

CYBER-RÉSILIENCE :

LA CLÉ DE
LA SÉCURITÉ
DES ENTREPRISES

#PASS2018

Introduction et sommaire	3
L'évolution des cybermenaces	5
Les défis à relever par les entreprises pour devenir cyber-résilientes	7
Adoption de la cyber-résilience	13
Les caractéristiques des entreprises cyber-résilientes	18
Conclusions	22

Introduction et sommaire

Une rapide recherche Google de l'expression « resilient company » (entreprise résiliente) donne plus de 45 millions de résultats en moins d'une seconde. Ce concept, défini comme « la capacité à récupérer rapidement d'une difficulté et à en ressortir plus fort », revêt maintenant une importance clé pour les entreprises qui sont confrontées à de nombreux risques dans le contexte d'une économie mondialisée. Ces risques englobent aussi bien les cyberattaques que les escroqueries et les vols de données personnelles à grande échelle, les effets potentiellement nuisibles des avancées technologiques telles que l'intelligence artificielle, la géoingénierie et la biologie synthétique, et ils peuvent affecter l'environnement, l'économie et, en fin de compte, les êtres humains eux-mêmes.

Nous assistons à une transformation des relations sociales, du tissu professionnel et des initiatives gouvernementales. Cette transformation repose sur le potentiel de la technologie, des données et de l'intelligence artificielle qui collecte, filtre, classe et rapproche des volumes de données importants à des fins d'apprentissage et de prévision.

La transformation numérique affecte les vies quotidiennes et le fonctionnement des entreprises à un degré tel qu'elle est aujourd'hui devenue une source de richesse pour les entreprises et un avantage concurrentiel pour les nations. Pour s'approprier cette richesse, il n'est plus nécessaire de mener des guerres traditionnelles. Un « simple » transfert numérique des données qui identifient et différencient un pays peut suffire. Une cyberbataille pour attaquer les ordinateurs clés et obtenir les informations nécessaires permet de fragiliser un gouvernement ou de lui retirer son avantage concurrentiel.

La résilience, qui s'entend comme « la capacité inhérente d'un organisme, d'une entité, d'une entreprise ou d'un état à surmonter une crise sans que son activité en soit affectée », est désormais un impératif.

Il ne s'agit pas simplement de restaurer l'activité,

mais d'opérer une véritable résurgence, une reprise en main après une série défavorable d'événements et garantir son intégrité face à la menace latente de cyberattaques.

Dans un contexte de sécurité, la cyber-résilience est la capacité d'une entreprise à maintenir ses objectifs fondamentaux.

Une entreprise cyber-résiliente sera capable d'empêcher, de détecter, de confiner et de récupérer face aux innombrables agressions contre les données, les applications et l'infrastructure informatique, en réduisant au maximum son exposition aux attaques et leur impact sur son activité. Cela concerne spécialement les terminaux et serveurs car ils hébergent les actifs les plus précieux de l'entreprise et leur compromission nuit également à l'intégrité des identités et des utilisateurs.

Avec l'aggravation des risques, les approches traditionnelles du maintien de la cyber-résilience ne suffisent plus. Un grand nombre d'entités survivent dans un équilibre précaire où le moindre changement, même négligeable par rapport à la taille de l'entreprise ou à l'importance de ses activités, peut précipiter une crise. Pour éviter une catastrophe, la gestion de la cybersécurité doit être méthodiquement revue et de nouveaux modèles de protection doivent être mis en œuvre.

Jusqu'à récemment, les principales cibles d'attaques étaient les institutions financières et les administrations. Aujourd'hui, étant donné que le développement des entreprises de toutes les tailles et de tous les secteurs dépend dans une mesure plus ou moins grande d'Internet, la menace est devenue universelle. Avec ces dangers de plus en plus pressants, les approches traditionnelles du maintien de la cyber-résilience ne fonctionnent plus. La gestion de la cybersécurité doit être revue en profondeur et de nouveaux modèles de sécurité ou des modèles plus performants doivent être adoptés.

Nous avons été confrontés il y a peu aux cas Spectre et Meltdown, qui ont révélé des vulnérabilités logicielles et matérielles. De même, entre 2011 et 2014, nous avons vu comment des fournisseurs d'énergie au Canada, en Europe et aux États-Unis ont été attaqués par le groupe de cyber-espionnage Dragonfly. En mai 2017, le logiciel de rançon WannaCry a pris en otage des entreprises publiques et privées de télécommunications, de santé et de logistique. En 2017 également, le logiciel de rançon NotPetya a ciblé des entreprises européennes majeures dans pratiquement tous les secteurs d'activité.

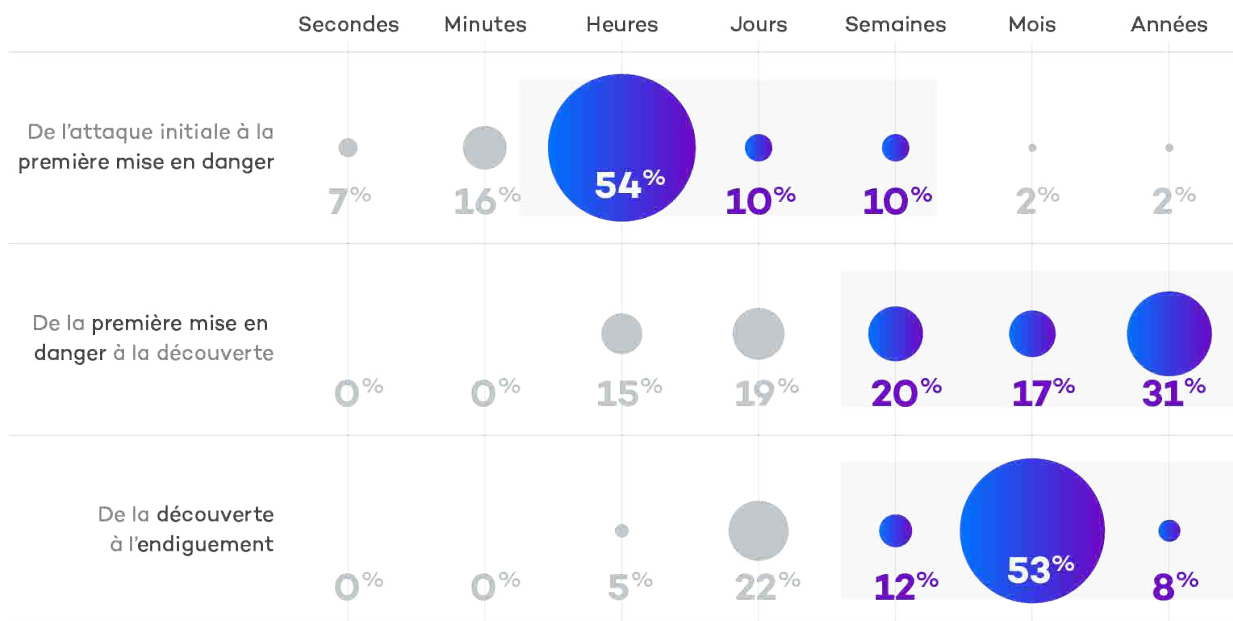
Mais alors que la collectivité est en plus en plus sensibilisée à la cybersécurité, ce sujet devient également de plus en plus confus. Les entreprises et leurs dirigeants sont submergés par l'ampleur de la tâche. Une étude a été menée cette année par Forrester Consulting pour Hiscox1 auprès de 4 100 cadres, RSSI, directeurs informatiques, et autres personnels décisionnaires au Royaume-Uni, aux États-Unis, en Allemagne, en Espagne et aux Pays-Bas. 57 % des entreprises interrogées ont déclaré s'attendre à devoir faire face à des cyberattaques. Une étude plus détaillée par le biais de questions indirectes montre toutefois que 73 % des entreprises interrogées sont à des faibles niveaux de maturité dans le domaine de la détection et de la réponse

aux cyberattaques. Seules 11 % des entreprises disposent d'experts dans leurs équipes de sécurité et sont, par conséquent, bien préparées aux défis actuels de la cybersécurité.

Pour augmenter et maintenir leur résilience face aux cyberattaques, les entreprises doivent adopter une nouvelle attitude : globale, stratégique et persistante, avec une nouvelle approche des programmes de sécurité capable de protéger l'entreprise sans imposer des restrictions inutiles à ses activités. Cette nouvelle attitude implique de renforcer les défenses préventives, en partant du principe qu'elles pourront être contournées par les attaquants ou que ceux-ci sont déjà présents dans l'entreprise.

Avec les nouvelles techniques de pénétration des défenses et de dissimulation des logiciels malveillants, les menaces peuvent rester longtemps dans le réseau d'une entreprise sans être détectées.

Les menaces internes ne doivent pas non plus être négligées. Les attaques de la part d'employés disposant d'un accès privilégié sont une des plus grandes menaces envers la sécurité des données des clients et des entreprises. Des études menées par le Ponemon Institute montrent que les pirates et les employés malveillants sont les principaux responsables des failles de sécurité et des fuites de données.



Données du DBIR (2016).

¹ 2018 Hiscox Cyber Readiness Report <https://www.hiscox.com/sites/default/files/content/2018-Hiscox-Cyber-Readiness-Report.pdf>

Une entreprise résiliente empêche la compromission de ses actifs et détecte les attaques en un temps réduit avant tout dommage. Il est temps à présent de mettre en application des techniques telles que la traque des menaces, les analyses a posteriori pour identifier la cause première d'une attaque, la détection et la réponse sur le poste client (EDR), et la surveillance constante des terminaux. L'étude minutieuse des incidents requiert des données d'analyse en temps réel.

Une entreprise expérimentée en résilience reconnaîtra également l'existence de défauts et d'erreurs, et aura les moyens de restaurer un fonctionnement normal pour sécuriser ses actifs et sa réputation. Autrement dit, l'entreprise pourra sortir renforcée de l'incident en appliquant des changements qui améliorent sa défense.

L' évolution des cybermenaces

Le cybercrime est une activité attrayante et hautement lucrative. Les attaquants ont à leur disposition des ressources, aussi bien techniques qu'économiques, d'un volume et d'une qualité qui n'ont jamais existé auparavant. Ils peuvent ainsi développer des attaques de plus en plus sophistiquées. Cela aboutit à des menaces plus complexes, plus dynamiques et plus nombreuses.

[Equifax](#), [CCleaner](#), [WPA2](#), [Vault7](#), [CIA](#), [KRACK](#), [NSA](#), [le piratage d'élections](#) sont quelques protagonistes ayant marqué le paysage de la cybersécurité d'entreprise de ces derniers mois. On aura ainsi vu des infections massives, des vols de données, des attaques par des logiciels de rançon, des applications piratées lançant des attaques contre un pays ou effectuant des attaques ciblées contre de grandes entreprises, ou encore des exploitations de vulnérabilités affectant des milliards d'appareils.

Les dégâts causés par trois événements récents doivent être examinés plus en détail. Entre 2011 et 2014, le groupe de cyberespionnage Dragonfly a fait régulièrement les gros titres en développant rapidement ses activités et en mettant en difficulté des entreprises du secteur de l'énergie en Europe et en Amérique du Nord. Dragonfly exploitait deux

composants de base d'un programme malveillant via des outils d'accès à distance, pour accéder à des ordinateurs infectés et les contrôler.

En 2017, **deux attaques se sont distinguées par leur impact et les dégâts qu'elles ont causés : WannaCry et GoldenEye/NotPetya.**

[WannaCry](#) est apparue en mai. Provoquant le chaos dans des réseaux d'entreprise et se propageant dans le monde entier, elle a été l'une des attaques les plus importantes de l'histoire. Bien que nous ayons pu voir par le passé des attaques beaucoup plus puissantes (comme Blaster ou SQLSlammer, pour n'en citer que deux), en nombre de victimes et en vitesse de propagation, les dommages que ces attaques avaient causés n'étaient que collatéraux. WannaCry, par contre, est un logiciel de rançon avec une capacité de ver réseau, faisant en sorte que chaque ordinateur infecté voit ses documents piratés.

[Goldeneye/NotPetya](#) a été la deuxième attaque la plus marquante de l'année 2017, comme une réplique du tremblement de terre WannaCry. Même si ses victimes se sont d'abord limitées à une zone géographique spécifique (l'Ukraine), elle a fini par toucher des entreprises dans plus de 60 pays.

Clairement planifiée, cette attaque avait été perpétrée via une application comptable très courante dans le milieu professionnel ukrainien, M.E.Doc. Les attaquants avaient compromis les mises à jour serveur de ce logiciel, afin que tous les ordinateurs sur lesquels M.E.Doc était installé puissent être infectés instantanément et automatiquement.

En plus de crypter les fichiers, si l'utilisateur connecté disposait de permissions d'administrateur, le logiciel malveillant ciblait le MBR (Master Boot Record) du disque dur. De prime abord, cela ressemblait à un logiciel de rançon de la même veine que WannaCry, mais une analyse poussée a montré que **ses auteurs n'avaient pas l'intention de permettre la récupération des données cryptées**. Quelques jours plus tard, le gouvernement ukrainien a ouvertement accusé la Russie d'être à l'origine de l'attaque.

En matière de cybersécurité, l'année 2018 n'aurait pu démarrer plus mal : [la faille de sécurité](#) découverte dans les processeurs Intel, AMD et ARM était, elle aussi, particulièrement grave.

Ce défaut de conception d'architecture, accompagné d'erreurs dans le système d'exploitation, mettait véritablement en péril le secteur technologique. Tous les intervenants concernés ont travaillé sans relâche pour y mettre un terme aussi rapidement que possible.

Cette faille, utilisée par **l'exploitation Meltdown** dans les architectures Intel, est particulièrement critique pour l'exfiltration de données sensibles telles qu'identifiants d'accès, e-mails, photos et autres documents. Elle permet à un attaquant, par le biais d'un processus malveillant s'exécutant au niveau utilisateur sur l'ordinateur ou le serveur, de lire la mémoire d'autres processus, y compris des processus à privilège du noyau du système d'exploitation.

Les particuliers et la plupart des entreprises sont affectés, car Specter peut agir sur les ordinateurs de bureau, les ordinateurs portables, les smartphones Android, les serveurs sur site et les serveurs Cloud. Plus les informations traitées sont critiques, plus le risque d'être la cible d'une attaque de ce type est grand.

Et il existe bien d'autres cas réels affectant les géants de différents secteurs. C'a été, par exemple, le cas d'**Apple**, avec l'arrestation en Chine de 22 personnes accusées d'accès frauduleux à ses données. Toutes les preuves ont pointé vers des employés internes, car certaines des personnes arrêtées travaillaient pour des sous-traitants d'Apple et avaient accès aux données faisant l'objet du trafic.

HBO a également été la cible de plusieurs cyberattaques ces derniers mois. Dans l'une d'entre elles, des serveurs ont été compromis et des épisodes entiers non encore diffusés de différentes séries télévisées ont été dérobés, de même que des informations internes.

InterContinental Hotels Group (IHG) a été victime d'un vol de données client. Bien que l'entreprise ait déclaré en février que l'attaque n'avait affecté qu'une douzaine de ses hôtels, nous savons maintenant que des terminaux de points de vente de plus d'un

millier de ses établissements ont été infectés. Ce groupe est notamment propriétaire des chaînes Holiday Inn, Holiday Inn Express, InterContinental, Kimpton Hotels et Crowne Plaza.

La **Saber Corporation** est une entreprise américaine qui gère les réservations pour 100 000 hôtels et plus de 70 compagnies aériennes à travers le monde. Un attaquant a obtenu des informations d'identification lui permettant d'accéder à l'un des systèmes de réservation de l'entreprise et donc à des informations de paiement et de réservation. Ce système gère les réservations de particuliers et d'agences de voyage pour 35 000 hôtels et établissements d'hébergement. Il a été compromis du 10 août 2016 au 9 mars 2017, soit pendant sept mois complets.

Mais la plus grande violation de sécurité de l'année — et l'une des pires de l'histoire — s'est produite un peu plus tard, lorsqu'on a appris que le géant de l'évaluation de crédit, **Equifax**, avait également été compromis. L'entreprise a indiqué que cette compromission avait affecté 147,9 millions d'individus. La question qui se pose est de savoir si une attaque pareille aurait pu être évitée ? La réponse est, bien sûr, affirmative. **Equifax avait laissé la porte ouverte aux cybercriminels en ne mettant pas à jour** le framework de développement d'applications Web **Apache Struts**. L'absence de correction de cette vulnérabilité a permis à des pirates d'accéder aux numéros de sécurité sociale, aux adresses postales et aux numéros de permis de conduire de millions de personnes. Il s'agit là d'un exemple montrant comment un manquement aux mesures de sécurité de base telles que l'application de correctifs peut avoir d'énormes conséquences.

Avec de tels précédents, il n'y a rien d'étonnant à ce que 75 % des entreprises (selon une étude récente de McKinsey²) considèrent que la cybersécurité est une priorité pour leur fonctionnement. La préparation à une cyberattaque est une préoccupation majeure dans des domaines tels que la banque ou la production automobile, alors qu'on pourrait croire que ces domaines sont davantage préoccupés par des changements et des risques de plus grande ampleur. Nous sommes face à une menace universelle et horizontale.

² <https://www.mckinsey.com/business-functions/risk/our-insights/a-new-posture-for-cybersecurity-in-a-networked-world>

La menace est trop grande et le nombre et le degré de sophistication des attaquants augmentent trop rapidement.

Pour augmenter et maintenir leur résilience face aux cyberattaques, les entreprises doivent adopter une nouvelle attitude : globale, stratégique et persistante, avec une nouvelle approche de leur programme de sécurité, capable de les protéger sans imposer des restrictions néfastes à leurs activités.

Cette nouvelle approche devrait reposer sur le renforcement des défenses préventives, mais en partant du principe que les attaquants peuvent les surmonter et qu'ils peuvent même être déjà dans l'entreprise, parce qu'ils y travaillent ou qu'ils sont parvenus à s'y infiltrer. La tâche consistera alors à les empêcher de compromettre les actifs de l'entreprise en les détectant avant tout dommage et en réagissant aussi rapidement que possible. Une entreprise résiliente doit aussi pouvoir ressortir de l'incident encore plus forte, ayant appliqué des changements qui améliorent ses capacités de défense.

Les défis à relever par les entreprises pour devenir cyber-résilientes

Chaque entité, entreprise ou état est soumis à des tensions du fait des événements, changements et incidents qui se produisent dans son environnement.

Ces situations de tension sont de nouveaux problèmes dont la résolution affecte le fonctionnement de l'entreprise dans la mesure où ils ne peuvent pas être gérés de façon automatique.

En matière de sécurité, une telle situation de tension nécessite une réflexion nouvelle sur le programme de sécurité de toute l'entreprise. Les entreprises doivent identifier les actifs ayant le plus de valeur et définir un nouveau modèle de gouvernance

de la sécurité qui centralise, avec une équipe de sécurité experte, la supervision de tous leurs efforts de cybersécurité. Le responsable de cette équipe prend alors part aux décisions de l'entreprise, au sein de son équipe dirigeante.

Des menaces plus nombreuses, et d'intensité plus grande

Aux États-Unis, la Comprehensive National Cybersecurity Initiative (CNCI) a été lancée par l'administration Bush en janvier 2008.

Cette initiative a introduit une approche différenciée de l'identification des menaces de cybersécurité existantes et émergentes, par la découverte et le blocage des vulnérabilités existantes, et l'accumulation de retour d'expérience face aux acteurs tentant d'accéder aux systèmes d'information fédéraux. Le président Obama avait déclaré que "les cybermenaces sont l'un des défis les plus graves pour l'économie et la sécurité nationale auxquels nous ayons affaire en tant que nation" et que "la prospérité économique des États-Unis au 21ème siècle dépendra de la cybersécurité."³

³ https://www.es.w3eacademy.com/wiki/State_security

Vers la cyber-résilience

La capacité à récupérer rapidement après des difficultés et à en ressortir plus fort.



Figure 1. Le progrès technologique contribue à l'évidence à la croissance des entreprises. Les entreprises et le monde en général sont plus connectés qu'ils ne l'ont jamais été et le développement technologique est le plus rapide qui ait jamais existé. Cette interconnectivité engendre à la fois des opportunités et des risques.

En décembre 2017, l'administration du président Donald Trump a publié un document de stratégie nationale⁴ évoquant à de nombreuses reprises les problèmes de cybersécurité et n'hésitant pas à désigner les pays susceptibles de se servir de réseaux de terminaux contre les États-Unis.

Ce document déclare notamment que les gouvernements de Russie, de Chine, de Corée du Nord et d'Iran ont le pouvoir de déstabiliser l'économie et de menacer les infrastructures critiques de la nation. Il indique que les États-Unis dissuaderont, se défendront et, si nécessaire, combattront et viendront à bout des acteurs qui utilisent des cyberattaques contre eux.

C'est là une réalité : partout dans le monde, la menace des cyberattaques grandit à la fois en quantité et en intensité, et l'évolution rapide et inéluctable de la transformation numérique contribue à créer de nouvelles opportunités pour les pirates. Voici quelques chiffres qui illustrent clairement cette tendance :

- 10 millions de nouveaux appareils se connectent chaque jour dans le monde entier. On estime que d'ici 2020, le nombre d'appareils interconnectés s'élèvera à 20,8 milliards⁵.
- Les entreprises investissent près de 500 millions de dollars en cybersécurité⁶, et 50 % des CEO

des entreprises réalisant plus de 500 millions de dollars de bénéfice ne s'estiment pourtant pas préparés à faire face aux cyberattaques avec toutes les garanties nécessaires⁷, 82 % des dirigeants sont en outre préoccupés ou très préoccupés par la cybersécurité⁸.

- Dans le monde entier, plus de 100 milliards de lignes de code sont écrites chaque année, générant des millions de vulnérabilités dans les ordinateurs et les serveurs.
- Chaque année, plusieurs milliards d'ensembles de données font l'objet d'une violation.
- En 2017, les pirates ont produit près de 120 millions de nouvelles variantes de logiciels malveillants. À ce jour, le nombre total de logiciels malveillants répertoriés par AV-TEST avoisine les 800 millions⁹.

⁴ <https://www.whitehouse.gov/wp-content/uploads/2017/12/NSS-Final-12-18-2017-0905.pdf>

⁵ https://www.isaca.org/chapters7/Monterrey/Events/Documents/20172408_Ciberseguridad_Fundamental_Trans_Digital.pdf

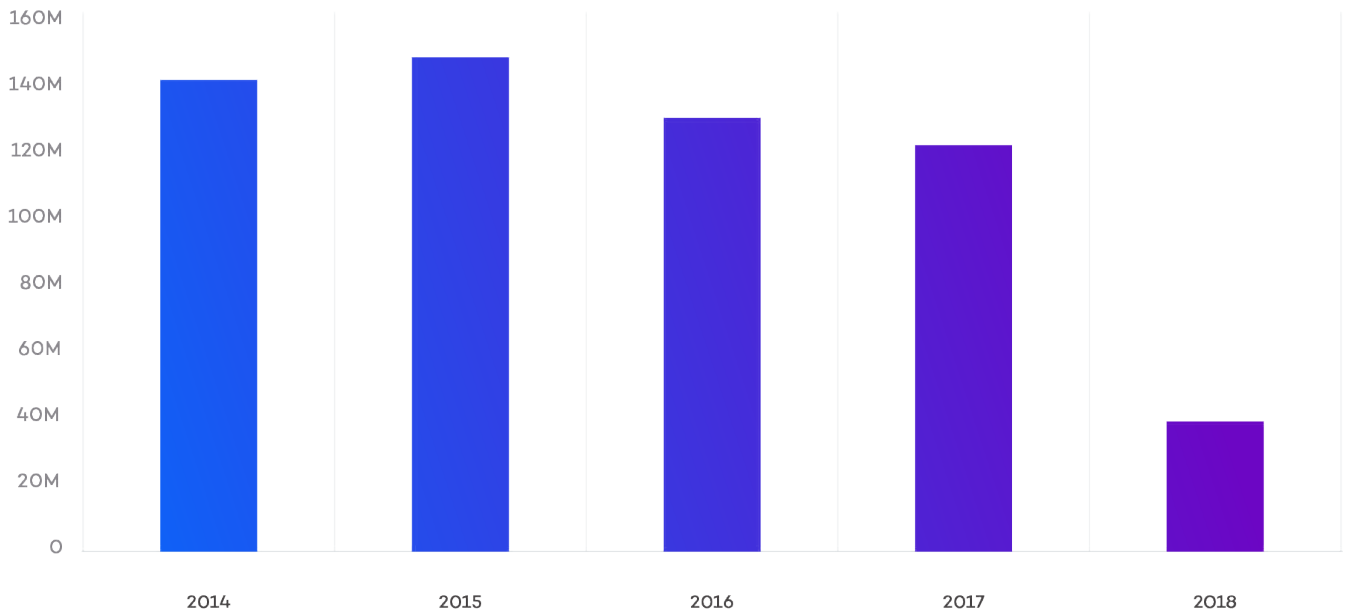
⁶ <https://cybersecurityventures.com/cybersecurity-market-report/>

⁷ Global CEO Outlook 2015 – KPMG. <https://assets.kpmg.com/content/dam/kpmg/pdf/2015/08/global-ceo-outlook-2015.pdf>

⁸ ISACA/RSA Conference State of Cybersecurity study

⁹ <https://www.av-test.org/en/statistics/malware/>

Nouveaux logiciels malveillants



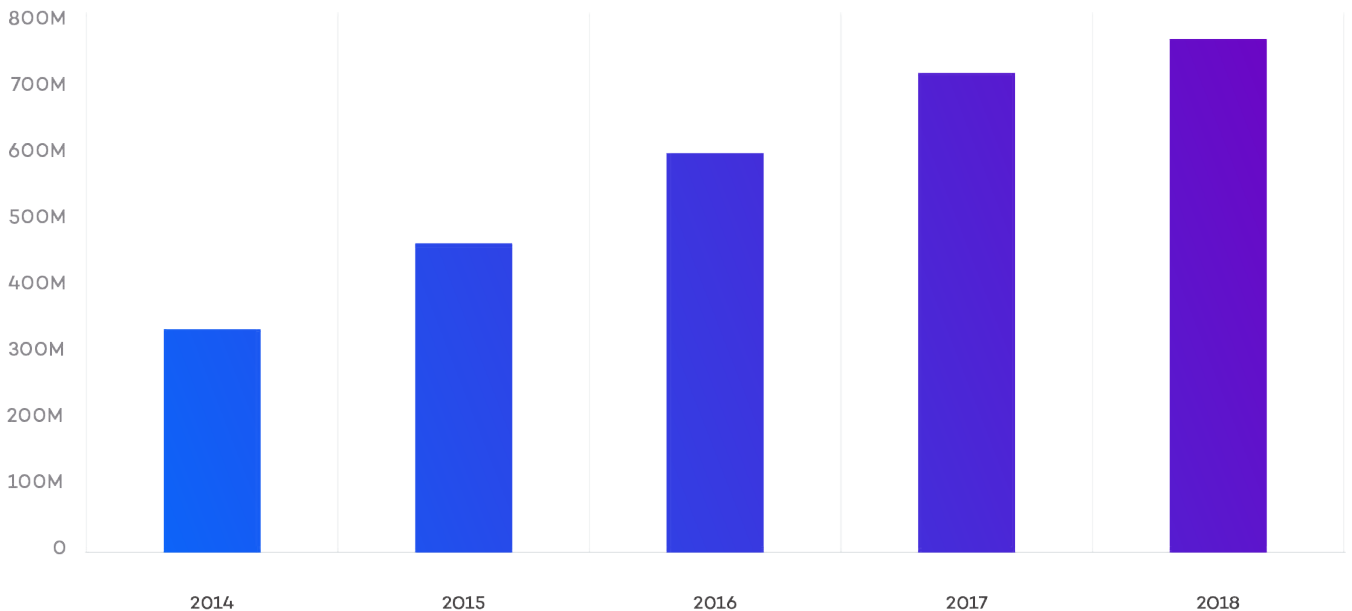
M=Million

Mise à jour : 04-09-2018

Copyright © AV-TEST GmbH, www.av-test.org

J.P. Morgan Chase & Co. a multiplié par deux son budget annuel de cybersécurité pour passer de 250 millions de dollars à 500 millions de dollars en 2017. Bank of America a déclaré que son budget pour combattre la cybercriminalité était illimité.

Nb total de logiciels malveillants



M=Million

Mise à jour : 04-09-2018

Copyright © AV-TEST GmbH, www.av-test.org

<https://www.av-test.org/en/statistics/malware/>. Mise à jour le 9 avril 2018.

Étonnamment, la plupart des entreprises victimes de NotPetya et WannaCry auraient probablement déclaré au moment des attaques qu'elles étaient bien protégées. Même lorsqu'elle n'est pas la cible principale, une entreprise court le risque d'être touchée par des attaques contre des applicatifs courants. Et malgré tous les nouveaux systèmes de défense, les entreprises ont toujours besoin de 191 jours, en moyenne, pour détecter une attaque masquée, ce qui représente quand même une amélioration par rapport aux 201 jours qui leur étaient nécessaires en 2016¹⁰. Les dommages qu'un attaquant peut infliger pendant cette période ne doivent pas être sous-estimés.

L'enquête SANS Institute on Incident Response¹¹ parue en 2016 a révélé que pour 21 % des entreprises, le temps moyen de détection (MTTD, Mean Time to Detect) était de deux à sept jours, et que 29 % seulement des entreprises avaient été capables

de détecter un incident en 24 heures maximum. La même étude indique que seulement 18 % des entreprises avaient pu aller de la détection à la réponse (MTTR) en une journée. Plus grave, 38 % ont admis qu'elles ne réagissent généralement pas en moins d'une semaine.

Selon l'étude sur l'importance de la résilience pour renforcer la sécurité dans les entreprises menée par le Ponemon Institute et publiée en mars 2018, la gravité et le volume des incidents de sécurité auxquels les entreprises sont confrontées augmentent avec le temps nécessaire à leur résolution.

Comme illustré à la Figure 1, tirée de l'étude du Ponemon Institute sur la cyber-résilience, 64 % des entreprises interrogées déclarent que le volume a augmenté et 65 % déclarent que la gravité a augmenté.

Figure 13. Évolution du volume et de la gravité des incidents de sécurité au cours des 12 derniers mois

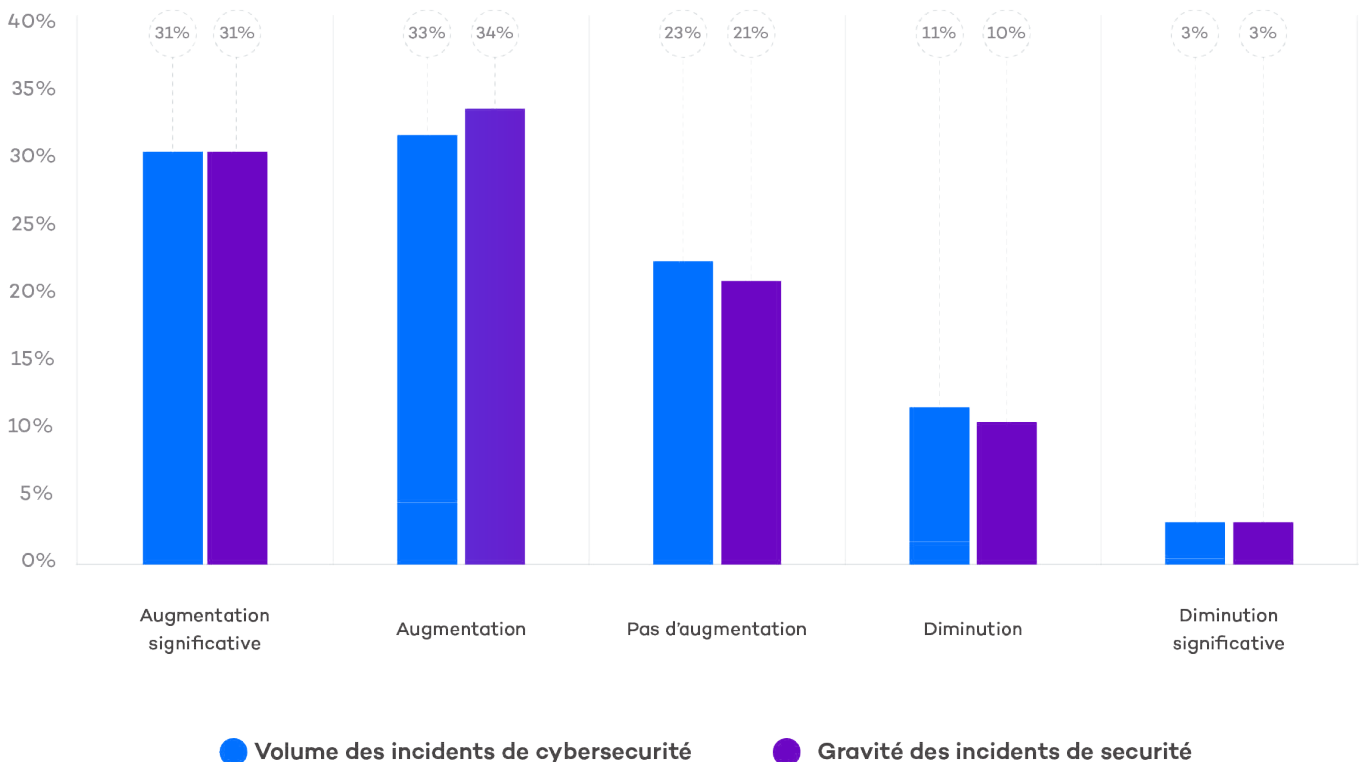


Figure 1. Évolution du volume et de la gravité des incidents de sécurité au cours des 12 derniers mois selon une étude du Ponemon Institute de mars 2018

¹⁰ 2017 Cost of Data Breach Study (Ponemon Institute for IBM Security)

¹¹ <https://www.sans.org/reading-room/whitepapers/incident/incident-response-capabilities-2016-2016-incident-response-survey-37047>

L'augmentation du volume et de la gravité affecte le temps de détection et de réponse, qui a augmenté de façon importante. La Figure 2 montre que 57 % des entreprises interrogées déclarent que ce temps a augmenté.

Complexité de l'infrastructure informatique

La complexité grandissante rend les entreprises plus vulnérables. Alors que les cybercriminels deviennent de plus en plus performants, les entreprises s'ouvrent de plus en plus au numérique, et donc aux vulnérabilités et aux cyberattaques. Les actifs tels que les conceptions de nouveaux produits, les réseaux de distribution ou les données client sont maintenant en danger. La connectivité numérique devient aussi de plus en plus complexe, une simple connexion numérique pouvant unifier des milliers de gens, et une quantité innombrable d'applications, de serveurs, de terminaux et autres appareils. Les actifs d'une entreprise sont aujourd'hui plus exposés qu'ils ne l'ont jamais été.

Quelques erreurs courantes

La cybersécurité d'entreprise lutte pour suivre le rythme rapide de l'évolution des cyber-risques¹², avec une approche erronée et une posture inefficace dans un grand nombre de cas. Voici quelques-unes des pratiques inappropriées les plus répandues :

- **Déléguer le problème au département informatique.** De nombreux cadres traitent la cybersécurité comme un problème technique et la délègue au département informatique. Cette réaction, due en partie aux nombreuses questions techniques soulevées, ignore le fait que défendre une activité économique et protéger des serveurs informatiques sont des problématiques différentes. Défendre une activité nécessite d'appréhender les éléments essentiels en jeu selon les priorités de l'entreprise. Cela requiert de connaître le modèle commercial et la chaîne de valeur, la culture du risque, les rôles, les responsabilités et la gouvernance de l'entreprise.

Figure 14. Évolution du temps nécessaire à la détection, au confinement et à la réponse à un cybercrime au cours des 12 derniers mois

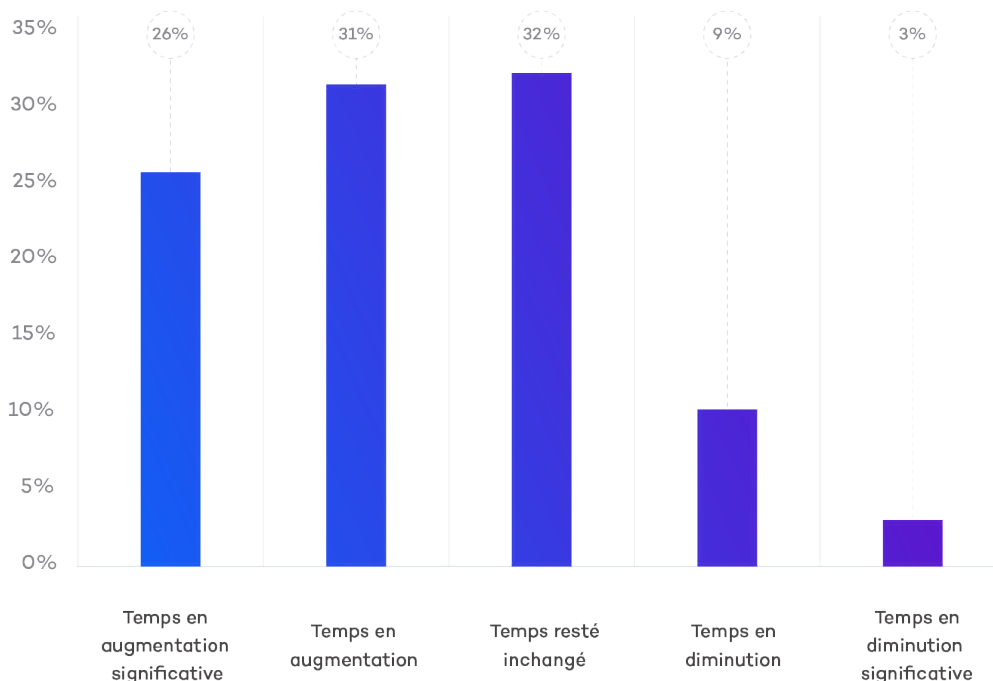


Figure 2. Évolution du temps moyen de détection et de réponse aux incidents de sécurité au cours des 12 derniers mois selon une étude du Ponemon Institute de mars 2018

¹² L'AV-TEST Institute enregistre plus de 250 000 nouveaux programmes malveillants chaque jour. <https://www.av-test.org/en/statistics/malware/>

- Le **département informatique** ne peut pas traiter la cybersécurité à lui seul ; celle-ci doit être l'affaire de l'entreprise tout entière.
- **Suivre la tendance consistant à utiliser des « Hackers » chevronnés ou des experts pour résoudre le problème.** D'autres entreprises supposent que la menace disparaîtra si elles engagent suffisamment de « Hackers » chevronnés. Mais même les meilleurs professionnels n'ont pas la capacité d'anticiper et de contenir les attaques contre les appareils d'un réseau complexe. La solution nécessite certes des experts, mais aussi des technologies et des processus préparés et qualifiés pour cette tâche. Des investissements à moyen terme et des efforts constants sont nécessaires pour sensibiliser au risque et à ses conséquences tous les départements de l'entreprise, y compris la direction, et les impliquer.
- **Traiter le risque comme un problème de conformité aux réglementations applicables.** Certaines entreprises ont tendance à introduire chaque semaine de nouveaux protocoles de sécurité et de nouvelles listes de vérification. De telles pratiques mettent trop fortement l'accent sur une conformité formelle plutôt que sur une résilience réelle.
- Donner la priorité aux actifs les plus précieux pour l'entreprise.
- Connaître, comprendre et donner la priorité aux menaces et aux adversaires les plus importants de l'entreprise.
- Connaître et mettre en œuvre les meilleures défenses contre les menaces actuelles et potentielles.
- Être prêt pour le cas où les adversaires pourraient contourner toutes les technologies de sécurité, et les détecter, les confiner et remédier à leurs actions aussi rapidement que possible pour minimiser les dommages pour l'entreprise.
- Adopter une position de crise qui recherche activement et de façon continue les menaces, et détecter les points vulnérables susceptibles d'être utilisés par des acteurs de menaces afin de réduire la surface d'attaque.
- Gérer au niveau de l'entreprise toutes les communications au sujet d'une compromission.
- Définir et mettre constamment en œuvre des initiatives pour minimiser les risques et relancer le cycle d'amélioration continue dans la gestion de la sécurité d'entreprise.

Adoption de la cyber-résilience

En ayant à l'esprit ce panorama complexe et réel, comment une entreprise qui souhaite protéger ses actifs de la manière la plus efficace possible peut-elle parvenir à une approche plus adaptative, plus complexe et plus collaborative dans sa lutte ?

La cybersécurité devrait être traitée comme un problème de gestion du risque d'entreprise, non comme un problème interne de l'informatique. Les éléments clés de cette gestion sont les suivants :

L'adaptation est essentielle. Les processus, technologies, outils et services de sécurité de l'entreprise devraient être revus et ajustés à mesure que les menaces évoluent, par une amélioration continue basée sur la défiance. Être résilient implique que cette adaptation s'effectue dans un temps minimum, à une vitesse maximum, voire même en temps réel.

L'approche complète de la gestion de la cybersécurité dans les entreprises

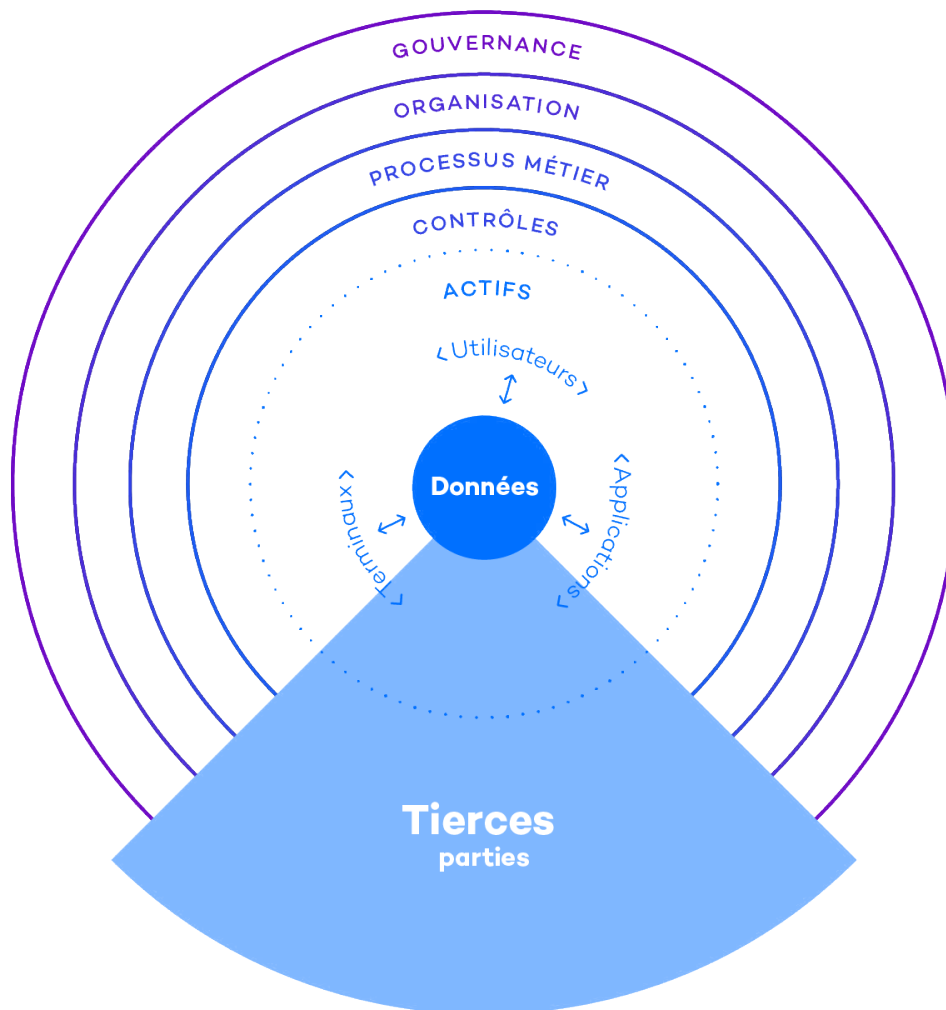


Figura 4. L'approche complète de la gestion de la cybersécurité dans les entreprises.

Les entreprises doivent analyser leurs risques et les réduire à tous les niveaux. Établir une liste complète de tous les actifs, des données aux applications, et surveiller toutes les actions entreprises sur ces actifs est un processus long et fastidieux, mais nécessaire. Les entreprises doivent utiliser des outils et services qui automatisent les tâches de profilage, de classification et de surveillance de leurs actifs (humains, données, infrastructure) à des fins de prévention et/ou de détection anticipée des adversaires.

Établir un « cycle de résilience ».

Les entreprises doivent comprendre et adopter le processus de « cycle de résilience », qui aidera les équipes de sécurité à profiter constamment de l'expérience acquise grâce aux menaces bloquées et/ou détectées.

Cela leur impose d'apprendre et de s'adapter aux phases clés de la résilience :

- **Dans la phase pré-incident,** grâce à la capacité à mieux prévenir les menaces et y résister, en incluant des technologies avancées susceptibles de détecter les logiciels malveillants connus et inconnus ou « zero-day ».
- **Pendant l'incident,** en réagissant rapidement avec des fonctions de détection, de confinement et de réponse aux événements soudains qui menacent l'entreprise. En réduisant également au maximum l'impact de l'incident sur l'activité et en exploitant les nouvelles fonctions de surveillance et d'observation des solutions de détection et de réponse sur le poste client (Endpoint Detection and Response, EDR).





Actifs	Menaces	Contrôles
 <p>Données</p>	<ul style="list-style-type: none"> • Violation de données • Mauvaise usage / manipulation d'informations • Corruption de données 	<ul style="list-style-type: none"> • Protection des données (ex, cryptage) • Capacité de récupération de données • Défense du périmètre
 <p>Personnes</p>	<ul style="list-style-type: none"> • Vol d'identité • "Man in the middle" • Ingénierie sociale • Abus d'autorisation 	<ul style="list-style-type: none"> • Accès contrôlé • Suivi de compte • Compétences en sécurité et formation • Filtrage en arrière-plan • Sensibilisation et contrôle des personnels
 <p>Terminaux</p>	<ul style="list-style-type: none"> • logiciel malveillant 	<ul style="list-style-type: none"> • Contrôle des accès privilégiés • Surveillance des processus • Prévention de l'exécution des logiciels malveillants • Contrôles du réseau (configuration, ports) • Inventaire • Configuration sécurisée • Évaluation en continue de la vulnérabilité
 <p>Applications</p>	<ul style="list-style-type: none"> • Manipulation de logiciel • Installation non autorisée de logiciel • Mauvaise utilisation du système d'information • Déné de service 	<ul style="list-style-type: none"> • Protection pour email et navigateurs web • Sécurités des logiciels et applicatifs • Inventaire • Configuration sécurisée • Évaluation en continue de la vulnérabilité

Figura 5. Risques et contrôles à mettre en œuvre à tous les niveaux, des données et des entités aux postes clients et aux applications qui s'exécutent dessus.

- **Dans la phase après incident**, en absorbant les chocs tout en continuant à atteindre les objectifs de sécurité stratégiques et en reconstruisant l'environnement d'exploitation de façon à se débarrasser des sources futures d'interruption. C'est ce qu'on appelle la «réduction de la surface d'attaque».

Prévention, détection et réponse.

Il est sain d'admettre que tôt ou tard chaque entreprise puisse être compromise par une cyberattaque. À cet instant, le temps nécessaire à la détection et à la réponse à l'incident est critique. Il faut trouver un bon équilibre entre la réponse et la restauration le plus rapidement possible du niveau de service de l'activité, et l'analyse de l'incident, de l'origine de l'attaque et la mise en place de mesures pour l'éviter dans le futur. Comme nous l'avons

définie dans l'introduction, la cyber-résilience est la capacité d'une entreprise à maintenir ses objectifs fondamentaux et son intégrité face à la menace d'attaques de cybersécurité. Une entreprise cyber-résiliente est capable d'empêcher, détecter, confiner et restaurer, en réduisant au maximum l'exposition et l'impact sur l'activité, face aux innombrables attaques contre les données, les applications et l'infrastructure informatique.

Cela concerne particulièrement le poste client, là où résident les actifs les plus précieux de l'entreprise, et l'intégrité des identités utilisateur.

Même si nous savons que la prévention totale n'est jamais garantie, les entreprises devraient s'efforcer de réduire au maximum le coût des cyberattaques en renforçant la prévention dans les phases avant exécution, en empêchant l'attaque d'exécuter du code malveillant sur les postes clients et les serveurs.

Il est également important de compléter une stratégie de cybersécurité par des capacités de détection et de réponse rapides dans les phases pendant et après l'exécution, pour identifier les dommages, restaurer les systèmes et ramener les opérations à la normale aussi rapidement que possible. Ce faisant, d'autres faiblesses et d'autres vulnérabilités peuvent être détectées, ce qui permet de les corriger et d'éviter ainsi une attaque ultérieure.

Mettre en œuvre des processus continus pour détecter les anomalies de comportement des utilisateurs, des postes clients et des applications.

Pour réduire au maximum l'impact sur l'activité, le temps qui s'écoule entre une violation et sa découverte est un facteur prépondérant dans le coût global de l'incident.

La surveillance, la visibilité du poste client et les technologies qui permettent d'automatiser la détection et l'investigation peuvent réduire

grandement ce temps.

La détection dans les profils des utilisateurs, dans les applications, et les appareils, de comportements anormaux ou malveillants symptomatiques de la présence d'un pirate dans les systèmes est cruciale.

La gestion des cyber-risques requiert une gestion globale et collaborative.

De nombreuses entreprises distinguent la sécurité physique de la sécurité informatique, l'informatique des opérations, la gestion de la poursuite d'activité de la protection des données, la sécurité interne de la sécurité externe. Dans l'ère numérique, ces divisions sont obsolètes. L'éparpillement des responsabilités peut faire courir des risques à toute l'entreprise. Les redondances doivent être limitées, et les réponses doivent être plus rapides pour augmenter la résilience globale.

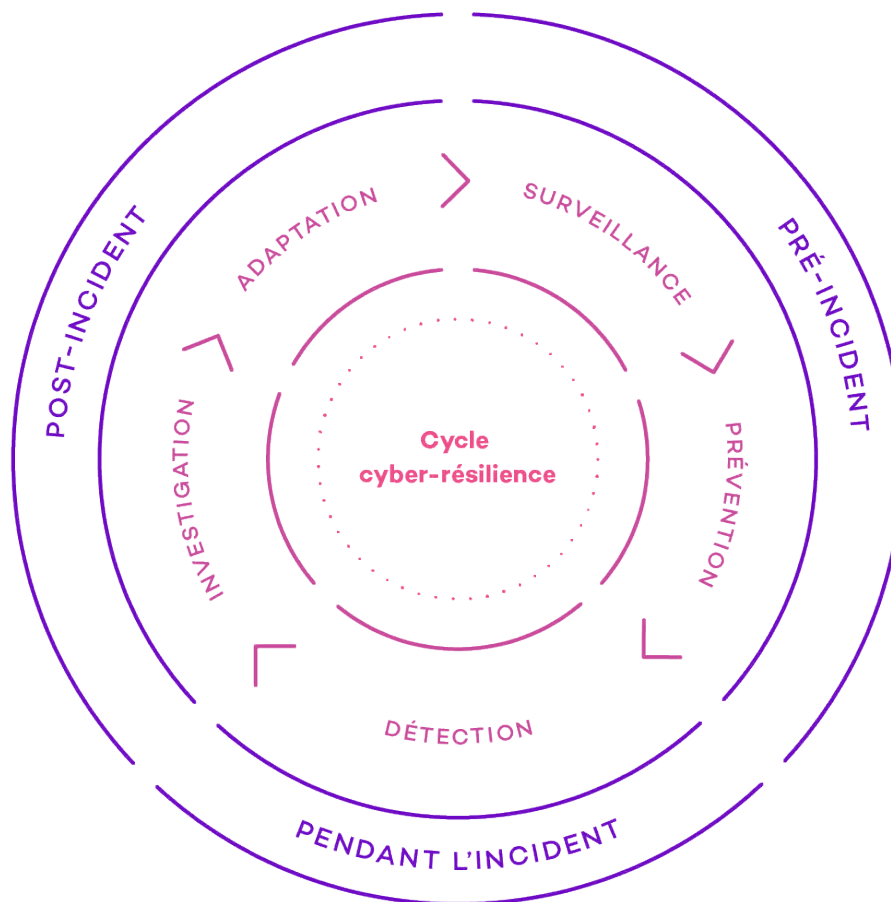


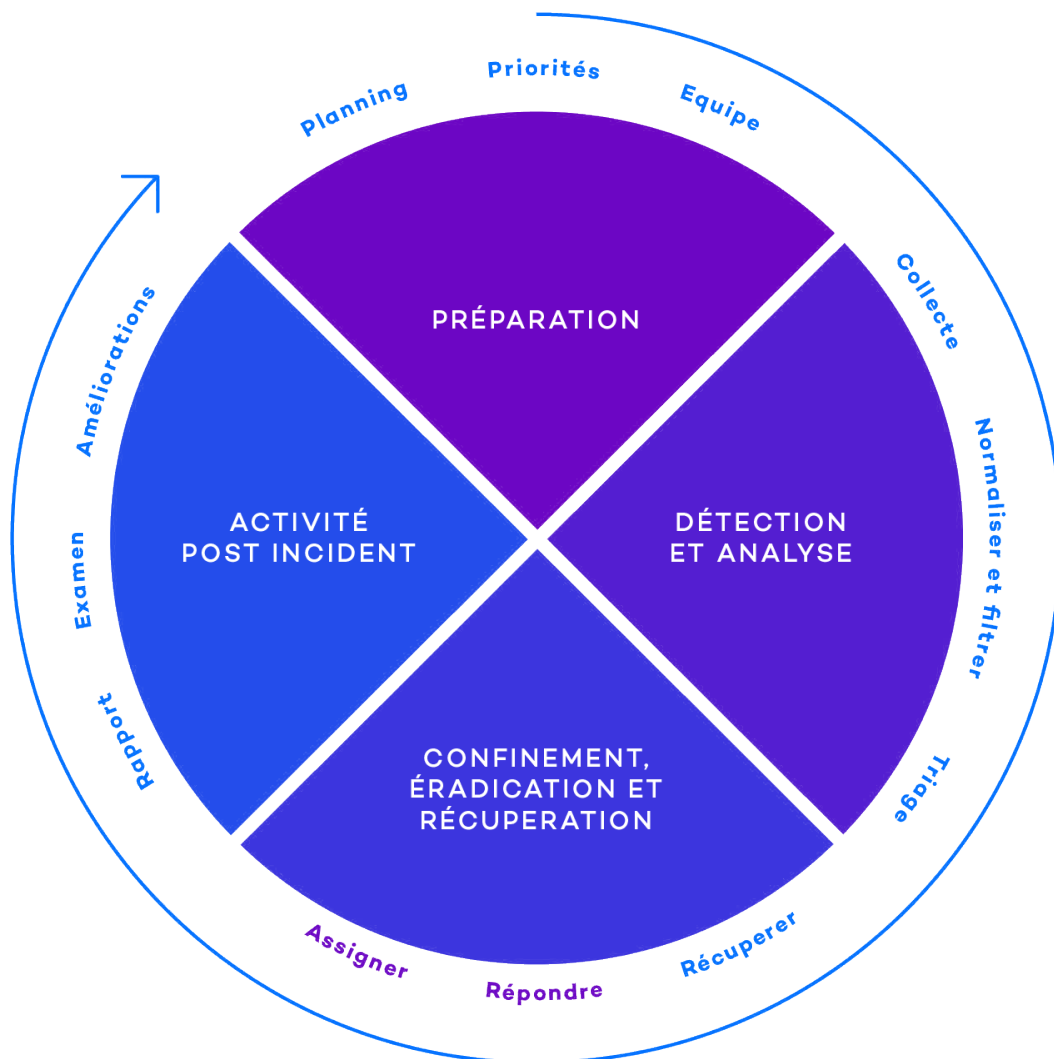
Figure 6. Le cycle d'amélioration continue de la cyber-résilience que chaque entreprise devrait développer et mettre en œuvre.

La figure suivante est tirée du rapport Gartner du 28 janvier 2018 : « Improve Operational Resilience Through to More Collaborative Incident Response Process ». Elle montre les secteurs du cycle de gestion et de réponse aux incidents où la collaboration et la coordination sont nécessaires — les cases bleues — et les fonctions où les capacités propres à chaque département, opérations et sécurité, s'appliquent — les cases violettes — L'objectif est de détecter les

incidents et d'y répondre dans le temps le plus court possible, tout en identifiant les zones d'amélioration:

Les entreprises qui adhèrent à ces principes ont tendance à mieux résister aux attaques que celles qui n'y adhèrent pas.

Gestion des incidents



Légende : ● Tâches et pratiques similaires
 ● Tâches et pratiques divergentes

Figure 7. Coordination entre les équipes des opérations et de la sécurité lors de la gestion d'un incident de sécurité. Gartner : « Improve Operational Resilience Through to More Collaborative Incident Response Process ». 25 janvier 2018. Analystes : Matthew T. Stamper, Kenneth Gonzalez

Les caractéristiques des entreprises cyber-résilientes

Pour l'étude sur la résilience d'IBM et du Ponemon Institute, « The Third Annual Study on the Cyber Resilient Organization »¹³, menée cette année, les caractéristiques des entreprises qui présentent un niveau élevé de cyber-résilience ont été identifiées.

On recommande aux entreprises d'évaluer leur situation au regard de ces caractéristiques et de prendre les mesures appropriées pour réduire l'écart entre leur situation actuelle et la situation idéale. Ces mesures sont diverses, en nature aussi bien qu'en nombre. L'adoption des technologies, des solutions et des services appropriés proposés par les éditeurs de sécurité et les fournisseurs de services peut permettre aux entreprises de démarrer immédiatement sans un investissement initial important. Cela s'avère payant à court terme du fait de la réduction importante des coûts d'exploitation occasionnés par les incidents et les violations de données.

Les entreprises qui présentent un haut niveau de cyber-résilience ont les caractéristiques suivantes :

Elle dispose d'un programme de cybersécurité avec des niveaux élevés de maturité, totalement ou au moins partiellement déployé dans toute l'entreprise et constamment amélioré.

Selon le rapport du SANS Institute « Behind the Curve? A maturity Model for Endpoint Security »¹⁴, lorsque le modèle de maturité se définit en termes de sécurité du poste client, une entreprise dans un état de forte maturité est capable d'empêcher les cyberattaques avant qu'elles puissent s'exécuter. Ou bien apporter des changements aux systèmes qui affectent le poste client, détecter les attaques qui ont été capables de contourner les solutions de sécurité déployées, communiquer l'état de l'incident, et empêcher la propagation de nouvelles attaques dans l'entreprise. En résumé, l'entreprise a déployé un programme de sécurité reposant sur une défense proactive, en améliorant grandement sa résilience globale.

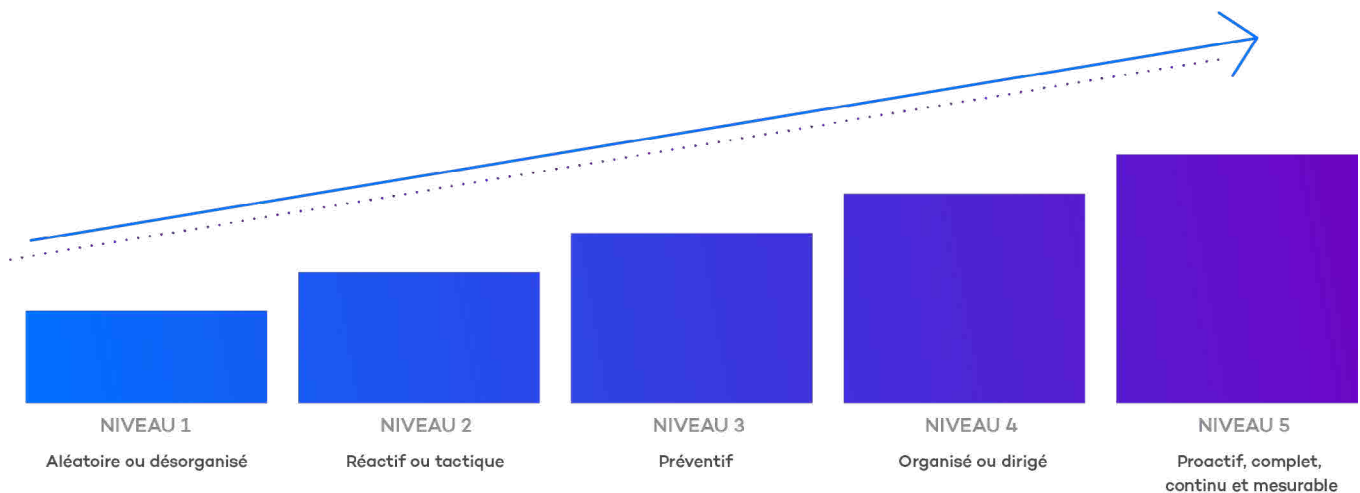


Figure 8. Modèle de maturité de la sécurité sur les postes de travail et les serveurs selon le SANS Institute, avec une définition des cinq niveaux de maturité par rapport au programme de sécurité développé et mis en œuvre.

¹³ <http://info.resilientsystems.com/2018-ponemon-cyber-resilient-organization-study>

¹⁴ <http://info.resilientsystems.com/2018-ponemon-cyber-resilient-organization-study>

Les entreprises à forte cyber-résilience ont développé des capacités importantes de prévention, de détection, de confinement et de récupération en cas de cyberattaque.

Comme décrit par l'étude du Ponemon Institute sur la résilience, les entreprises les plus résilientes sont celles qui ont investi dans le développement de capacités de prévention, de détection et de réponse.

Figure 22. Entreprises confiantes dans la prévention, la détection, le confinement et la réponse à une cyberattaque

1 = faible capacité à 10 = forte capacité, réponses 7 ou plus

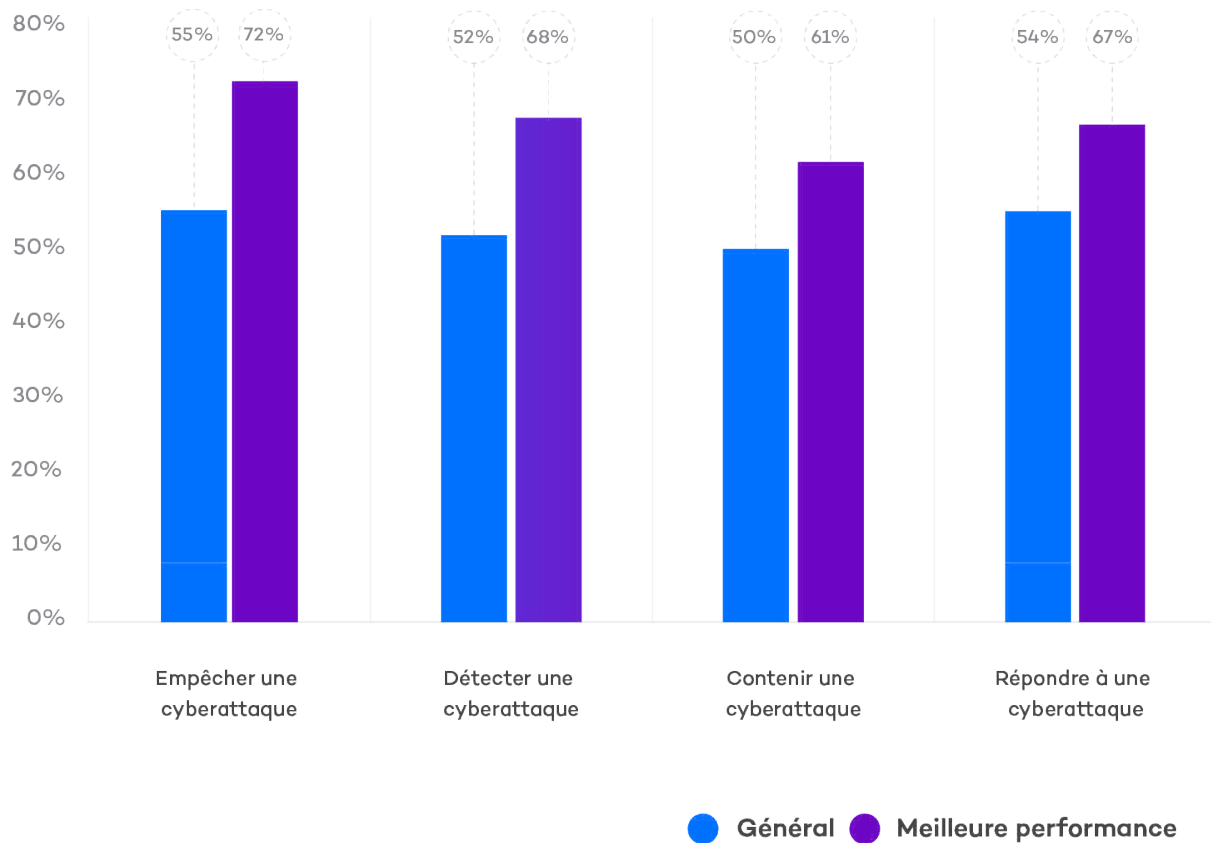


Figure 9. Ponemon Institute : relation entre la cyber-résilience et la capacité de prévention, de détection, de confinement et de réponse.

Les entreprises fortement cyber-résilientes ont développé un plan de réponse aux incidents de cybersécurité (Cybersecurity Incidents Response Plan, CSIRP). Ce plan repose sur la surveillance continue et la corrélation des événements grâce

aux données collectées par des capteurs sur les appareils réseau et/ou les postes clients, ainsi que sur des mécanismes de détection, d'investigation et de réponse automatisée et/ou gérée par des experts en sécurité, ou de traque des menaces.

Qu'est-ce qui décrit le mieux votre plan de réponse aux incidents de cybersécurité (CSIRP) ?

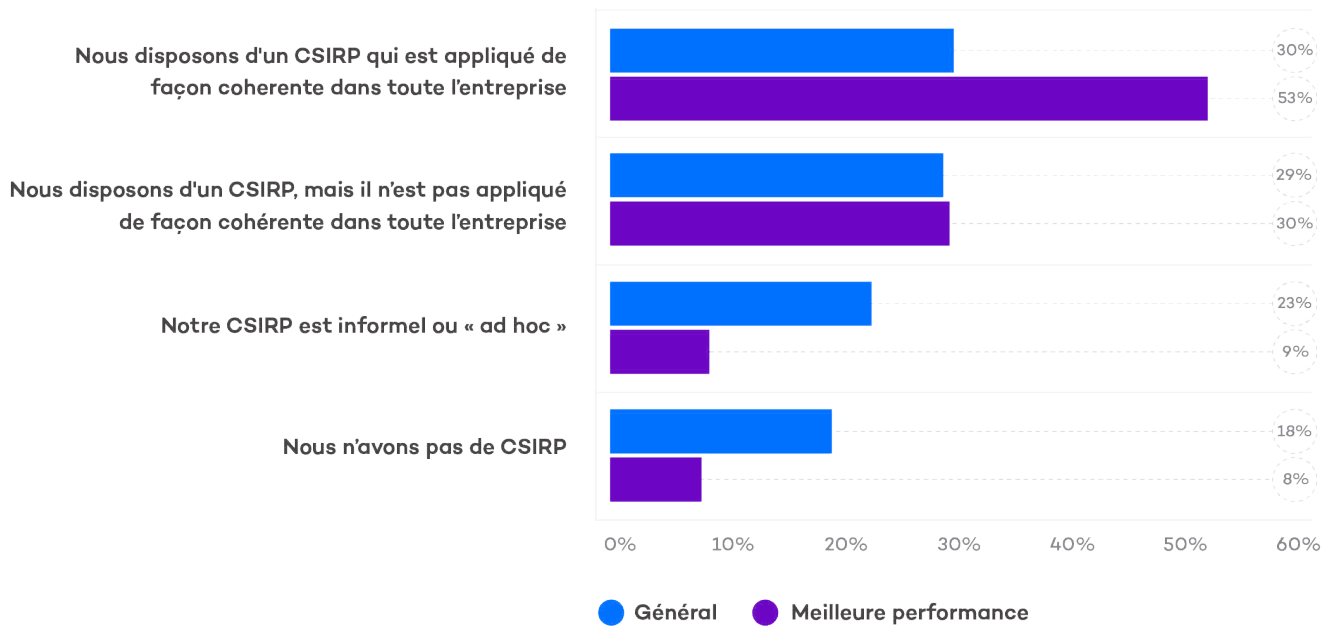


Figure 10. Ponemon Institute: relationship between cyber-resilience and the implementation of a response plan for cybersecurity incidents.

En outre, la plupart des entreprises qui présentent un haut niveau de cyber-résilience considèrent qu'il est essentiel d'avoir, au sein de l'équipe de sécurité

interne ou par le biais d'un prestataire externe, un personnel hautement qualifié en cybersécurité dans le cadre du plan de réponse aux incidents.

Il est important d'avoir des professionnels compétents en cybersécurité dans son CSIRP

1 = faible capacité à 10 = forte capacité, réponses 7 ou plus

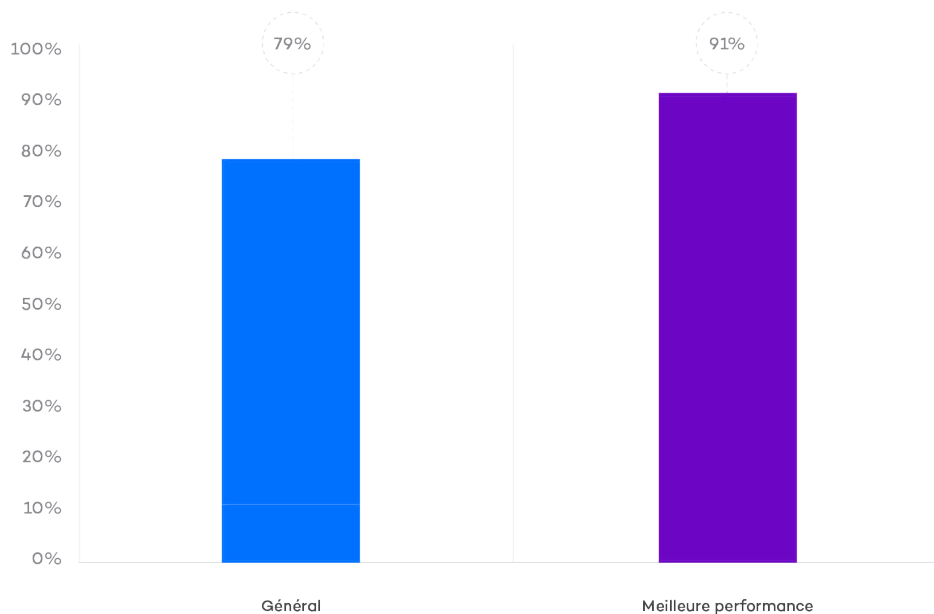


Figure 11. Ponemon Institute: relation entre la cyber-résilience et la nécessité d'avoir des ressources spécialisées hautement qualifiées, dédiées à la cybersécurité

Gouvernance d'entreprise cyber-résiliente:

Les dirigeants des entreprises fortement cyber-résilientes sont sensibles à la relation entre ce facteur et la croissance économique, ainsi qu'au renforcement de la marque et de la réputation de leur entreprise.

Sensibilisation de la direction à l'impact positif de la cyber-résilience sur l'entreprise

Sensibilisation de la direction à l'impact positif de la cyber-résilience sur l'entreprise

Réponses D'accord et Entièrement d'accord

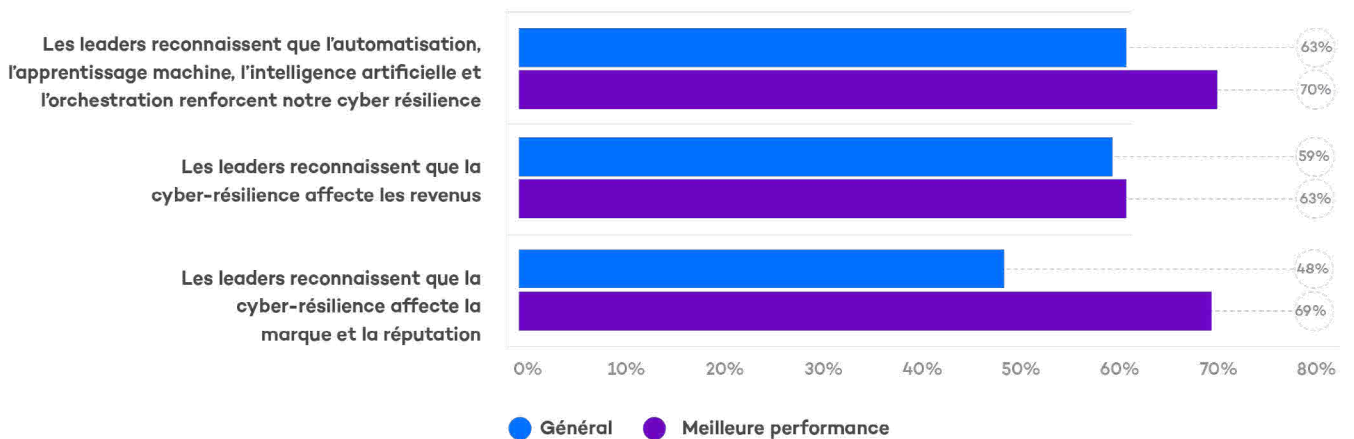


Figure 12. Ponemon Institute : l'importance de l'implication de la direction dans l'instauration d'un niveau élevé de cyber-résilience dans les entreprises.

Conclusions

La transformation numérique qui s'opère dans tous les aspects de nos existences prend une importance particulière avec l'évolution des entreprises, des organisations et des administrations, des appareils interconnectés, des applications, des outils et des processus de production.

Face à la concurrence, la recherche de l'optimisation au moyen d'instruments, de méthodes, de capacités et de processus nouveaux ou améliorés est à l'origine de pratiquement toutes les initiatives dans le secteur privé et le secteur public.

Il y a toutefois un aspect que nous ne pouvons pas ignorer dans cette transformation numérique : la nécessité de s'investir fortement dans la gestion de la sécurité et du risque professionnel.

L'investissement doit être d'autant plus important que le nombre et la sophistication des menaces évoluent. Le cybercrime est une activité attrayante et très lucrative. Les pirates disposent de ressources plus nombreuses et de meilleure qualité, à la fois au niveau technique et au niveau économique. Ces ressources leur permettent de développer des attaques de plus en plus sophistiquées, ce qui aboutit à des menaces plus complexes, plus dynamiques et plus nombreuses.

[Equifax](#), [CCleaner](#), [WPA2](#), [Vault7](#), la CIA, [KRACK](#), la NSA, [WannaCry](#), [Goldeneye/NotPetya](#), [Meltdown/Specter](#), [les piratages d'élections...](#) Ce sont là quelques exemples récents d'infections massives, de vols, de fuites de données personnelles, d'attaques par logiciels de rançon, de piratages d'applications pour lancer des attaques contre un pays entier ou contre des grandes entreprises ciblées, et de vulnérabilités affectant des milliards d'appareils.

Avec des cas réels comme ceux-ci, il n'y a rien d'étonnant à ce que 75 % des entreprises (selon une étude récente de McKinsey¹⁵) considèrent que la

cybersécurité est une priorité pour le développement de leurs activités. La « situation de stress » décrite plus haut nécessite une réaction qui implique toute l'entreprise dans le programme de sécurité, qui développe et renforce une attitude professionnelle de cyber-résilience.

La **cyber-résilience** est la capacité d'une entreprise à maintenir ses objectifs fondamentaux et son intégrité face à la menace latente d'attaques de cybersécurité.

Une entreprise cyber-résiliente est capable de prévenir, détecter, confiner et récupérer, en réduisant au maximum le temps d'exposition et l'impact sur l'activité, face aux innombrables menaces graves contre les données, les informations, les applications et l'infrastructure informatique. Cela concerne particulièrement les appareils, là où résident les actifs les plus précieux de l'entreprise. Cibler les appareils revient aussi à s'attaquer à l'intégrité des identités et des utilisateurs.

Pour parvenir à la cyber-résilience, la nouvelle approche de la sécurité doit traiter au moins les points suivants :

1. Gérer la cybersécurité comme un problème de gestion du risque d'entreprise, non comme un problème informatique, **et adopter un « cycle de résilience »**. Les éléments clés du cycle de cyber-résilience sont :

1. Donner la priorité aux actifs les plus précieux de l'entreprise.
2. Connaître, comprendre et donner la priorité aux menaces et aux adversaires les plus importants de l'entreprise.
3. Connaître et mettre en œuvre les meilleures défenses contre les menaces actuelles et potentielles.
4. Être prêt pour le cas où des adversaires

¹⁵ <https://www.mckinsey.com/business-functions/risk/our-insights/a-new-posture-for-cybersecurity-in-a-networked-world>

parviendraient à contourner toutes les technologies de sécurité, et les détecter, les confiner et remédier à leurs actions aussi rapidement que possible pour minimiser les dommages pour l'entreprise.

5. Adopter une position de crise qui recherche activement et continuellement les menaces, et détecter les points vulnérables susceptibles d'être utilisés par des acteurs de menaces afin de réduire la surface d'attaque.

6. Gérer au niveau de l'entreprise toutes les communications au sujet d'une compromission.

7. Définir et mettre constamment en œuvre de nouvelles initiatives pour minimiser les risques et relancer le cycle de l'amélioration en continue de la gestion de la sécurité d'entreprise.

2. Renforcer les quatre piliers clés : prévention, détection, traque des menaces, et confinement, réponse & réduction de la surface d'attaque.

3. S'adapter continuellement aux nouvelles techniques et tactiques des pirates et autres

attaquants. Être résilient implique que cette adaptation s'effectue dans un temps minimum, à la vitesse maximum, voire même en temps réel.

4. Prioriser et réduire les risques à tous les niveaux de l'entreprise. Les entreprises doivent se doter d'outils, de produits et de services gérés qui automatisent les fonctions de profilage, de classification et de surveillance de l'activité (humaine, des données et de l'infrastructure). Un apprentissage constant est également nécessaire, pour des systèmes de sécurité prédictifs qui accélèrent la prévention et/ou la détection précoce des adversaires en réduisant le risque organisationnel sans coûts disproportionnés, notamment d'exploitation.

5. Gérer le cyber-risque avec une approche globale et collaborative.

Il est interdit de dupliquer, de reproduire, d'enregistrer sur un système de stockage ou de retransmettre ce rapport, en totalité ou en partie, sans une autorisation écrite préalable de Panda Security.

© Panda Security 2017. Tous droits réservés.

Plus d'information sur:

<https://www.pandasecurity.com/france/business/>

ou en appelant:

0800 368 9158

ou par email à

pbp@fr.pandasecurity.com

#PASS2018