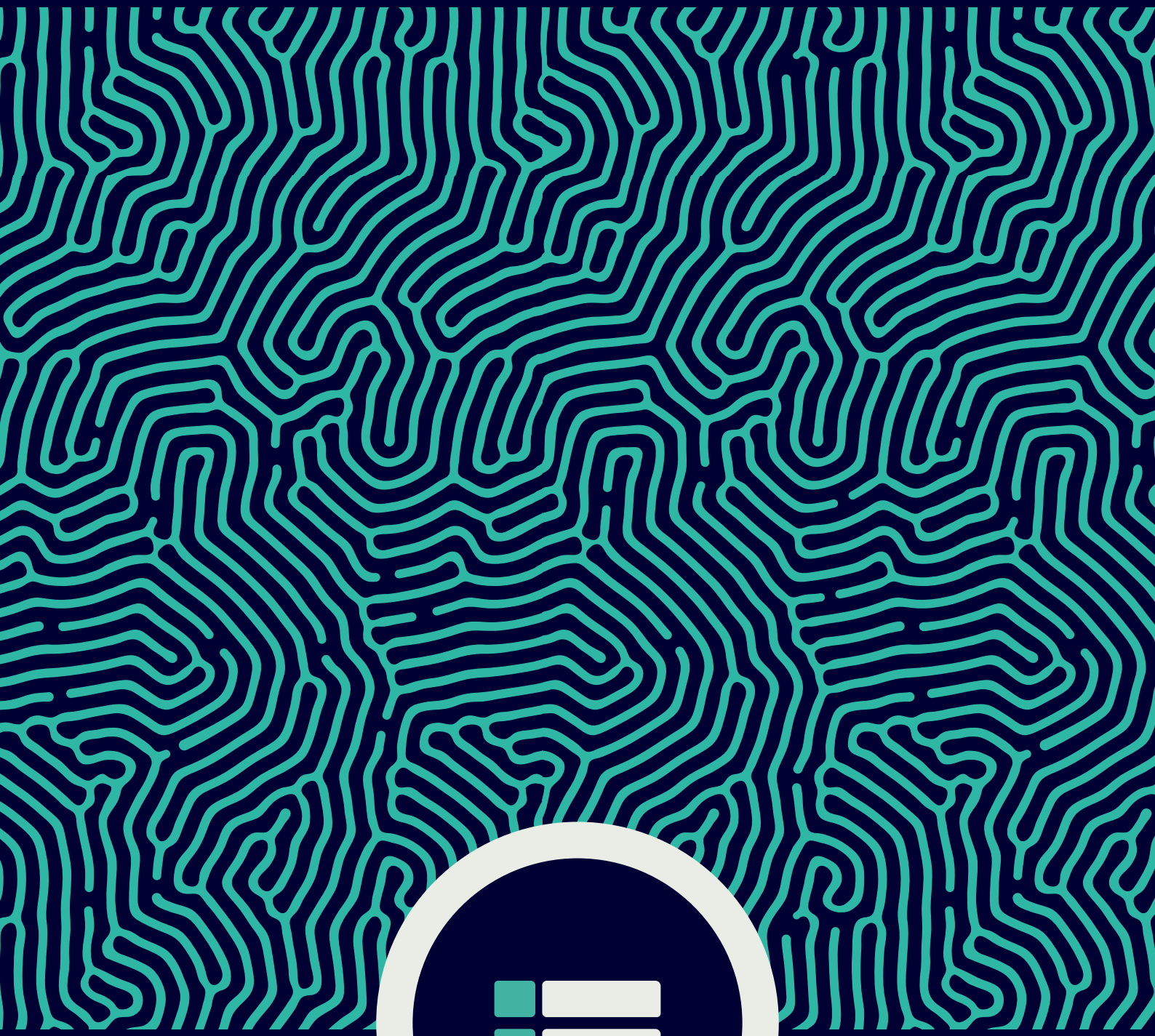
ENQUÊTE SUR INTERNET DANS LE MONDE 2016



Synthèse

Introduction

Le piratage des données est de plus en plus fréquent. Son impact sur les utilisateurs, les consommateurs, les employés et les organisations, est profond et durable, avec des coûts financiers et autres importants. Pire encore, dans de nombreux cas le piratage des données aurait pu être évité. Et lorsqu'il n'aurait pas pu être évité, les dégâts causés auraient pu être limités.

Le problème au cœur de cette enquête est donc simple, sous certains aspects :

Pourquoi les organisations ne prennent-elles pas toutes les mesures disponibles pour protéger ceux qui leur confient leurs renseignements personnels ? Est-ce parce qu'elles ne supportent pas l'ensemble du coût du piratage de données ? Est-ce parce qu'elles ne voient pas suffisamment d'intérêts à mieux protéger les données de leurs utilisateurs ? La réponse aux deux questions est oui.

Lorsque les utilisateurs supportent les coûts durables de chaque piratage, la confiance en Internet en est l'ultime victime. Internet Society a pour objectif de rendre l'Internet accessible à tous et partout. La confiance en Internet est au cœur de cette vision. Sans celle-ci, les utilisateurs en ligne sont moins enclins à fournir leurs renseignements personnels sur Internet, et ceux qui ne sont pas encore en ligne auront une raison de le rester. L'économie en ligne ne progressera pas aussi vite qu'elle le pourrait, et les objectifs de développement durable établis par l'ONU seront d'autant plus difficiles à atteindre.[1]

Avec cette enquête, Internet Society cherche à augmenter la prise de conscience sur le sujet des failles de sécurité et notre responsabilité collective dans la préservation de l'écosystème des données. Nous effectuons des recommandations pour réduire le nombre et l'impact des piratages de données. De manière fondamentale, les utilisateurs doivent être au centre des discussions, car ce sont les ultimes victimes des piratages. Il faut gagner et conserver leur confiance pour aider Internet à respecter complètement ses promesses pour tous.

Qu'est-ce qu'un piratage de données ?

« Une faille de sécurité entraînant une destruction accidentelle ou illégale, une perte, une modification, une publication illégale ou un accès à des données personnelles transmises, conservées ou autrement traitées dans le cadre de la fourniture d'un service par communications électroniques publiques »

Le Bureau du commissaire à l'information du Royaume-Uni[2]

[1] Comme cela a été signalé, les données, comme le pétrole, ont leur mauvais côté, et dans cette analogie, les piratages de données sont les nouvelles marées noires. Lire l'article suivant rédigé par Robin Wilton, assistant technique en matière d'identité et de confidentialité pour Internet Society, à l'adresse : https://www.internetsociety.org/blog/tech-matters/2014/10/they-say-« personal-data-new-oil »-thats-good-thing.
[2] Lire https://ico.org.uk/for-organisations/guide-to-pecr/communications-networks-and-services/security-breaches/.

Données et tendances

Les piratages de données sont une tendance à la hausse :

- Ceux-ci affectent un nombre croissant de personnes. Les signalements de piratage sont en augmentation, avec un nombre croissant de données piratées connues et un nombre encore plus grand de piratages inconnus. La cause principale est l'attaque extérieure, principalement à des fins de gain financier. La plupart des piratages semblent se produire aux États-Unis, mais la raison probable est la politique de notification des piratages de données qui entraîne plus de signalements.

- Les enquêtes n'indiquent pas encore que les piratages de données signalés ont une influence importante sur la disposition d'utilisateurs potentiels à se connecter à Internet. Cependant, à mesure que de plus en plus d'utilisateurs seront affectés par des piratages de données et auront leur identité volée à des fins de profit, ceux-ci hésiteront de plus en plus à utiliser les services en ligne exigeant de fournir des renseignements personnels. Ils pourront aussi cesser d'utiliser les services d'une entreprise ayant été piratée. Une augmentation de la méfiance parmi les utilisateurs pourra aussi fournir aux non-utilisateurs une raison de ne pas se connecter à Internet.

- Les organisations dépensent plus dans la prévention, mais cela n'a pas encore diminué de manière remarquable le nombre de piratages, ni l'impact ni le coût de ceux-ci lorsqu'ils se produisent. D'un autre côté, le coût des piratages, lorsqu'il est calculé, n'inclut généralement que le coût pour l'entreprise, et non le coût total pour les utilisateurs qui ont été les ultimes victimes de ceux-ci.

On ne peut pas laisser ces tendances perdurer sans que cela n'affecte de manière importante la confidentialité des utilisateurs et leur confiance en Internet, entraînant un usage moindre et plus restreint d'Internet.

Études de cas

L'enquête souligne certaines causes principales de piratage de données, et leur impact sur les organisations et les utilisateurs. Les chiffres sont saisissants : Target s'est fait voler les numéros de carte de crédit de 40 millions de clients, qui ont été mis en vente sur Internet. Les fichiers d'Ashley Madison sur 37 millions de personnes mariées et leurs liaisons romantiques personnelles ont été prises et publiées en ligne. Le Bureau américain de la gestion du personnel s'est fait voler les données de 21,5 millions d'anciens employés, d'employés actuels et à venir.

L'impact de ces piratages sur les consommateurs, les utilisateurs, les employés et les tiers qui ne savaient même pas que les organisations conservaient leurs données est profond et durable. Certains utilisateurs ont perdu du temps et de l'argent à protéger leurs finances et leur

identité contre les voleurs, certains ont vu leur mariage se briser, et ont même été jusqu'au suicide, et d'autres peuvent être victimes de chantage et d'exposition publique.

Les cas étudiés montrent la facilité d'exécution de certaines attaques, mais aussi la difficulté pour les organisations de se protéger contre toutes les menaces. Pour les utilisateurs, les études de cas soulignent l'augmentation du sentiment d'insécurité en ligne, exigeant la confiance des utilisateurs en des organisations dont ils ne peuvent pas vérifier la sécurité. Un nombre toujours croissant d'utilisateurs a été directement ou indirectement affecté par un piratage de données. Les cas étudiés rendent concret l'impact réel et ultime de ces piratages sur les utilisateurs dont la confiance envers les organisations, en tant que clients ou employés, est trahie.

Questions

Face aux coûts financiers et autres soulignés par les données et les études de cas, il est surprenant qu'un grand nombre de ces piratages exploitent des **vulnérabilités connues** et évitables. Pour certaines d'entre elles, des correctifs étaient disponibles mais n'ont pas été appliqués. Certains piratages utilisent des attaques d'ingénierie sociale, qui trompent les employés pour qu'ils donnent leur mot de passe ou téléchargent un virus, généralement par des techniques évitables.

Bien sûr, tous les piratages ne proviennent pas d'attaques, et toutes les attaques ne sont pas évitables. Certaines exploitent des failles « zero-day » qui ne sont pas connues avant d'avoir été exploitées. D'autres proviennent de publication accidentelle de données, comme par exemple à travers la perte d'un appareil contenant des données sensibles. Même s'ils ne sont pas évitables, ces piratages sont au moins prévisibles compte-tenu de leur fréquence. Il est possible d'en limiter l'impact en minimisant la quantité de données collectées et en chiffrant celles qui sont enregistrées et échangées.

La question subsiste : pourquoi, compte-tenu du coût des piratages, les organisations ne font-elles rien de plus pour empêcher les attaques évitables et pour minimiser le coût et l'impact des attaques prévisibles ? Cela soulève le problème de l'économie de la confiance.

C'est une **défaillance du marché** qui régit les investissements dans la sécurité informatique. D'abord, les piratages de données ont des conséquences **externes**, des coûts qui ne sont pas comptabilisés par les organisations. Ensuite, même lorsque des investissements sont réalisés, en raison **d'informations asymétriques**, il est difficile pour les organisations de transmettre le niveau de sécurité informatique résultant au reste de l'écosystème. C'est pourquoi l'envie d'investir dans la sécurité informatique est limitée. Les organisations ne supportent pas tous les coûts liés au manque d'investissement, et ne peuvent pas en tirer tous les avantages lorsqu'elles investissent.

L'entreprise piratée ne supporte pas tous les coûts de l'attaque – le coût subi par d'autres est une conséquence externe qui n'entre pas forcément en compte dans la prise de décisions sur la manière de se protéger contre les piratages de données. De plus, le poids des piratages de données affecte la confiance des utilisateurs, ce qui est une conséquence externe, et d'un point de vue économique, les organisations n'ont pas de raison logique de comptabiliser cela. Cependant, il y a un impact que la société ne peut pas négliger.

Les intervenants ne sont pas complètement informés des risques en ligne, ce qui rend difficile la prise de décisions éclairées. En particulier, il est difficile pour les organisations de tirer profit d'avoir pris les bonnes mesures pour éviter les piratages, car elles ne peuvent pas transmettre leur niveau de sécurité des données aux clients. Cela démotive l'investissement dans la sécurité des données.

Recommandations

L'enquête souligne cinq recommandations pour répondre aux problèmes soulevés concernant l'économie des piratages de données.

R1 Placer les utilisateurs au centre des solutions, Et inclure les coûts pour les utilisateurs et les organisations dans l'évaluation des coûts des piratages de données.

R2 Augmenter la transparence à travers les notifications et la divulgation des piratages de données.

R3 La sécurité des données doit être une priorité. De meilleurs outils et de meilleures approches doivent être disponibles. Les organisations doivent respecter les normes de bonnes pratiques en matière de sécurité des données.

R4 Les organisations doivent être responsables de leurs défaillances. Des règles générales concernant l'affectation de la responsabilité et la compensation en cas de piratage de données doivent être établies au préalable.

R5 Stimuler l'investissement dans la sécurité en catalysant un marché pour une évaluation fiable et indépendante des mesures de sécurité des données.

La *première recommandation* est de mettre les utilisateurs au centre des solutions. Pour lancer cette approche du piratage centrée sur l'utilisateur, notre *deuxième recommandation* consiste à créer plus de transparence sur les risques, la fréquence et l'impact des piratages de données dans le monde.

Une meilleure prise de conscience augmentera l'exigence de meilleurs outils. Notre *troisième recommandation* est que la sécurité des données doit être une priorité. De meilleurs outils et de meilleures approches doivent être disponibles. Les organisations doivent être responsabilisées face aux normes de bonnes pratiques.

- **Prévention.** Pour éviter les failles connues, les outils de sécurité doivent être plus faciles à utiliser et à actualiser, y compris pour l'application de correctifs de sécurité critiques. Pour éviter les attaques d'ingénierie sociale, les organisations doivent appliquer des outils de confiance et de bonnes pratiques pour bloquer les e-mails d'hameçonnage et les maliciels intégrés, et également former leurs employés à éviter ces attaques

- **Limitation.** Les organisations doivent collecter le minimum de données nécessaires pour fournir les services souhaités tout en préservant les droits et les attentes des personnes. Les organisations doivent aussi appliquer le chiffrement aux données collectées et enregistrées, durant les échanges et le stockage. Le chiffrement doit être facile à utiliser, et dans l'idéal être appliqué par défaut, en particulier pour les particuliers.

Bien sûr, aussi pratiques que soient les outils, leur implémentation coûtent toujours du temps et de l'argent, que toutes les organisations se sont pas disposées à investir pour éviter les piratages de données et pour limiter leur impact lorsqu'ils ne peuvent être évités. Les deux dernières recommandations portent sur la façon dont ces défaillances du marché peuvent être abordées à travers des stimulations économiques sur les coûts et les avantages.

- *Quatrième recommandation.* Accroître la responsabilisation. En imposant qu'une plus grande part des conséquences externes d'un piratage de données soit supportée par les organisations les conservant, leurs coûts augmenteront et les organisations amélioreront leurs efforts pour éviter ces piratages et en limiter l'impact.

- *Cinquième recommandation.* Information de sécurité. En permettant aux organisations de signaler qu'elles sont moins vulnérables, et donc en réduisant l'asymétrie des informations, celles-ci seront plus compétitives, ce qui augmentera le retour sur l'investissement dans la prévention des piratages de données.

Les cinq recommandations sont résumées dans le cercle de sécurité.

Deux principes importants sous-tendent ces cinq recommandations : une bonne gestion des données et la responsabilité collective.

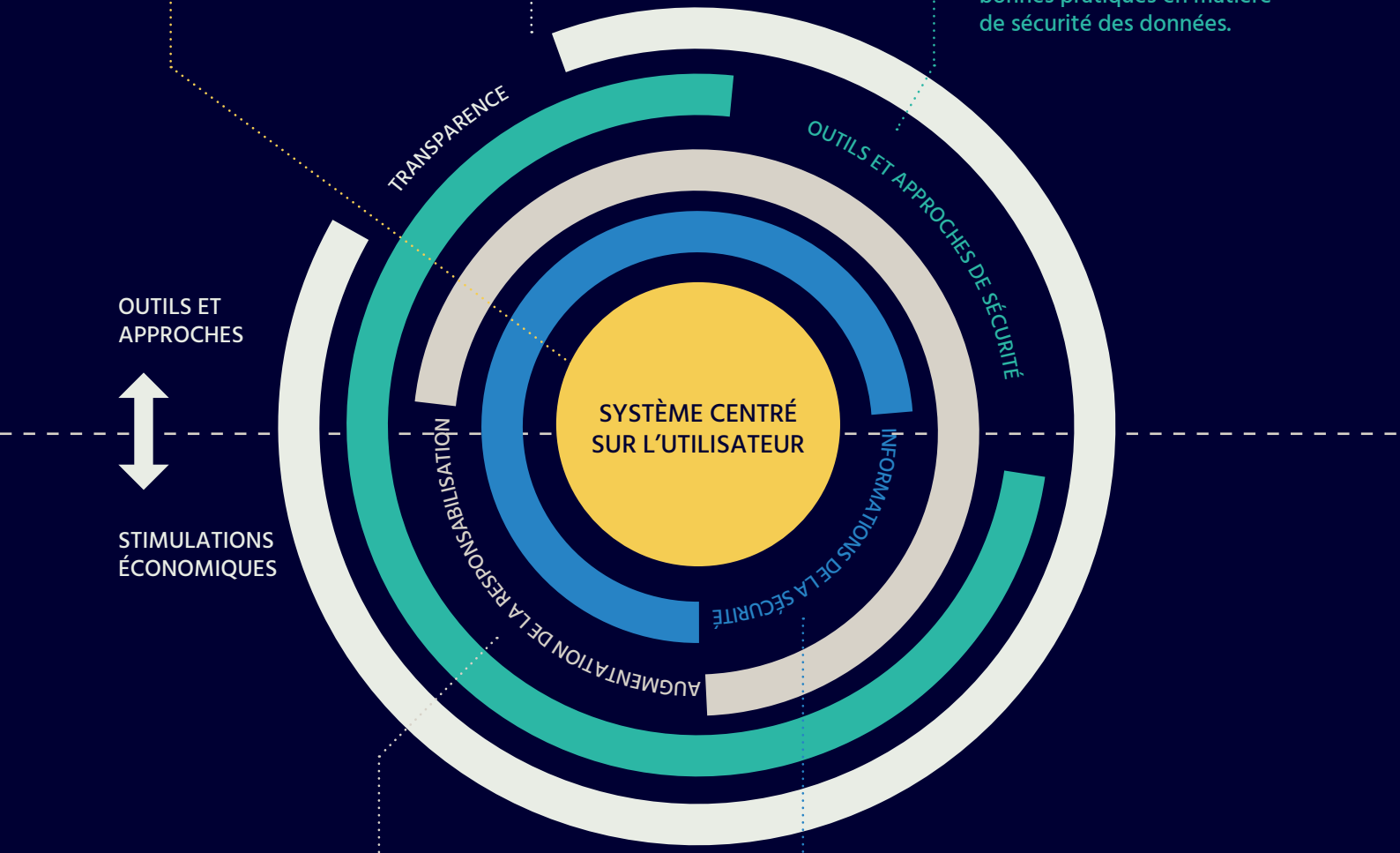
Gestion des données. Les organisations doivent se considérer comme dépositaires des données des utilisateurs, et protéger celles-ci non seulement par nécessité commerciale mais aussi au nom des utilisateurs eux-mêmes. Les organisations doivent appliquer une approche éthique à la gestion des données et comprendre qu'elles peuvent prospérer en agissant bien : protéger les utilisateurs doit être une fin en soi, protégeant ainsi l'organisation.

Cercle de sécurité

1. Placer les utilisateurs au centre des solutions, et inclure les utilisateurs et les organisations dans l'évaluation des coûts des piratages de données.

2. Augmenter la transparence à travers les notifications et la divulgation des piratages de données.

3. La sécurité des données doit être une priorité. De meilleurs outils et de meilleures approches doivent être disponibles. Les organisations doivent respecter les normes de bonnes pratiques en matière de sécurité des données.



4. Les organisations doivent être responsables de leurs défaillances. Des règles générales concernant l'affectation de la responsabilité et la compensation en cas de piratage de données doivent être établies au préalable.

5. Stimuler l'investissement dans la sécurité en catalysant un marché pour une évaluation fiable et indépendante des mesures de sécurité des données.

Responsabilité collective. Sur Internet, tout le monde est connecté. Une faille peut en amener une autre (en d'autres mots « votre défaillance pourrait être la mienne »). Les organisations ont la responsabilité de sécuriser les données qu'elles conservent. Elles partagent également une responsabilité collective avec les autres intervenants pour sécuriser l'écosystème de données dans son ensemble. Cela inclut les fournisseurs, les employés, les gouvernements et les autres. Si l'un de ces maillons est défaillant, toute la chaîne de la confiance peut être brisée.

En résumé, notre message aux organisations est le suivant :

- Les données personnelles sont précieuses et inestimables, protégez-les !
- Ne collectez que ce qui absolument nécessaire et chiffrez ce que vous conservez
- Restreignez l'accès à ceux qui en ont besoin
- Signalez le niveau de sécurité des données que vous offrez
- Détruisez les données lorsqu'elles ne sont plus utilisées
- Soyez plus transparents sur les évènements de piratage de données
- Soyez vigilants par rapport aux failles, préparez-vous, informez et agissez immédiatement

Conclusion

Les piratages de données sont une préoccupation grandissante dans le monde. Pour limiter ce problème et son impact économique, l'enquête propose de changer d'approche face au piratage et d'impliquer l'ensemble des intervenants.

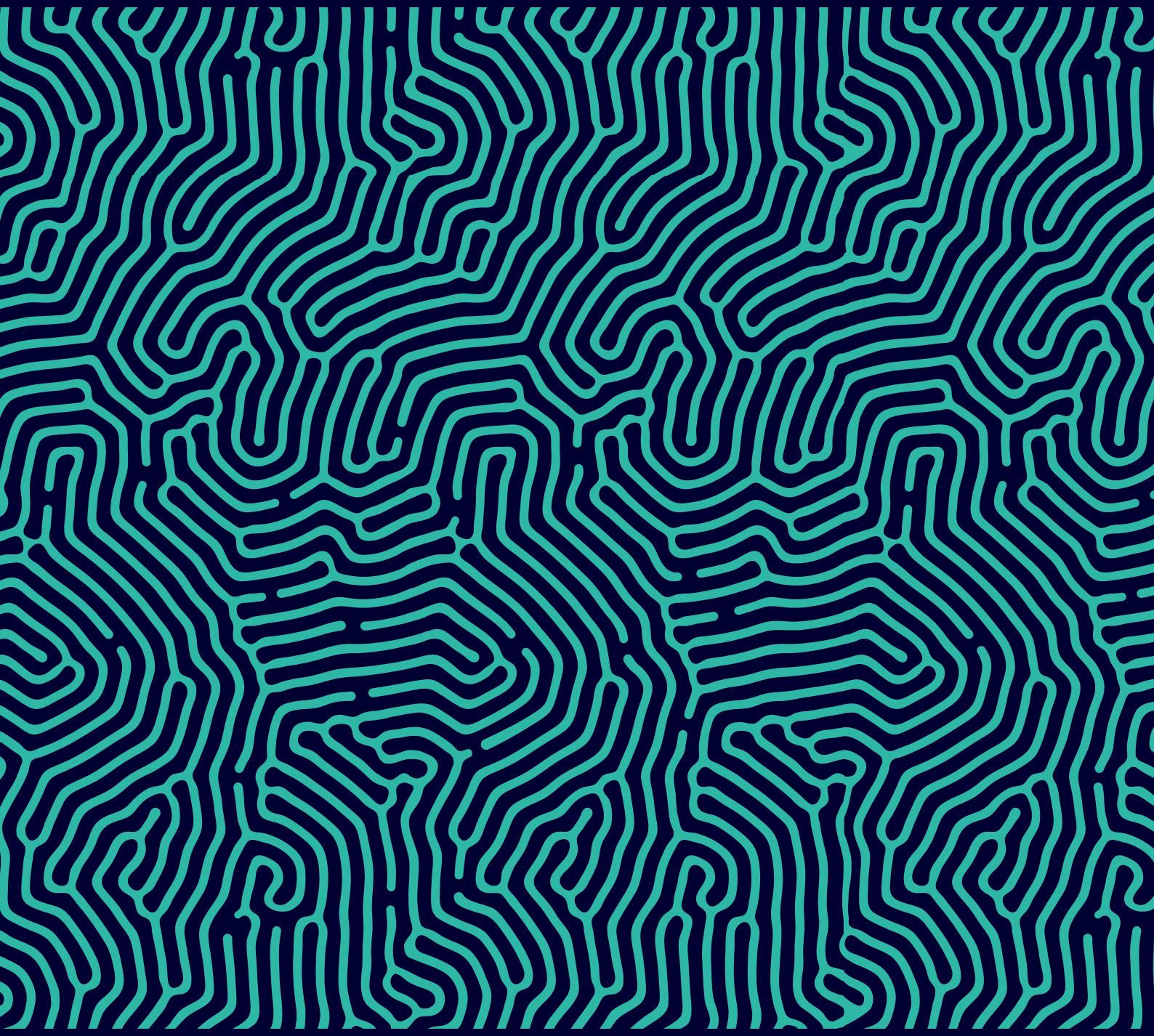
À mesure que les utilisateurs déplacent leur vie en ligne, la confiance est essentielle pour garantir les bénéfices complets d'Internet dans le monde. Cette confiance dépend de la manière dont les données des utilisateurs sont protégées contre le piratage. Chaque piratage de données crée un nouveau groupe d'utilisateurs dont la confiance a été trahie, et qui passe le mot à ses relations et plus largement à travers les articles d'information, ce qui crée le doute et sape la confiance des utilisateurs en général.

À travers cette enquête, l'objectif d'Internet Society est de proposer des recommandations pour améliorer la sécurité des données. Cela permettra d'augmenter l'usage d'Internet et d'augmenter l'impact économique et social d'Internet sur l'économie et la société au sens large. Cela permettra en retour de conforter la vision partagée par Internet Society qu'Internet est pour tous et partout.

Objets connectés

Face à un monde où les objets connectés seront partout, les vulnérabilités entraînant des piratages de données peuvent aussi s'appliquer à ces objets, avec peut-être un impact encore plus grand sur les utilisateurs. D'abord, bien évidemment, les objets connectés comme les interphones pour bébé peuvent contenir des capteurs audio et vidéo pouvant révéler des renseignements personnels sur leurs propriétaires. Cependant, d'une manière plus large que pour le piratage de données, les gens peuvent mettre leur sécurité personnelle sous le contrôle des objets connectés, comme à travers d'appareils médicaux ou de voitures connectées. Il est incroyablement pénible d'être victime du vol et de la revente de son dossier médical. Il est potentiellement fatal d'être victime du piratage et de la prise de contrôle de ses appareils de santé.

Plus largement, la plupart de nos recommandations sont valables pour la prévention ou la limitation du piratage de l'ensemble des objets connectés, et non pas seulement des données qu'ils collectent à travers leurs capteurs, mais aussi face aux failles de sécurité pouvant entraîner des risques de sécurité personnelle ou publique. C'est pourquoi Internet Society encourage l'application de ces résultats à toute la gamme de problèmes pertinents survenant de l'émergence des objets connectés. Même s'il s'agit d'un problème plus large que les piratages de données, les causes peuvent être les mêmes et doivent être prises en compte dans la priorisation de la sécurité générale de ces appareils.



Internet Society