraient chacune pu être maîtrisée.