La sécurité de l'information dans l'industrie des services financiers

Nous protégeons ce qui compte.

Shred-it®

C’est aux États-Unis que le coût moyen d’une brèche de données est le plus élevé dans le monde :

$7,35 millions

de dollars, comparativement à 7,01 millions une année auparavant.[1]

Table des matières

Shred-it®

Aperçu et présentation de la sécurité de l'information

De nos jours, la sécurité des données doit être une priorité pour tous les milieux de travail.

Les entreprises ont une probabilité de 25 % de subir une brèche de données[2], un événement qui risque d'être très coûteux et d'entraîner d'énormes coûts financiers, des temps d'arrêt, des atteintes à la réputation et la perte de clients. Les personnes dont on a volé les renseignements personnels et confidentiels sont exposées au vol d'identité et à d'autres crimes. Si le vol physique de données sur support papier ou dans un téléphone cellulaire demeure préoccupant, le vol électronique constitue le crime à la croissance la plus rapide aux États-Unis. Et, comme la technologie évolue à une vitesse effrénée, le paysage de la sécurité des données demeure également une cible mouvante.

La sécurité totale des données peut tout changer. Il faut que tous les lieux de travail soient dotés de politiques et de procédures garantissant la sécurité de tous leurs actifs informationnels, de la création des données jusqu'à leur destruction, en passant par leur manipulation et leur archivage.

Chaque jour dans le monde, près de cinq millions de dossiers de données – soit 58 dossiers par seconde – sont perdus ou volés.[3]

Dans un sondage,

67%

des chefs de la sécurité informatique interrogés ont indiqué qu'il était probable que leur entreprise soit victime d'une cyberattaque ou d'une brèche de données en 2018.[4]

Shred-it®

La sécurité de l'information dans l'industrie des services financiers

En tant que gardiens de confiance de l'information financière confidentielle de leurs clients, les cabinets de services financiers doivent avoir comme priorité de protéger ces données contre le vol et d'autres types d'atteintes à leur sécurité. Même si elle est fortement réglementée, l'industrie est ciblée plus que toute autre, et les brèches de données ont triplé dans le secteur au cours des cinq dernières années[5]. Puisque de plus en plus d'entreprises et de particuliers effectuent en ligne leurs opérations bancaires, leurs paiements de factures et leurs achats, le risque est plus élevé que jamais.

L'argent demeure une grande source de motivation, mais les voleurs d'information sont aussi à la recherche de numéros de compte et d'autres données, puisque ces renseignements les aident à commettre des fraudes de compte bancaire, des vols d'identité, etc. La période n'a donc jamais été aussi propice pour les cabinets de services financiers de mettre en place une gamme complète de mesures de sécurité de l'information.

Le saviez-vous?

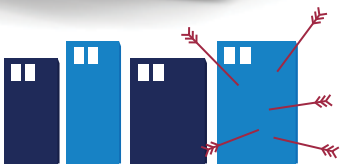
42% des

CABINETS DE SERVICES FINANCIERS ONT DÉJÀ ÉTÉ TOUCHÉS PAR UNE BRÈCHE DE DONNÉES

La proportion des atteintes à la protection des données est passée de 19 % en 2016 à 24 % en 2017.[1]

Les cabinets de services financiers sont victimes de près **DE PRÉS (24%) DE TOUTES LES BRÈCHES DE DONNÉES.**[2]

CYBERATTAQUES dans l'industrie des services financiers **PROVIENNENT DE L'INTÉRIEUR DE L'ENTREPRISE.**[3]



En moyenne, une entreprise de services financiers connaît **65 % PLUS D'ATTAQUES QUE LES ENTREPRISES D'AUTRES INDUSTRIES.**[3]

PRÉS DE 90% des PROFESSIONNELS DES TI FINANCIÈRES sondés en 2017 ont indiqué que leur établissement était **"VULNÉRABLE AUX MENACES ENVERS LES DONNÉES".**[1]

CABINETS DE SERVICES FINANCIERS envisageaient de consacrer davantage de temps et de **RESSOURCES À LA CYBERSÉCURITÉ.**[4]

L'INDUSTRIE DES SERVICES FINANCIERS A CONNU UNE HAUSSE DE 389% DU NOMBRE DE DOSSIERS VOLÉS AU COURS DE LA PREMIÈRE MOITIÉ DE 2017.[5]

Sources:

1. 2017 Thales Data Threat Report, Financial Services Edition.
2. 2017 Data Breach Investigations Report, 10e édition, Verizon.
3. 2017 Cost of Data Breach Study, United States, Ponemon Institute.
4. IBM X-Force Threat Intelligence Index, 2017
5. « 86 Percent of Financial Services Firms to Increase Cyber Security Spend in 2017 », eSecurityplanet.com, avril 2017.
6. IBM Future of Identity Study, 2018.
7. Breach Level Index, Gemalto, 2018.

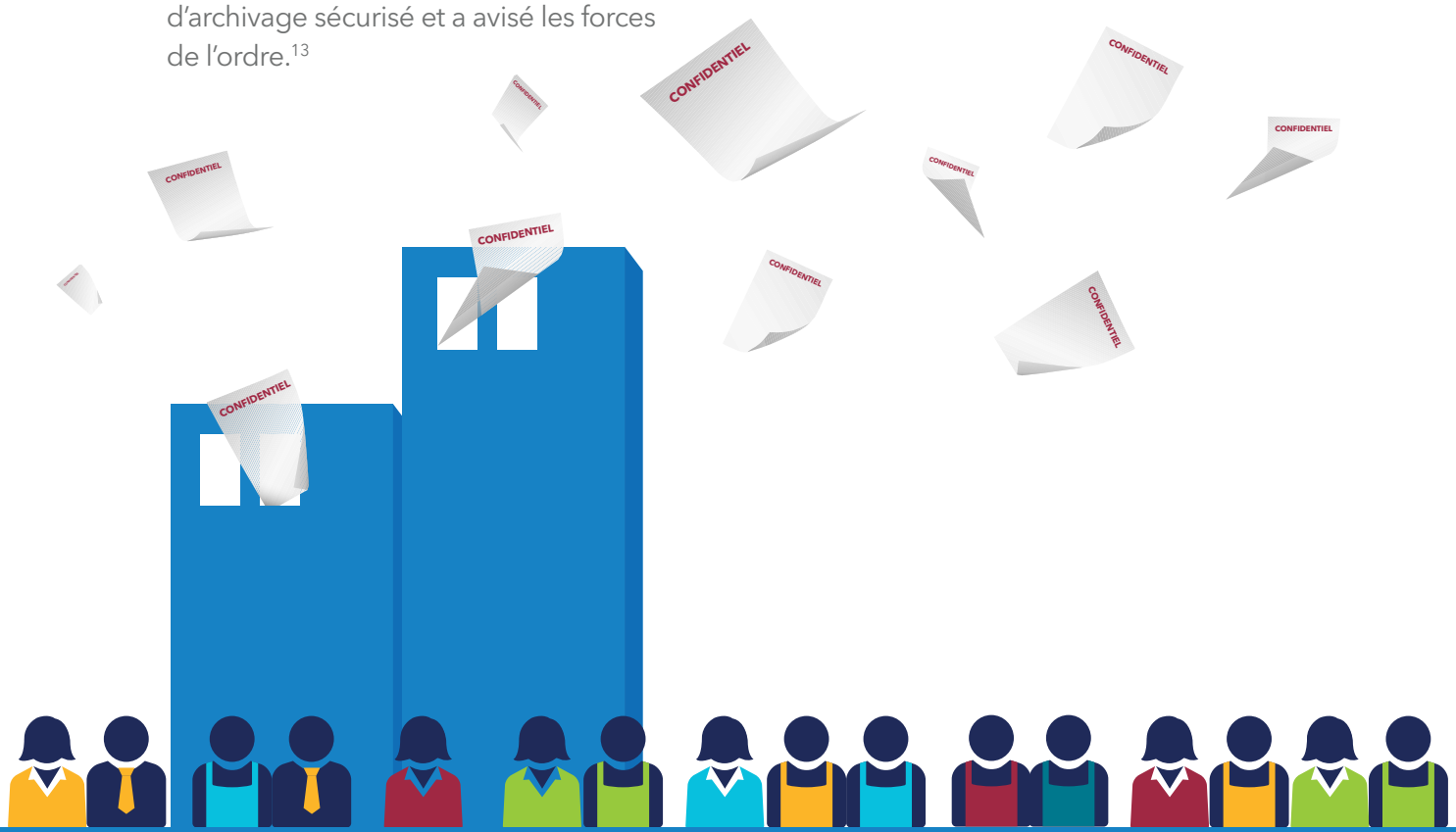
Shred-it®

Exemples de brèches de données dans l'industrie des services financiers

1. En 2017, des cybercriminels ont piraté l'un des plus importants bureaux de crédit des États-Unis et ont volé l'information confidentielle de 147,9 millions de personnes. Cette attaque est considérée comme l'une des pires atteintes de tous les temps en raison de la somme de renseignements confidentiels en cause, notamment des numéros de sécurité sociale, des dates de naissance, des adresses et des numéros de permis de conduire. L'entreprise a révélé le piratage deux mois après qu'il se soit produit; elle a indiqué que la brèche était attribuable à la vulnérabilité d'une application sur l'un de ses sites Web. [11]

2. En 2017, un homme capté par une caméra de surveillance aurait été en train de voler 17 000 $ au guichet automatique d'une coopérative de crédit. Fait intéressant, selon la police de Gainesville, en Floride, le suspect aurait utilisé les données d'identification de plus de 40 personnes dont les informations avaient été dérobées au cours d'une brèche qui avait eu lieu un peu plus tôt dans un restaurant. Les données avaient servi à cloner des cartes de crédit, qui ont ensuite été utilisées avec leur NIP pour retirer de l'argent au guichet. La police croit que le suspect avait acheté les informations d'identification sur le Web invisible.[12]

3. Une entreprise de services financiers qui se spécialise dans le transfert de fonds partout dans le monde a connu une brèche de données en 2018. La société, dont le siège social est situé au Colorado, a déclaré que des cybercriminels avaient accédé sans autorisation à des dossiers numériques de clients à partir d'une entreprise externe d'archivage de données. Lorsque l'atteinte a été découverte, la société a déplacé ses dossiers dans un autre système d'archivage sécurisé et a avisé les forces de l'ordre.[13]



Quels documents doit-on déchiqueter?

Dans l'industrie des services financiers, de nombreux documents doivent être déchiquetés en toute sécurité lorsqu'ils ne sont plus nécessaires.

Renseignements de clients

- Numéros de compte
- Renseignements permettant d'identifier une personne
- Demandes de prêt et documents connexes
- Données bancaires

Comptabilité et technologie de l'information

- Listes de clients
- Information sur les fournisseurs
- Rapports internes
- Feuilles de paie

Ressources humaines

- Demandes d'emploi
- Curriculum vitæ
- Documents de santé et sécurité
- Dossiers médicaux
- Information de paie
- Évaluations de rendement
- Information et guides de formation

Haute direction

- Budgets et autres données financières
- Correspondance
- Contrats
- Rapports stratégiques
- États financiers

Shred-it®

Qu'est-ce qui expose une entreprise de services financiers à un risque de brèche de données?

Attaques par refus de service :

Ce type d'attaques, qui englobe les attaques par refus de service distribué et par réseau de zombies, constitue le type d'incidents le plus fréquent dans l'industrie des services financiers.[7] Il s'agit d'inonder un réseau ou un appareil de trafic ou d'informations pour provoquer un crash, empêchant ainsi l'accès aux services.

Escroquerie par hameçonnage :

La compromission du courriel d'affaires constitue l'une des escroqueries les plus fréquentes. Elle vise à soutirer de l'argent et des données financières confidentielles aux victimes. Un criminel accède à un compte courriel d'affaires et usurpe l'identité du propriétaire pour frauder l'entreprise.

Partenaires tiers :

Bon nombre d'entreprises de services financiers dépendent de différents fournisseurs, partenaires ou tiers pour mener leurs activités. Toutefois, dans un sondage, 60 % des chefs de la sécurité informatique interrogés ont indiqué qu'ils redoutaient une brèche de données provenant d'un tiers compromis.[4]

Cybercriminels :

Les cybercriminels (40 %) sont considérés comme la principale menace externe pour le secteur des services financiers. Ils sont suivis des États (18 %), des cyberactivistes (16 %) et des entreprises concurrentes (13 %).[6]

Numérisation :

Les relations des banques et des autres fournisseurs de services financiers avec leurs clients se passent de plus en plus en ligne, par téléphone mobile ou par l'Internet des objets, mais les différents appareils branchés à un réseau ne sont pas toujours sécurisés.

Menaces internes :

Dans un récent rapport, 60 % des services financiers interrogés dans le monde ont pointé les utilisateurs privilégiés comme la plus importante menace interne, suivis des cadres (48 %) et des entrepreneurs (38 %) (6). Le transfert de fonds frauduleux ou l'utilisation d'informations personnelles de clients à des fins de vol d'identité constituent des exemples de mauvais usage de privilèges.

Équipement vétuste :

Les cabinets de services financiers intègrent constamment de nouveaux systèmes, logiciels et technologies dans leurs activités et ils héritent des vieux systèmes de TI des entreprises qu'ils acquièrent. L'accumulation de ceux-ci rend l'entité vulnérable aux attaques.

Négligence des employés :

Des recherches ont montré que la négligence des employés qui ne suivent pas les politiques et les procédures de façon appropriée constitue la plus grande menace pour une entreprise en matière de sécurité (16). Les erreurs d'imprudence, comme communiquer un mot de passe à voix haute, transporter avec soi de l'information confidentielle sans raison et laisser ses appareils mobiles sans surveillance à l'extérieur du travail, risquent d'entraîner une brèche de données.

Maliciels financiers :

Les maliciels financiers constituent une menace énorme. En effet, 1,2 million de détections sont signalées chaque année, et ils sont 2,5 fois plus fréquents que les rançongiciels (14). Dans une étude menée au cours des dernières années, on avait découvert que 75 % des principales banques commerciales américaines étaient infectées par des logiciels malveillants.[15]

Lois sur la protection des renseignements personnels

Le secteur financier est fortement réglementé et assujetti à différentes lois sur la protection des renseignements personnels fédérales, provinciales et des États.

Voici quelques lois, normes et règlements applicables :

La Gramm-Leach-Bliley Act (GLB Act)

exige des institutions financières qu'elles expliquent à leurs clients leurs pratiques en matière de communication de renseignements et qu'elles protègent les données confidentielles.[17]

La Fair Credit Reporting Act (FCRA)

protège la confidentialité des renseignements contenus dans les dossiers des agences de renseignements sur le consommateur.[19]

La Can-Spam Act

fixe les règles concernant les courriels commerciaux, notamment en exigeant qu'il y soit clairement indiqué que les courriels proviennent de l'institution financière.[25]

La Fair and Accurate Credit Transactions Act (FACTA)

contribue à réduire les risques de vol d'identité en réglementant le traitement des renseignements sur les comptes de clients.[23]

La Norme de sécurité des données de l'industrie des cartes de paiement (PCI DSS)

enjoint aux entreprises de protéger les données des titulaires de cartes.[21]

La Sarbanes-Oxley Act (SOX)

protège les investisseurs contre les activités comptables frauduleuses des sociétés; elle prévoit également des exigences en matière de divulgation d'information financière.[20]

La Red Flag Rule

exige la création d'un programme de prévention du vol d'identité visant à détecter des indices de vol d'identité dans les opérations courantes[18]

Le Règlement général sur la protection des données (RGPD)

protège les données personnelles et la vie privée des citoyens de l'Union européenne (UE). Il s'applique à toutes les entreprises, peu importe où elles se trouvent dans le monde, qui traitent des renseignements sur des citoyens de l'UE. [22]

La Disposal Rule

qui fait partie de la FACTA, exige l'élimination adéquate des informations contenues dans les rapports et les dossiers des consommateurs. Les documents papier doivent être déchiquetés sur-le-champ et en toute sécurité, et les dossiers numériques doivent être détruits.[24]

La Loi sur la protection des renseignements personnels et les documents électroniques (LPRPDE)

régit la façon dont les entreprises privées du Canada recueillent, utilisent ou communiquent les renseignements personnels. Les renseignements doivent être protégés par des mesures de sécurité appropriées[26]

Le nombre de cyberattaques contre des cabinets de services financiers ayant été signalées a grimpé de 80% au cours de la dernière année.[27]

Shred-it®

Conseils et pratiques exemplaires en matière de sécurité de l'information

Plan de sécurité des données :

Toutes les entreprises de services financiers doivent se doter d'un programme de sécurité exhaustif qui couvre les gens, les politiques et les procédures. Il est crucial de mettre en œuvre des mesures de protection technologiques, comme les filtres antipourriel, les pare-feu, le cryptage de tous les disques durs, les logiciels de détection des attaques par refus de service distribué et les technologies de prévention des pertes de données.

Conformité et protection des données :

Le secteur des services financier est fortement réglementé. Les contraventions risquent d'être coûteuses et de pulvériser la crédibilité d'une entreprise. Les vérifications périodiques permettent de veiller au respect de tous les règlements. La conformité est le principal motif des dépenses en matière de sécurité, ayant été citée par 49 % de répondants américains du secteur des services financiers.[6]

Essais de pénétration :

Effectuez des essais de pénétration et de vulnérabilité des systèmes pour déceler et régler les problèmes de sécurité.

Culture de sécurité :

Instaurez une culture de sensibilisation à l'égard de la sécurité à l'échelle de votre entreprise. Tous les employés, des cadres au personnel en relation directe avec le public, doivent contribuer à garantir la sécurité de l'information.

Mise à jour des logiciels et du matériel :

Vérifiez périodiquement si des correctifs et autres mises à jour sont offerts pour les logiciels de sécurité de vos ordinateurs et vos systèmes d'exploitation. Soyez technologiquement à jour et détruisez en toute sécurité vos anciens équipements.

Formation continue des employés :

Informez tous les employés sur les brèches de données et la façon de les éviter. La formation devrait inclure le repérage des menaces dangereuses comme les escroqueries par hameçonnage. Mettez l'accent sur la conservation des clients et les activités visant à préserver la réputation et la valeur de la marque. La formation doit être continue, puisque le secteur connaît un taux de roulement du personnel de 7,1 %; c'est le plus élevé de tous les secteurs de l'industrie.[1]

Politique en matière de mots de passe :

Mettez en place une politique qui exige des mots de passe sûrs pour chaque appareil, réseau, service et site Web. Dans un récent sondage, les trois quarts des clients de services financiers ont indiqué qu'ils utilisaient plus d'un mot de passe et près de neuf sur dix étaient favorables à l'implantation de mesures de sécurité biométriques dans l'avenir.[10]

Partenaires tiers :

Choisissez des partenaires tiers qui possèdent de l'expérience en matière de sécurité, pour qui cet enjeu est important, et qui se conforment à la réglementation.

Plan d'intervention :

Soyez préparé à toute atteinte à la sécurité des données et ayez un plan d'intervention et de récupération en place. Tous doivent savoir ce qu'il faut faire en cas de brèche de données.

Destruction des documents :

Faites affaire avec une entreprise de destruction de documents qui a mis en place une chaîne de garde sécurisée et qui s'occupe de détruire le papier, les disques durs et les supports électroniques. Un certificat doit vous être remis après la destruction de ces articles.

Shred-it®

Comment Shred-it® peut-elle vous aider

Lieu de travail protégé par Shred-it

Notre suite intégrée de produits et de services comprend le déchiquetage de documents papier, la destruction de disques durs et des politiques sur la sécurité des lieux de travail. Tous nos produits et services sont conçus pour protéger ce qui compte le plus, chaque jour. Par ailleurs, nos services sont effectués dans le respect le plus strict d'une chaîne de garde sécurisée.

Destruction sécurisée de documents et de disques durs

- Des processus de chaîne de garde sécurisée du début à la fin
- Un certificat de destruction remis après chaque service
- Des solutions adaptées aux besoins de votre entreprise

Conseils et expertise

- Des spécialistes formés en sécurité de l'information
- Une évaluation de la sécurité des données faite sur votre lieu de travail pour repérer les risques en matière de sécurité de l'information

Apprenez-en davantage sur la sécurité de l'information dans l'industrie des services financiers à shredit.com/finance ou au 1 888 979-4048

Sources:

1. 2017 Cost of Data Breach Study, United States, Ponemon Institute.
2. 2017 Cost of Data Breach Study, Global Overview, Ponemon Institute.
3. Breach Level Index, Gemalto, 2018.
4. What CISOs Worry About in 2018 Survey, Ponemon Institute et Opus, 2017.
5. 2017 Cost of Cyber Crime, Financial Services, Ponemon Institute et Accenture.
6. 2017 Thales Data Threat Report, Financial Services Edition.
7. 2017 Data Breach Investigations Report, 10e édition, Verizon.
8. IBM X-Force Threat Intelligence Index, 2017.
9. « 86 Percent of Financial Services Firms to Increase Cyber Security Spend in 2017 », eSecurityplanet.com, avril 2017.
10. IBM Future of Identity Study, 2018.
11. « The 17 Biggest Data Breaches of the 21st Century », CSOonline.com, janvier 2018.
12. « Chipotle Data Breach Leads to Illegal ATM Withdrawal », Scmagazine.com, July 2017.
13. « Western Union Customer Data Stolen », wccftech.com, février 2018.
14. Internet Security Threat Report, Financial Threats Review 2017, Symantec.
15. 2016 Financial Industry Cybersecurity, Security ScoreCard.
16. Promoting Data Security in the Workplace infographic, University of Alabama at Birmingham; 2016 State of the Endpoint Report, Ponemon
17. GLBA : Gramm-Leach-Bliley Act, Federal Trade Commission.
18. Red Flags Rule, Federal Trade Commission.
19. Fair Credit Reporting Act, Federal Trade Commission.
20. SOX: Sarbanes-Oxley Act, Soxlaw.com.
21. Norme de sécurité de l'industrie des cartes de paiement, Conseil des normes de sécurité PCI.
22. Règlement général sur la protection des données (RGPD), Eugdpr.org.
23. Fair and Accurate Credit Transactions Act, Federal Trade Commission.
24. Disposal Rule, Federal Trade Commission.
25. Can-Spam Act, Federal Trade Commission.
26. Loi sur la protection des renseignements personnels et les documents électroniques, Commissariat à la protection de la vie privée du Canada.
27. « Rise in Cyber Attacks Against Financial Services Firm », Information Age, janvier 2018.

Nous protégeons ce qui compte.

Shred-it®