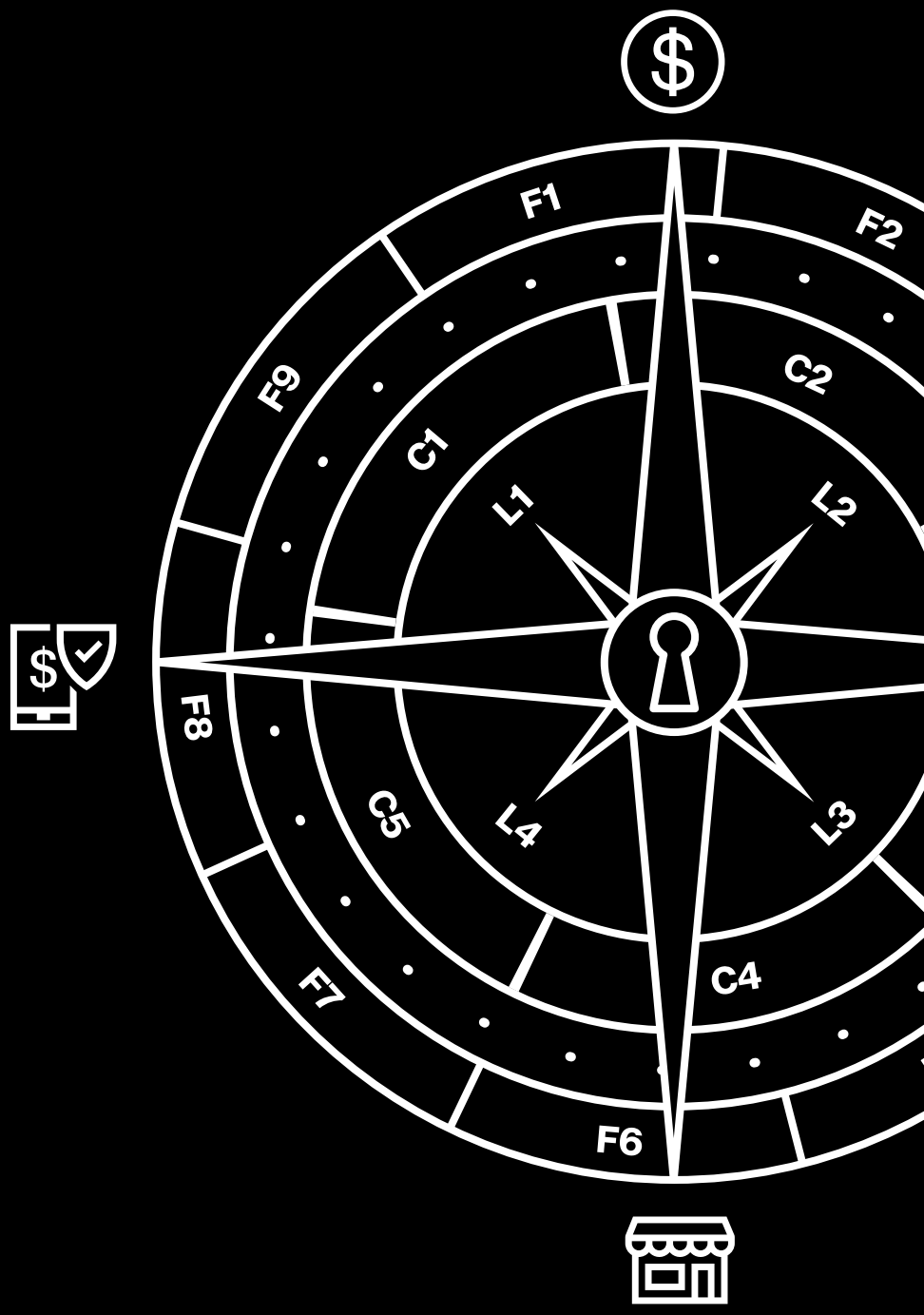
Rapport 2019 sur la sécurité des paiements

Gros plan sur les services financiers



verizon business ready

Les acteurs des services financiers évoluent dans un environnement en pleine mutation. Leurs clients exigent de nouveaux modes d'interactions et de transactions personnalisées – notamment sur smartphones et tablettes – tandis que de nouveaux entrants viennent grignoter des parts de marché.

Dans cet univers ultra-concurrentiel et strictement règlementé, la capacité à protéger les données de carte de paiement peut constituer un facteur de différenciation essentiel. Exigeants, les clients attendent des prestataires de services financiers qu'ils maîtrisent mieux que quiconque les impératifs de sécurité des paiements.

Pour les acteurs de ce marché, le rapport Verizon sur la sécurité des paiements (PSR) s'impose donc comme une lecture incontournable. L'édition 2019 ne déroge pas à la tradition en leur livrant des éclairages inestimables, à commencer par l'importance de nouveaux outils comme notre Cadre 9-5-4 d'évaluation des performances des programmes de conformité.

Un taux de conformité en baisse

Maintenir des contrôles de sécurité efficaces pour protéger les données de carte de paiement et se conformer au standard PCI DSS (Payment Card Industry Data Security Standard), c'est gagner la confiance de ses clients et prendre l'avantage sur ses concurrents. Pourtant, les conclusions du rapport Verizon PSR 2019 sont sans appel : les acteurs des services financiers vont devoir hausser leur niveau de jeu.

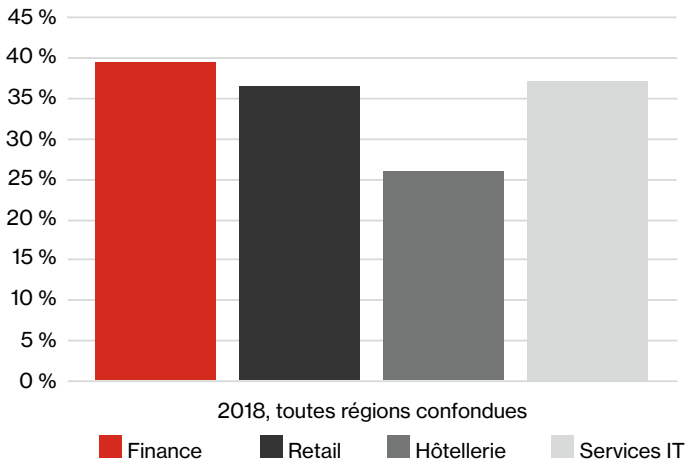


Figure 1 : Taux de conformité mondial par secteur

Si la finance affiche les meilleurs taux de conformité PCI DSS (39 %) parmi tous les secteurs étudiés (retail, hôtellerie et services informatiques), son taux de conformité global connaît une forte baisse depuis deux ans. De 59,1 % en 2017, il est passé à 47,9 % dans le PSR 2018, pour encore chuter à 39 % cette année.

Qu'est-ce que le standard PCI DSS ?

Les principales marques de cartes de paiement ont instauré le standard PCI DSS (Payment Card Industry Data Security Standard) pour aider les entreprises à réduire la fraude dans ce domaine. Si le standard vise à protéger les données de carte de paiement, il repose néanmoins sur des principes de sécurité éprouvés qui s'appliquent à tous les types de données. PCI DSS couvre des thèmes comme les politiques de conservation, le chiffrement, la sécurité physique, l'authentification et le contrôle des accès. Pour en savoir plus, rendez-vous sur pcisecuritystandards.org.

Sécurité des cartes de paiement : un enjeu vital, mais une conformité loin d'être totale

Le déclin de la conformité des services financiers n'est pas un cas isolé. Depuis la première publication du PSR il y a neuf ans, nous avons constaté une hausse annuelle du taux de conformité PCI DSS dans tous les secteurs jusqu'en 2017. Toutefois, depuis deux ans, la tendance s'est inversée dans toutes les industries étudiées. Les données d'autres évaluateurs de sécurité qualifiés (QSA) viennent étayer ce constat.

Bien que le PSR 2019 indique une chute du taux de conformité global, l'écart de conformité PCI DSS, qui mesure l'intervalle exact séparant une entreprise de la pleine conformité, est quant à lui resté stable par rapport à l'année dernière (7,2 %). Lorsque l'on se penche uniquement sur le cas des entreprises ayant échoué à leur audit intermédiaire, l'écart de conformité a heureusement perdu 6,2 points de pourcentage en un an, pour descendre à 10,2 % dans le rapport PSR 2019.

Sur le plan géographique, les entreprises de la région Asie-Pacifique (APAC) s'en sortent mieux que les autres puisque 69,6 % d'entre elles sont 100 % conformes au standard PCI DSS. La zone EMEA (Europe, Moyen-Orient et Afrique) affiche un taux de conformité totale de 48,4 %, tandis que moins d'un quart des entreprises de la zone Amériques (20,4 %) sont 100 % conformes.

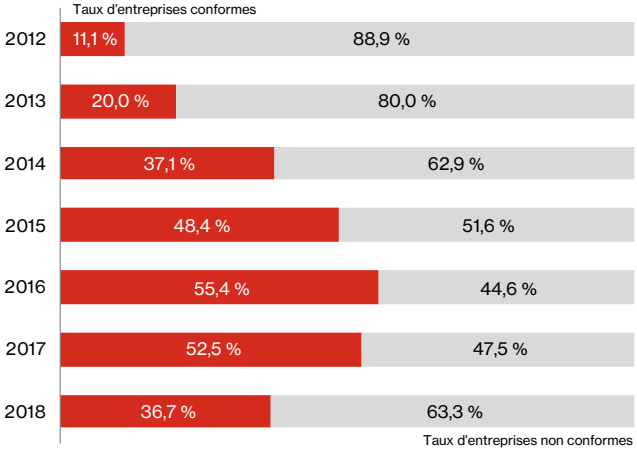


Figure 2 : Taux de conformité totale des entreprises par année

Pourquoi se conformer aux conditions PCI DSS ?

Nous avons établi un recoupement entre les taux de conformité PCI DSS et les statistiques de compromission de données de carte de paiement depuis 2008. Résultat : parmi les entreprises conformes aux 12 conditions du standard PCI DSS, aucune n'a été victime d'une telle compromission.

La bonne nouvelle, c'est que des axes d'amélioration existent. D'après les 55 entreprises interrogées pour le rapport PSR 2018, elles sont 18 %, tous secteurs confondus, à ne pas avoir défini un programme de conformité et de protection des données (DPCP). Aucune ne fait état d'un niveau de maturité optimal de son programme. En clair, les entreprises peuvent mieux faire en termes de développement et de maintenance d'un programme de conformité PCI DSS capable de renforcer la sécurité des paiements.

18 %

des entreprises, tous secteurs confondus, n'ont pas défini de programme de conformité et de protection des données. Aucune ne fait état d'un niveau de maturité optimal de son programme.

Impossible de miser sur les DPCP existants pour assurer la sécurité des cartes de paiement

Bons points

D'après le rapport PSR 2019, le secteur des services financiers s'en sort mieux que tous les autres sur quatre conditions PCI DSS :

- Maintien d'une configuration de pare-feu (condition 1)
- Modification des paramètres de sécurité par défaut des fournisseurs (condition 2)
- Contrôle des accès physiques (condition 9)
- Gestion de la sécurité (condition 12)

En matière de maintenance des pare-feu, la finance a même gagné 2,2 points de pourcentage par rapport à 2018 – une lueur d'espoir dans une année de baisse globale pour tous les secteurs étudiés. En 2019, les établissements de services financiers sont également les plus proches d'une conformité totale à cette condition, avec un écart de 7,3 %.

Enfin, il s'agit du seul secteur à avoir renforcé la sécurité des données de carte stockées (condition 3) par rapport à 2018. Autre signe encourageant, il enregistre la plus grosse diminution d'écart dans ce domaine (de 14,1 % en 2018 à 5,9 % cette année).

Mauvais points

Le transfert de données financières représente le gros de l'activité de certains établissements. Pourtant, il semble que des progrès restent encore à accomplir en matière de chiffrement des données en transit (condition 4). Dans ce domaine, le secteur a enregistré la pire chute du taux de conformité à cette condition (17,1 points de pourcentage).

La finance peine également à se protéger contre les malwares (condition 5), puisqu'elle affiche le taux de conformité globale le plus bas (82,9 %) et l'écart de conformité le plus élevé (8,5 %) de tous les secteurs étudiés.

Enfin, les services financiers se classent en avant-dernière position sur le terrain de la préparation aux incidents de sécurité, les faiblesses les plus récurrentes étant dans les domaines du suivi des accès (condition 10) et de la reconstitution des compromissions de sécurité à partir de pistes d'audit.

Faits intéressants

Dans notre étude PSR 2019, nous avons inclus des corrélations plus détaillées des investigations forensiques PCI (PFI) de l'équipe Verizon Threat Research Advisory Center (VTRAC) | Investigative Response. Sur le long terme, les tendances montrent que 11,5 % des compromissions de données provenaient du secteur financier. C'est convenable, même si les acteurs des services financiers auraient tout intérêt à s'inspirer du taux observé dans les services IT (2,7 % des compromissions).

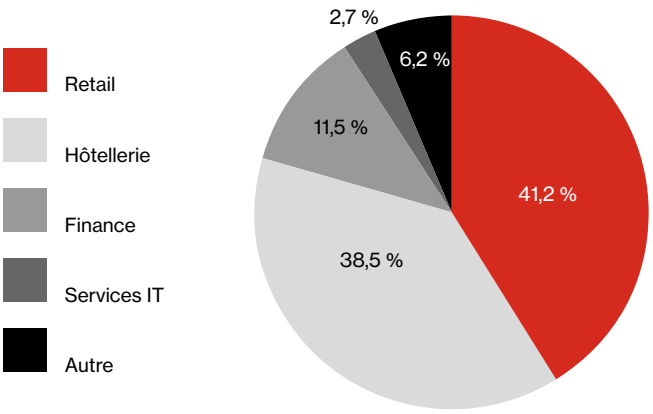


Figure 3 : Compromissions de données par secteur sur six ans, nombre d'investigations Verizon PFI à l'échelle mondiale, 2010-2016

Recommandations

Améliorez votre préparation aux incidents.

Les incidents sont inévitables. Ce qui compte vraiment, c'est la capacité d'une entreprise à y répondre. En clair, vous avez tout intérêt à prendre le temps d'élaborer un plan de réponse à incident (IR) solide. Les pistes d'audit représentent un autre axe d'amélioration essentiel. Sans elles, les experts en conformité et en cybersécurité ne disposent d'aucun élément pour retracer l'incident. Pour en savoir plus sur les avantages et la mise en place de plans IR, consultez le rapport Verizon de préparation et de réponse à incident (VIPR).

Mettez l'accent sur la sécurité mobile.

L'Internet mobile en général, et les applications de banque mobile en particulier, connaissent une véritable explosion. Dans ce contexte, mieux vaut prendre le problème de la sécurité à bras le corps sur les terminaux de vos salariés, y compris les appareils BYOD. D'après le Mobile Security Index 2019 de Verizon (MSI), les terminaux mobiles représentent un problème de sécurité croissant pour les établissements de services financiers. D'après le rapport MSI 2019, le taux de compromission signalé est passé de 25 % en 2018 à 42 % des établissements étudiés en 2019[1]. Les rapports PSR et MSI de 2019 font tous deux le point sur les menaces actuelles et les moyens de conjuguer mobilité et sécurité.

Maturation des programmes de sécurité

La faiblesse de certains programmes de conformité n'a évidemment rien de volontaire. Le problème s'explique d'abord par la difficulté de la tâche. Toutefois, avec les bons outils, tout devient possible.

C'est dans cet esprit que nous avons conçu le Cadre Verizon 9-5-4 d'évaluation des performances des programmes de conformité. Fusion des éditions passées et de nouvelles recommandations, cette nouveauté du PSR 2019 offre une véritable boussole qui permettra aux entreprises d'améliorer leur programme de conformité PCI DSS. Le Cadre Verizon 9-5-4 renforce leur niveau de visibilité et de contrôle, avec à la clé des processus plus homogènes et reproductibles, et des résultats plus prévisibles.

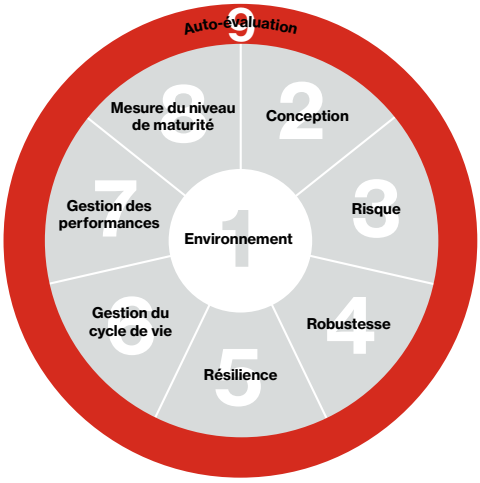


Figure 4 : Modèle relationnel des 9 facteurs d'efficacité et de pérennité des contrôles

La conformité, levier de différenciation

Dans les établissements de services financiers, l'innovation et la conformité réglementaire sont deux axes stratégiques prioritaires. Pour preuve, ils sont aujourd'hui très nombreux à avoir progressé dans le domaine de la détection des fraudes par intelligence artificielle. Il est grand temps que ce genre d'innovation investisse la terrain de la conformité PCI DSS. L'enjeu est d'autant plus important que l'amélioration de la sécurité des paiements et de la conformité PCI DSS a le pouvoir de différencier une entreprise et d'augmenter fortement sa cote de confiance auprès de ses clients.

Plus d'infos

Pour définir vos priorités en matière de sécurité et améliorer votre programme de conformité, rendez-vous sur enterprise.verizon.com/resources/reports/payment-security/ ou contactez votre représentant Verizon.

verizon business ready

1 « Les cybercriminels misent sur l'absence de sécurité des terminaux mobiles. Êtes-vous prêts ? », Verizon Mobile Security Index 2019 – Services financiers https://enterprise.verizon.com/resources/reports/mobile-security-index/