Kaspersky for Business

KASPERSKY lab

Faire évoluer les budgets de sécurité informatique pour protéger les initiatives de transformation numérique

Kaspersky Lab

Table des matières

Introduction

C'est une période difficile pour les entreprises. Nous vivons dans une nouvelle ère du consommateur « pressé », où les clients exigent des résultats immédiats, où la concurrence se déplace plus vite que jamais auparavant et où 70 % des consommateurs s'accordent à dire que la technologie leur permet de changer de fournisseur facilement.

47 %

des PDG

sont mis au défi par leur conseil d'administration de passer au numérique

Dans ce contexte, de multiples entreprises se lancent dans des stratégies de transformation numérique. En effet, **Gartner a constaté que près de la moitié (47 %) des PDG** sont mis au défi par leur conseil d'administration de se transformer numériquement pour améliorer leurs perspectives de croissance et leurs relations avec la clientèle. Beaucoup, par exemple, déplacent un nombre croissant de leurs plates-formes et de leurs données vers le cloud, ce qui leur permet d'évoluer ou de répondre aux tendances du marché selon les besoins et avec l'agilité nécessaire pour tenir leurs concurrents à distance.

En effet, ces données constituent aujourd'hui la pierre angulaire de la transformation numérique. Les initiatives axées sur les données ont pris de l'ampleur pour jouer un rôle de premier plan dans les organisations de toutes tailles, fournissant aux chefs d'entreprise les connaissances nécessaires pour exécuter avec succès leurs stratégies à court et à long terme.

À mesure que les entreprises se transforment numériquement, les considérations de cybersécurité doivent de plus en plus jouer un rôle stratégique dans les affaires, ce qui se reflète dans les débats actuels autour des structures de rapport du RSSI et le besoin souvent cité de donner une place à la sécurité de l'information lors des conseils d'administration.

Les raisons de prendre la cybersécurité au sérieux dans les entreprises sont claires : à mesure que celles-ci deviennent de plus en plus dépendantes des plates-formes numériques, elles ne peuvent tout simplement pas se permettre que ces plates-formes leur fassent défaut. Et c'est là que réside le problème : le monde des risques de sécurité informatique est en constante évolution. De nouvelles menaces émergent chaque jour et au fur et à mesure que les infrastructures des entreprises s'adaptent, de nouvelles vulnérabilités se forment.

Comprendre les complexités et les pressions de la sécurité informatique est notre mission, afin que les entreprises puissent aider à protéger ce qui compte le plus pour elles. Cette étude, qui poursuit notre recherche annuelle sur l'économie de la sécurité informatique, complète les données des années précédentes pour déterminer comment les organisations réagissent aux changements dans le paysage des menaces et pour comprendre les habitudes de dépenses en sécurité informatique qui pourraient être à l'origine de la création ou du démantèlement d'entreprises partout dans le monde. Voici un aperçu de nos conclusions.

Les attaques sont de plus en plus sophistiquées et dévastatrices

La mauvaise nouvelle pour les entreprises de toutes les industries, c'est que l'impact financier des cyberattaques et les coûts de récupération qui en découlent ne cessent d'augmenter. **Pour les entreprises, le coût moyen d'une violation de données est maintenant d'un peu plus de 1,2 million de dollars, soit une augmentation de 24 % par rapport à 2017 et de 38 % par rapport à 2016. Il en va de même pour les PME. L'impact financier d'une violation de données a augmenté de 37 % au cours des 12 derniers mois, passant de 88 000 $ en 2017 à 120 000 $ en 2018.**

L'amélioration des logiciels et de l'infrastructure est maintenant la conséquence la plus coûteuse d'une violation de sécurité pour les entreprises et les PME. Cela montre à quel point les diverses épidémies de ransomwares, les exploits dévastateurs et les attaques contre les chaînes d'approvisionnement au cours des 12 derniers mois ont endommagé l'infrastructure des entreprises, brossant un portrait de l'ampleur du travail nécessaire pour renouveler ces systèmes et les rendre plus durables en réponse à une attaque.

Pour les entreprises du monde entier, l'amélioration de l'infrastructure après une violation coûte 193 000 $ en moyenne, soit une augmentation de plus de 46 % par rapport aux **132 000 $** qu'il leur en coûtait en 2017. En effet, ce chiffre est le plus élevé pour les entreprises de tous les pays, à l'exception de l'Amérique latine, ce qui montre que la majorité des entreprises sont dans le même bateau lorsqu'il s'agit des implications financières d'une violation de données. Notre étude met également l'accent sur la façon dont les incidents de cybersécurité peuvent nuire directement à leur façon de fonctionner, les dommages aux cotes de crédit et aux primes d'assurance (**180 000 $**) et les pertes d'affaires (**131 000 $**) faisant partie des cinq conséquences les plus coûteuses d'une violation de données.

Des sommes importantes sont également consacrées à l'amélioration du niveau de connaissances et d'expertise auxquelles les entreprises ont accès, par la formation de leurs salariés (**137 000 $**), l'embauche de professionnels externes (**126 000 $**) ou l'embauche de nouveaux salariés (**106 000 $**). Le défi pour toutes les entreprises est que la pénurie continue de compétences à l'échelle de l'industrie rend de plus en plus difficile de trouver les bons talents à un prix abordable. C'est probablement la raison pour laquelle les entreprises se concentrent beaucoup plus sur la formation de leur personnel actuel que sur le recrutement.

Les stratégies de transformation numérique en péril

Les résultats de cette année ont montré que les incidents les plus coûteux sont liés à l'infrastructure dans le cloud. Ce qui est évident, c'est que le cloud en plein essor et les tendances mobiles représentent de nombreuses opportunités pour les cybercriminels. Elles exposent également les entreprises aux risques liés à l'erreur humaine, tandis que la nature distribuée de l'infrastructure dans le cloud présente des complexités de gestion. L'utilisation des plates-formes de cloud computing est en hausse depuis un certain temps, tant au sein des entreprises que des PME, ce qui, bien qu'offrant de multiples avantages aux entreprises, met également en danger les données de celles-ci.

Si l'on examine les trois principaux types de menaces les plus coûteuses, les incidents de sécurité affectant l'infrastructure informatique hébergée par un tiers ont eu le plus grand impact pour les PME (**118 000 $**) et le deuxième impact financier le plus important pour les entreprises (**1,11 million de dollars**). Les incidents affectant les services cloud de tiers que l'entreprise utilise ont également un impact financier important sur les PME (**89 000 $**), ce qui signifie que les stratégies de transformation numérique des entreprises (et l'adoption du cloud dans ce contexte) peuvent être menacées par des incidents informatiques si les entreprises ne parviennent pas à trouver un moyen d'atténuer les risques.

Une sécurité de plus en plus stratégique

du budget informatique
est alloué
à la cybersécurité

Pour lutter contre ces menaces, la sécurité prend de plus en plus d'importance pour les entreprises. Les organisations commencent à ressentir l'impact réel de la cybersécurité sur leurs activités. Les résultats de l'étude montrent que les craintes du coût d'un incident **obligent les chefs d'entreprise à accorder une plus grande part du budget informatique (23 %) et plus d'attention lors des réunions du conseil d'administration qu'au cours des années précédentes**.

Les entreprises s'attendent à ce que leurs budgets de sécurité informatique augmentent de 15 % au cours des trois prochaines années. Il en va de même pour les TPE : cela représente un investissement important pour les entreprises de moins de 50 salariés, dont les ressources sont souvent insuffisantes, alors que les PME s'attendent à une croissance de 14 % de leurs dépenses en cybersécurité d'ici 2021. Les entreprises de la région META, quant à elles, s'attendent à ce que leurs budgets de sécurité informatique augmentent de près d'un cinquième (19 %) au cours des trois prochaines années, contrairement aux entreprises du Japon (12 %) et de l'Amérique du Nord (11 %) à l'autre bout de l'échelle.

L'une des raisons possibles est que les contrôles réglementaires croissants, par exemple l'introduction de la législation du RGPD dans l'UE, ont probablement un impact sur l'importance accordée à la sécurité informatique ; la législation tiendra les entreprises responsables de la protection des données personnelles des clients et promet des amendes strictes en cas d'infraction. Il est donc quelque peu surprenant que les entreprises européennes s'attendent à ce que leurs budgets de sécurité informatique n'augmentent que de 13 % au cours des trois prochaines années, ce qui est faible par rapport à d'autres régions.

Non seulement ces résultats mettent en évidence les coûts croissants associés à la défense contre les cyberattaques, mais ils illustrent également la valeur et l'importance que les chefs d'entreprise accordent à la protection de leur entreprise contre les menaces les plus récentes ; il y a une volonté de sécurité informatique à tous les niveaux.

En effet, l'implication de la direction dans le débat sur la cybersécurité est un signe certain que la sécurité est de plus en plus intégrée dans la stratégie des entreprises. Une chose ressort clairement de notre étude : il est plus important que jamais de réagir aux incidents de sécurité et aux violations de données et de s'en remettre. Lisez ce qui suit pour en savoir plus.

Méthodologie

L'étude de Kaspersky Lab sur les risques liés à la sécurité informatique pour les entreprises est une enquête mondiale menée chaque année auprès des décideurs informatiques depuis 2011. **Au total, 6 614 répondants de 29 pays ont été interrogés sur les dépenses de leur entreprise en matière de sécurité informatique, les types de menaces auxquelles ils ont été confrontés et les coûts de récupération après une attaque.** Les régions couvertes sont l'Amérique latine, l'Europe, l'Amérique du Nord, l'Asie-Pacifique et la Chine, le Japon, la Russie et la région META (Moyen-Orient, Turquie et Afrique).

Tout au long du rapport, les entreprises seront désignées en fonction de leur taille : TPE (très petites entreprises, moins de 50 salariés), PME (petites et moyennes entreprises, de 50 à 999 salariés) et grandes entreprises (entreprises de plus de 1 000 salariés). Tous les résultats de l'enquête ne sont pas inclus dans ce rapport.

Principales conclusions

Le coût des violations de données a grimpé de plus d'un cinquième pour les grandes entreprises et les PME. L'incidence financière moyenne d'une violation de données s'élève maintenant à **1,23 million de dollars** pour les grandes entreprises, soit une augmentation de 24 % par rapport à **992 000 $** en 2017. Il en va de même pour les PME, les coûts passant de **88 000 $** l'an dernier à **120 000 $** en 2018, soit une augmentation de 37 %.

Les entreprises de l'Asie-Pacifique, du Japon et de l'Amérique du Nord connaissent les coûts de récupération les plus élevés. C'est au Japon **(1,7 million de dollars)** qu'une violation de données coûte le plus cher aux grandes entreprises, suivi de l'Amérique du Nord **(1,6 million de dollars)** et de l'Asie-Pacifique **(1,5 million de dollars)**. L'Amérique du Nord arrive en tête pour les PME **(149 000 $)**. Pour les entreprises et les PME, l'incidence financière moyenne d'une violation de données est la plus faible pour les entreprises basées en Russie, soit **246 000 $** et **74 000 $** respectivement.

Les budgets de sécurité moyens ont augmenté pour toutes les tailles d'entreprises. Les entreprises dépensent maintenant en moyenne **8,9 millions de dollars** pour la cybersécurité, tandis que les budgets de sécurité des PME sont passés de **201 000 $** en 2017 à **246 000 %** en 2018. L'augmentation a été la plus importante pour les TPE, les budgets de sécurité moyens étant passés de **2 400 $** à **3 900 $** au cours des 12 derniers mois, ce qui prouve que même les plus petites entreprises prennent maintenant la sécurité informatique au sérieux.

Les menaces les plus coûteuses sont liées au fait que les données quittent les locaux de l'entreprise. Les incidents affectant l'infrastructure informatique hébergée par un tiers est l'une des menaces les plus coûteuses pour les entreprises **(1,09 million de dollars)** et les PME **(118 000 $)**, suivis de près par le partage inapproprié de données par les appareils mobiles et les incidents affectant les services cloud de tiers.

La complexité de l'infrastructure et le manque de connaissances motivent les investissements dans la sécurité informatique. Plus d'un tiers des entreprises citent la complexité accrue de leur infrastructure informatique (34 %) et la nécessité d'améliorer le niveau d'expertise des spécialistes de la sécurité (34 %) comme motivations pour investir dans la cybersécurité.

Le coût moyen des violations de données

Les entreprises, grandes et petites, doivent maintenant tenir compte d'un éventail de facteurs de coûts à la suite d'une violation de données, allant des frais de personnel au paiement d'amendes et de compensations. Mais à quoi ressemble exactement une violation de données « typique » d'un point de vue financier ? Pour les grandes entreprises, le coût moyen d'une violation de données s'élève maintenant à plus de 1,23 million de dollars, contre 992 000 $ en 2017. Bien que les coûts les plus élevés proviennent de l'amélioration des logiciels et de l'infrastructure (193 000 $), des facteurs comme les dommages aux cotes de crédit et aux primes d'assurance (180 000 $) et la formation (137 000 $) ont également un impact majeur.

Il en va de même pour les PME : le coût moyen d'une violation de données est passé de 87 800 $ en 2017 à 120 000 $ en 2018. Les PME font face aux mêmes coûts que les grandes entreprises, l'emploi de professionnels externes, les dommages aux cotes de crédit et les pertes de contrats (15 000 $) ayant le plus grand impact, ce qui peut représenter une grande partie des revenus d'une PME.

Après d'importants incidents coûteux l'année dernière, il semble que les grandes entreprises investissent massivement dans l'amélioration de la protection et le renforcement de la couverture d'assurance

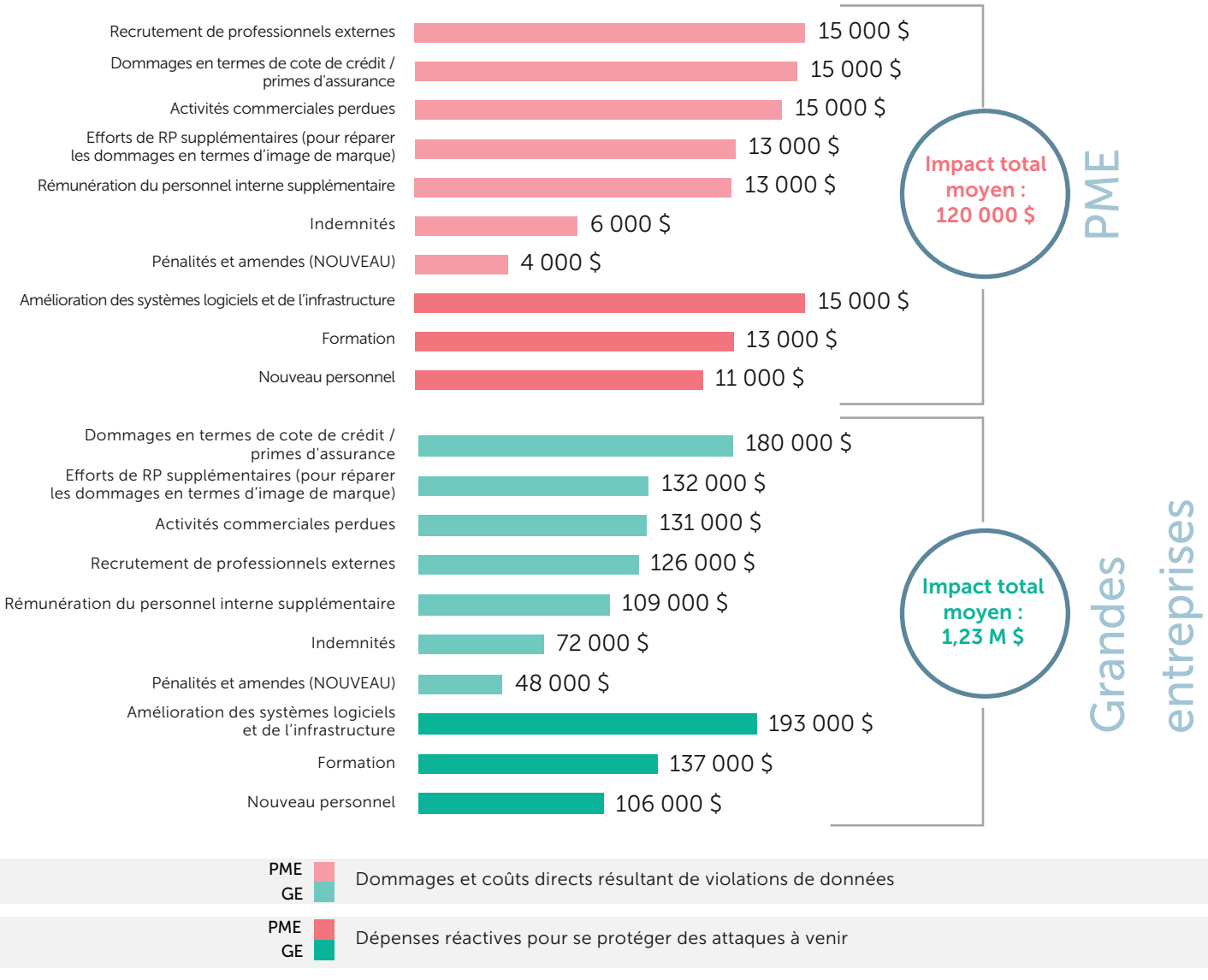


***Figure 1 :** impact financier moyen d'une violation de données dans le monde*

Il est intéressant de noter que les coûts associés à la récupération à la suite d'une violation de données varient considérablement d'une région à l'autre. Pour les PME, les coûts moyens ont augmenté dans les sept régions incluses dans l'étude, l'Amérique du Nord (149 000 $), l'Asie-Pacifique et la Chine (135 000 $) étant les plus chers et la Russie (74 000 $) étant les moins élevés.

Et il en va de même pour les grandes entreprises. Le coût moyen d'une violation de données s'élève maintenant à 1,7 million de dollars pour les grandes entreprises du Japon, 1,6 million de dollars en Amérique du Nord et 1,5 million de dollars dans l'Asie-Pacifique et en Chine. Comme pour les PME, les violations de données ont l'impact financier le plus faible pour les grandes entreprises en Russie (246 000 $), soit une augmentation de 6 000 $ depuis 2017.

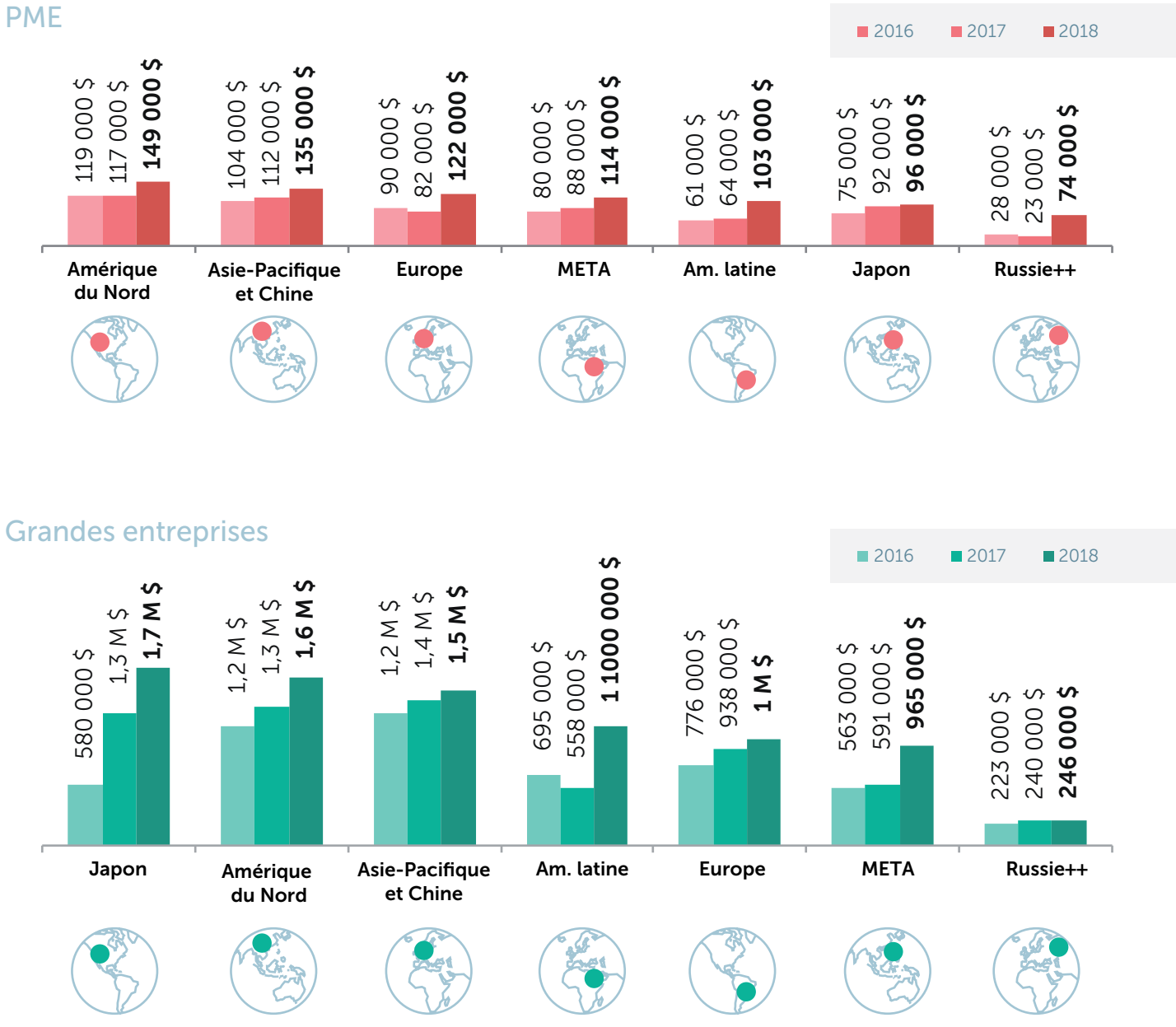


***Figure 2** : impact financier moyen d'une violation de données par région*

Quelle qu'en soit la raison, les coûts augmentent clairement à tous les niveaux, ce qui exerce de sérieuses pressions financières sur les entreprises, grandes et petites, et illustre pourquoi la sécurité devient un enjeu si important à mesure que les entreprises continuent de se transformer. Mais où tout cet argent supplémentaire est-il dépensé ?

Pourquoi les coûts augmentent-ils ?

Étant donné les coûts associés à une violation de données découlant d'un si grand nombre de domaines différents, il peut être difficile pour les entreprises de savoir exactement à quoi sert leur argent. Notre étude a révélé que l'apport d'améliorations techniques à la suite d'un incident entraîne maintenant un fardeau financier particulièrement lourd pour les grandes entreprises et les PME, ainsi que des dommages aux primes d'assurance et aux activités visant à améliorer l'expertise interne.

Pour les grandes entreprises, l'amélioration des logiciels et de l'infrastructure représente les coûts les plus élevés à la suite d'une violation de données, soit 193 000 $, suivie de près par les dommages aux cotes de crédit et aux primes d'assurance (180 000 $) et les investissements en formation (137 000 $). La tendance est similaire pour les PME, où quatre coûts différents se partagent la première place (les améliorations de l'infrastructure, l'embauche de professionnels externes, les dommages aux cotes de crédit et la perte d'activité) et coûtent en moyenne 15 000 $ aux PME.

11 000 $

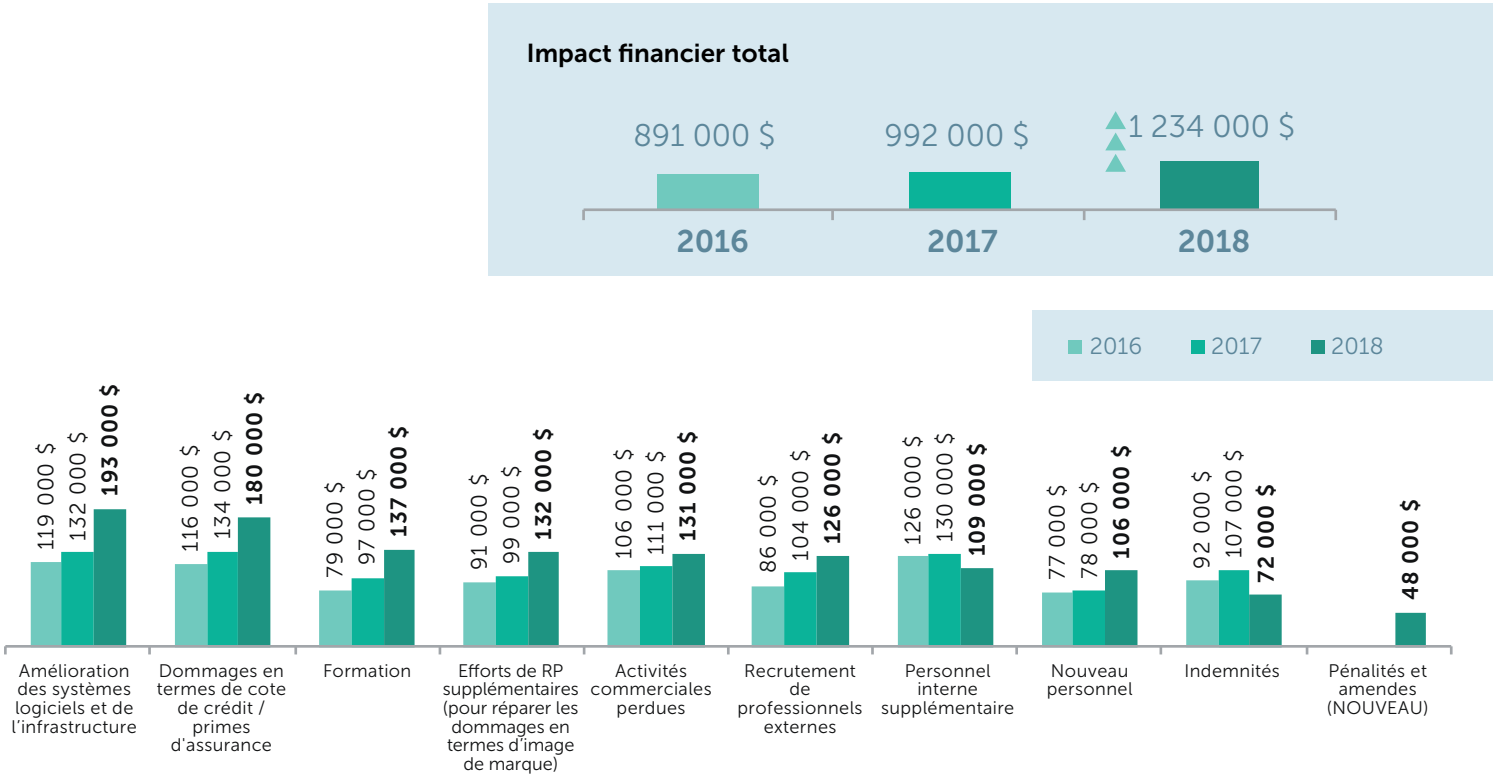


***Figure 1** : suivi de l'impact financier d'une violation de données pour les grandes entreprises*

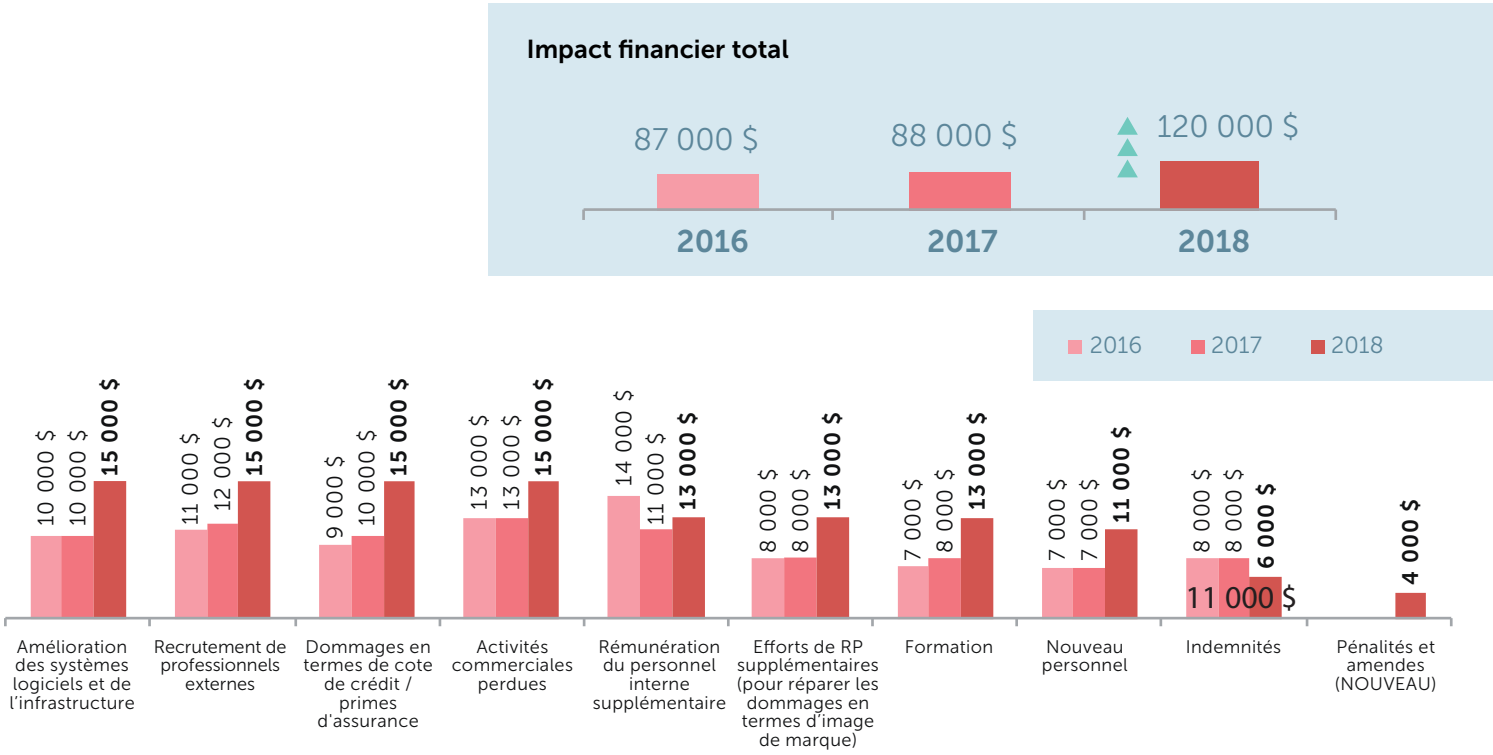


***Figure 2** : suivi de l'impact financier d'une violation de données pour les PME*

Il existe également des variations régionales intéressantes qui méritent d'être mentionnées. Par exemple, le recours à des professionnels externes est l'une des conséquences les plus coûteuses d'une violation de sécurité pour les PME en Amérique du Nord, en Amérique latine et en Europe, ce qui donne à penser que les entreprises de ces régions ont davantage besoin d'expertise supplémentaire.

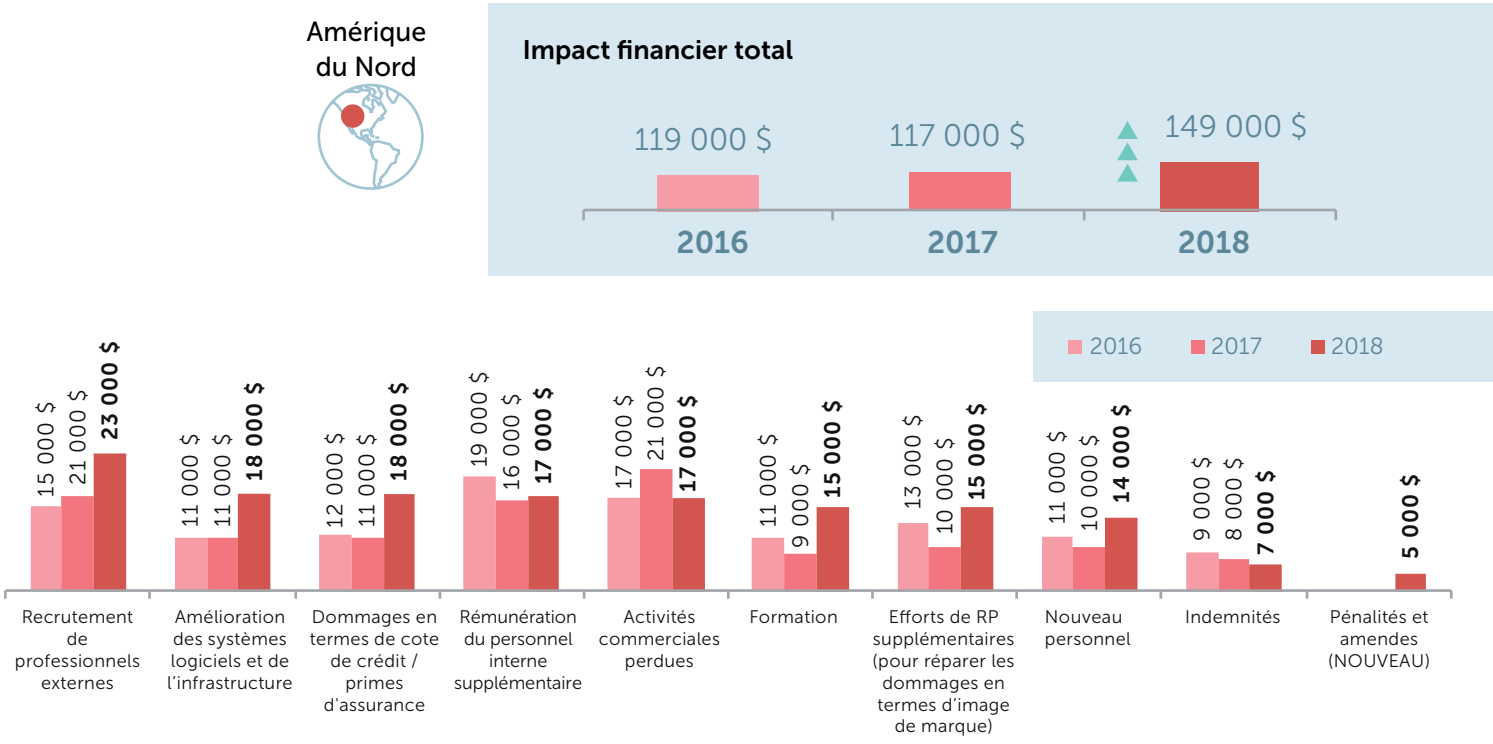


***Figure 3** : impact financier d'une violation de données pour les PME en Amérique du Nord*

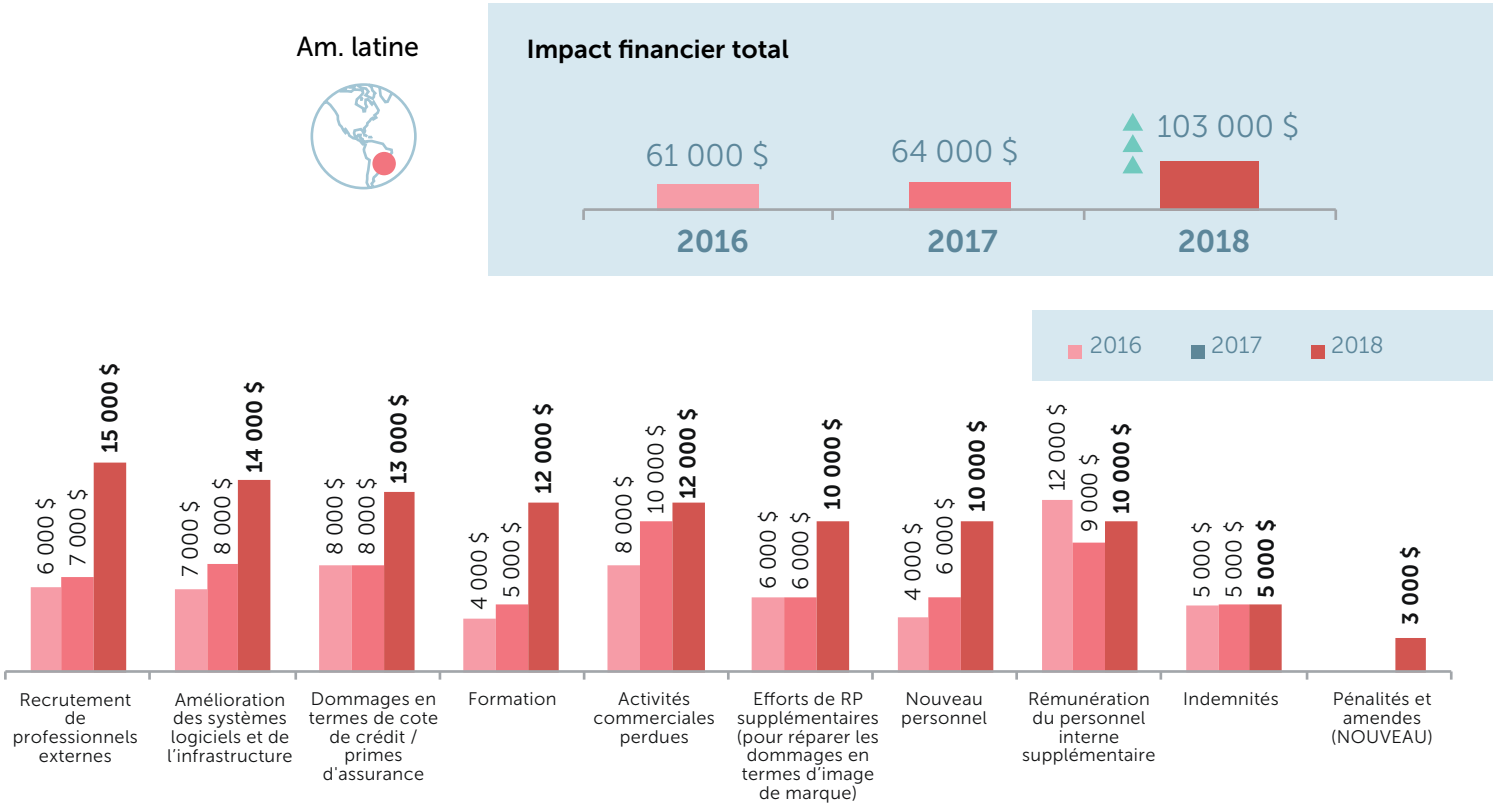


Figure 4 : impact financier d'une violation de données pour les PME en Amérique latine

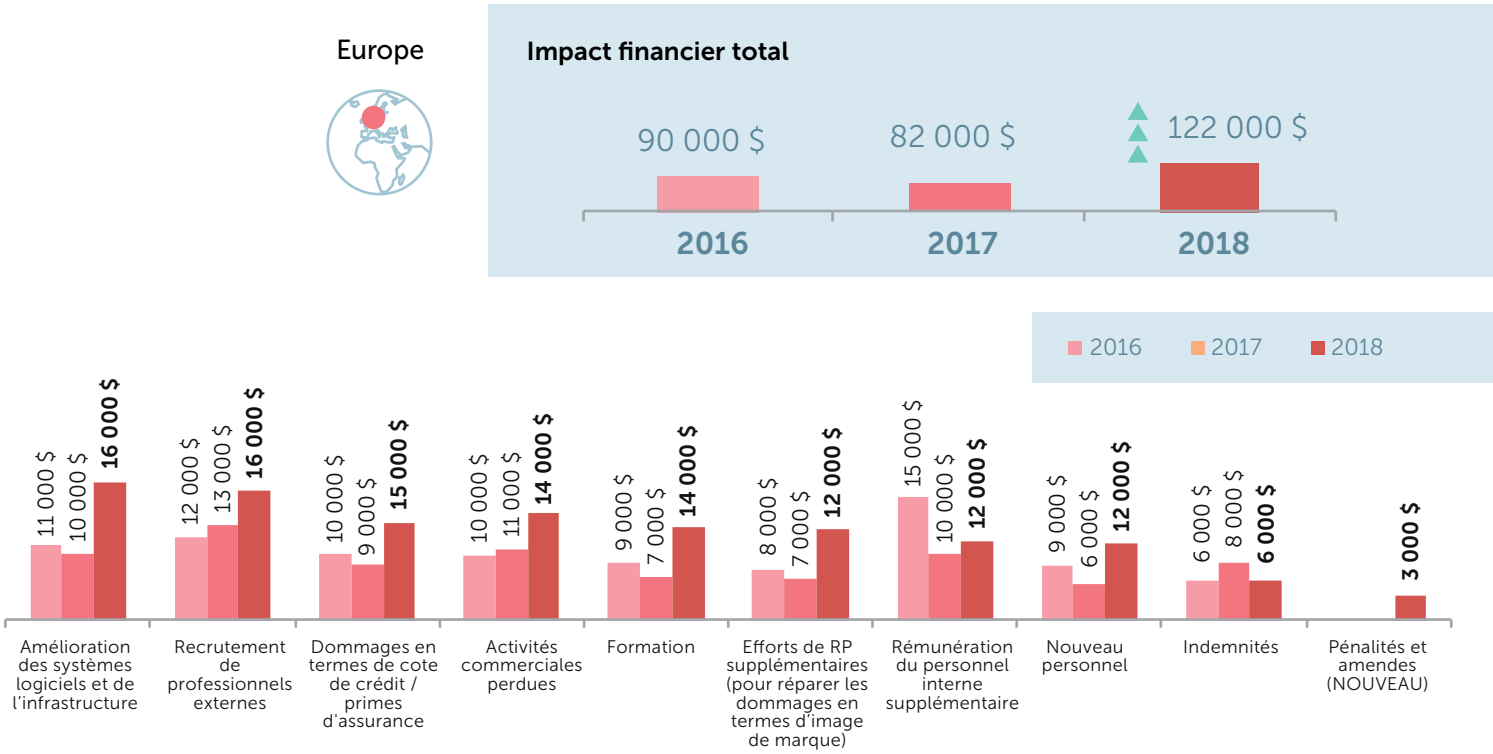


Figure 5 : impact financier d'une violation de données pour les PME en Europe

De plus, il y a certaines régions où la réduction ou la réparation des atteintes à la réputation est beaucoup plus prioritaire. Les relations publiques supplémentaires pour réparer les dommages causés à la marque se classent au deuxième rang des facteurs les plus coûteux pour les PME au Japon (13 000 $) et au troisième rang des facteurs les plus coûteux pour les entreprises de la région META (113 000 $) et les PME en Russie (8 000 $).

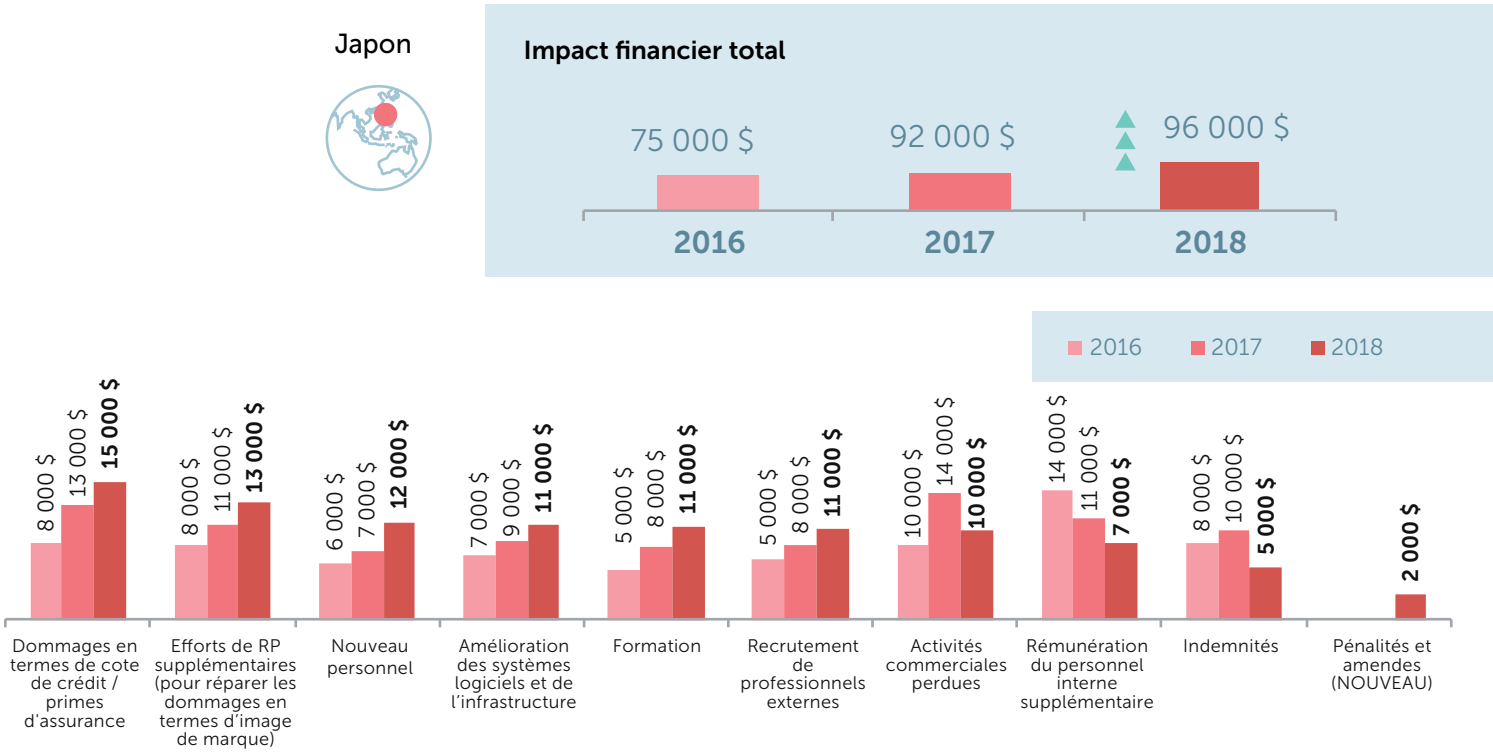


Figure 6 : impact financier d'une violation de données pour les PME au Japon

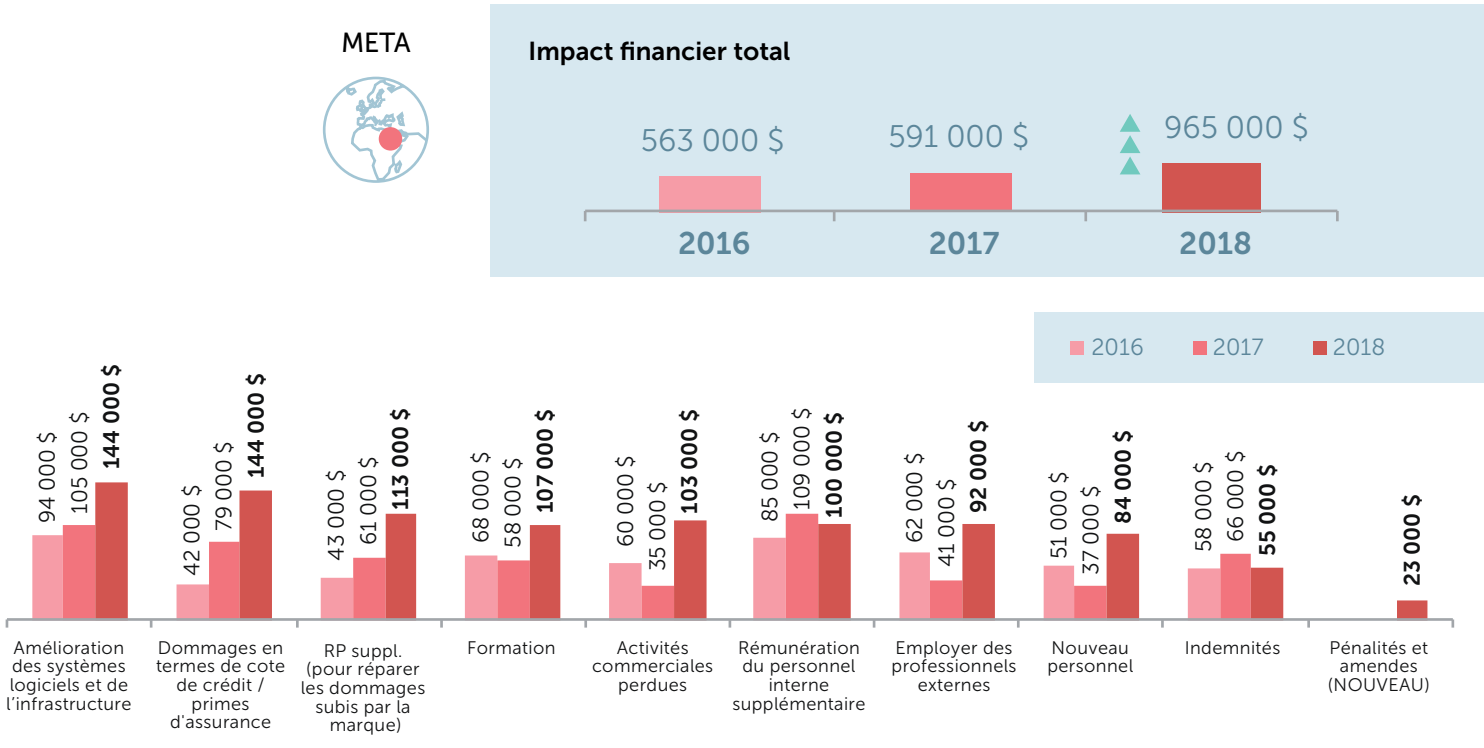


Figure 7 : impact financier d'une violation de données pour les grandes entreprises de la région META

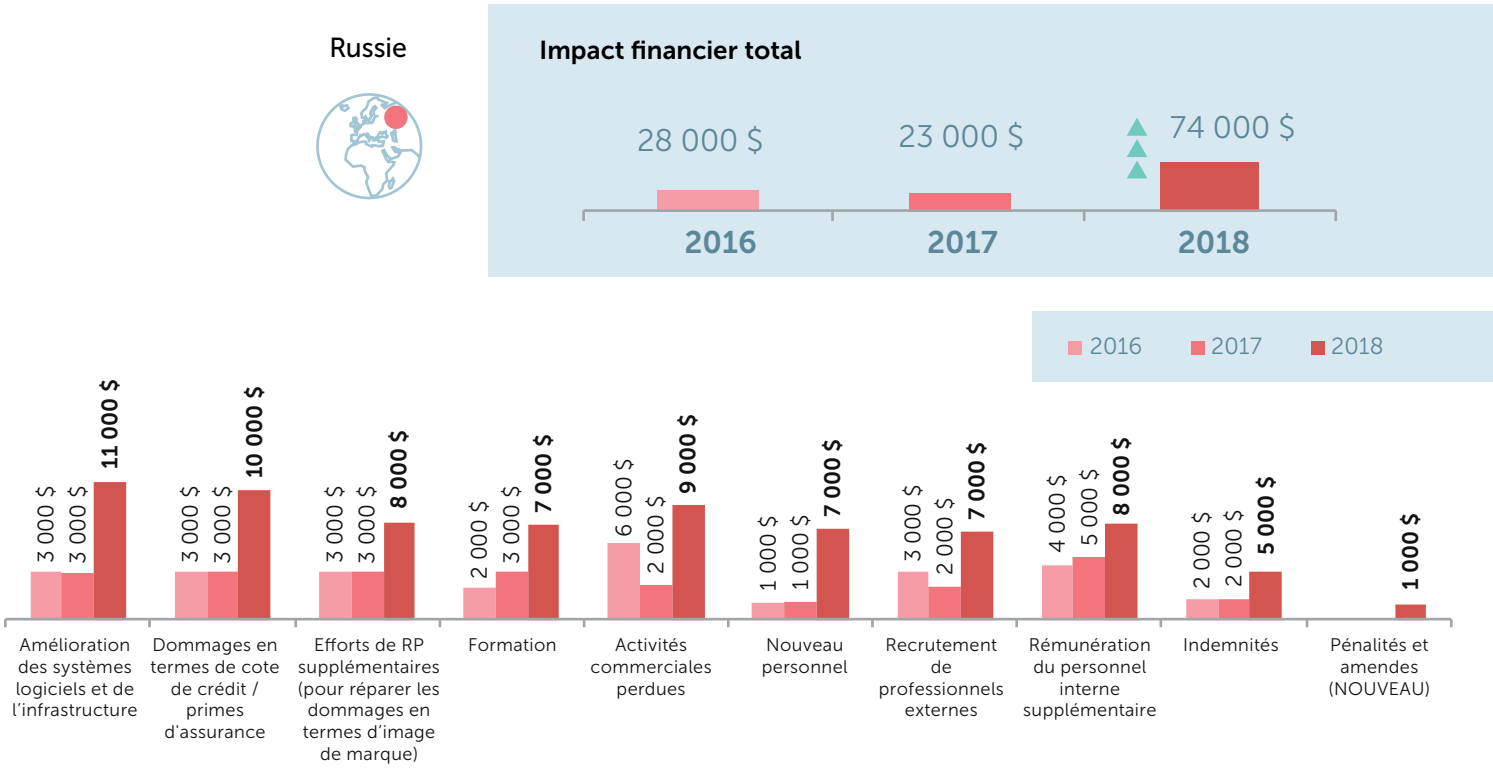


Figure 8 : impact financier d'une violation de données pour les PME en Russie

Enfin, les PME de l'Asie-Pacifique et de Chine doivent faire face à des pertes de contrats à la suite d'une violation de données, ce qui leur coûte en moyenne 17 000 $ et laisse entendre que les clients locaux sont particulièrement impitoyables envers les entreprises qui sont victimes de violations de données.

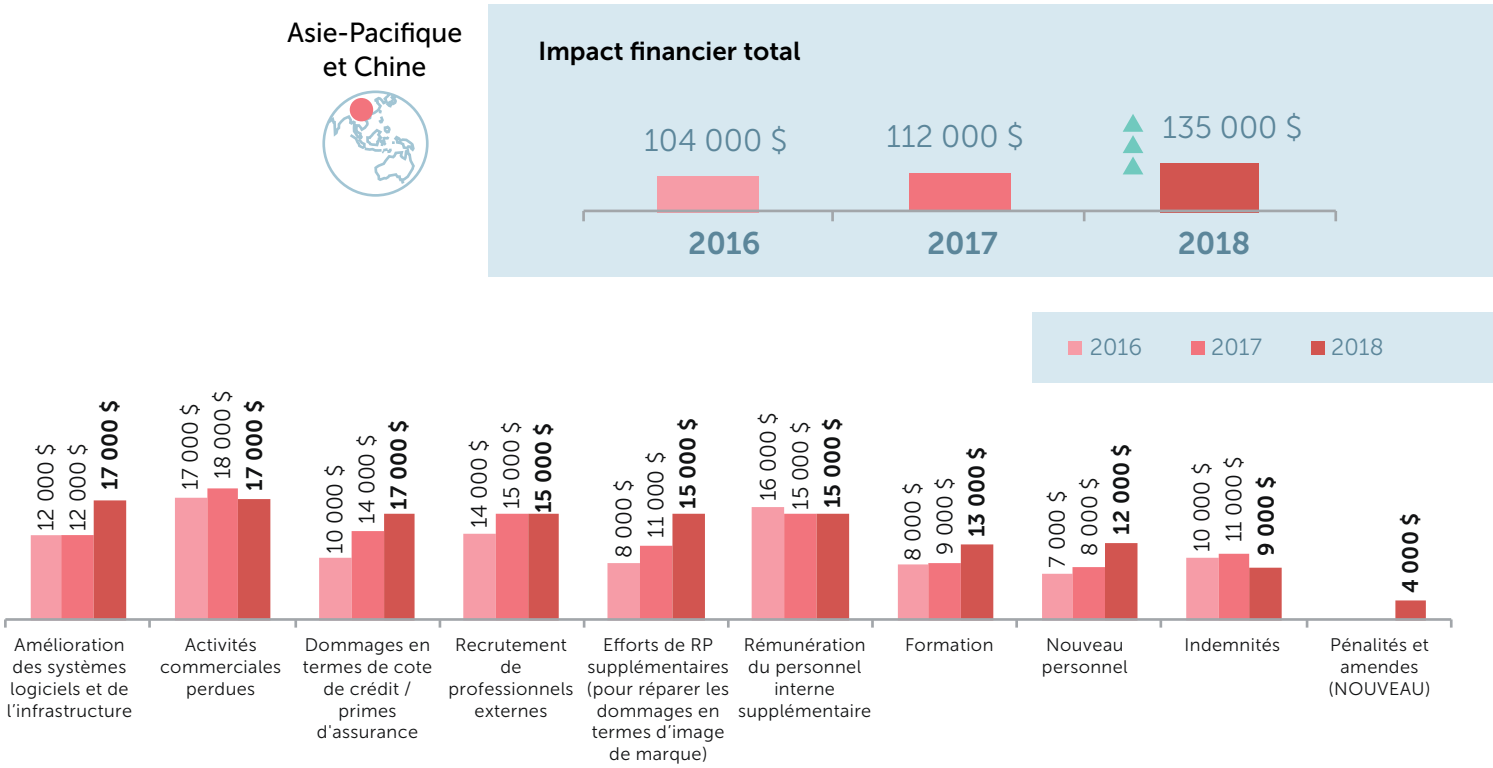


Figure 9 : impact financier d'une violation de données pour les PME en Asie-Pacifique/Chine

Les attaques les plus coûteuses : tout sur les données en déplacement

Il ne suffit pas de savoir combien coûte une violation de données. La compréhension des différents types de menaces auxquelles les entreprises sont confrontées et qui, si elles réussissent, coûtent le plus cher en matière de récupération est un atout précieux. **Les cinq principaux types de violation de données ayant les répercussions financières les plus importantes pour les grandes entreprises étaient les suivantes :**

- Attaques ciblées - **1,64 million de dollars**
- Incidents affectant l'infrastructure informatique hébergée par un tiers - **1,47 million de dollars**
- Perte physique des appareils ou des supports de l'entreprise - **1,42 million de dollars**
- Incidents impliquant des appareils non informatiques connectés - **1,41 million de dollars**
- Incidents affectant des services cloud tiers que nous utilisons - **1,38 million de dollars**

À titre de comparaison, les 5 dépenses principales des PME étaient les suivantes :

- Incidents affectant l'infrastructure informatique hébergée par un tiers - **179 000 $**
- Incidents impliquant des appareils non informatiques connectés - **148 000 $**
- Incidents affectant les environnements virtualisés - **146 000 $**
- Incidents affectant des services cloud tiers que nous utilisons - **130 000 $**
- Incidents affectant des fournisseurs avec lesquels nous partageons des données - **130 000 $**

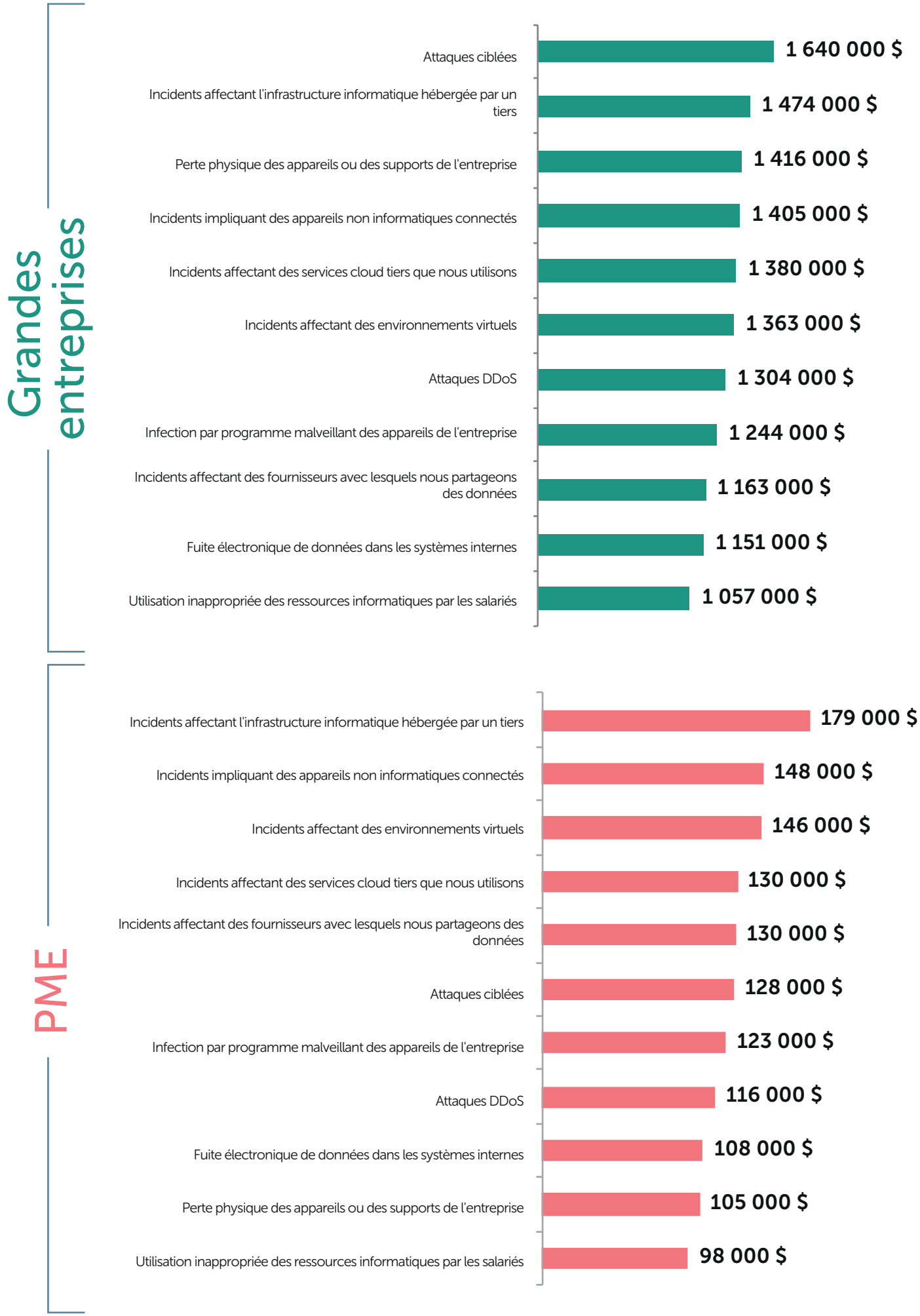


Figure 9 : types de violations de données et leur impact financier

> Dans le cadre de stratégies de transformation numérique, les entreprises travaillent souvent avec des tiers pour migrer les données ou modifier l'accès à leur infrastructure. Les entreprises doivent être convaincues que leurs fournisseurs externes prennent les précautions de sécurité nécessaires.

Toutefois, la nature coûteuse des violations de données provenant de tiers montre que cette confiance est souvent mal placée, car toute défaillance du côté du fournisseur aura également un impact direct sur le client.

Lorsqu'il s'agit de tous les incidents de cybersécurité, la situation est très similaire, les tiers étant à l'origine des types d'incidents les plus coûteux. **Les cinq principaux types d'incidents affectant les entreprises étaient les suivants :**

- Attaques ciblées - **1,11 million de dollars**
- Incidents affectant l'infrastructure informatique hébergée par un tiers - **1,09 million de dollars**
- Incidents impliquant des appareils non informatiques connectés - **993 000 $**
- Incidents affectant des services cloud tiers que nous utilisons - **942 000 $**
- Fuite électronique de données dans les systèmes internes - **909 000 $**

Pour les PME, les cinq principaux types d'incident étaient les suivants :

- Incidents affectant l'infrastructure informatique hébergée par un tiers - **118 000 $**
- Incidents impliquant des appareils non informatiques connectés - **98 000 $**
- Incidents affectant des services cloud tiers que nous utilisons - **89 000 $**
- Attaques ciblées - **87 000 $**
- Incidents affectant des fournisseurs avec lesquels nous partageons des données - **83 000 $**

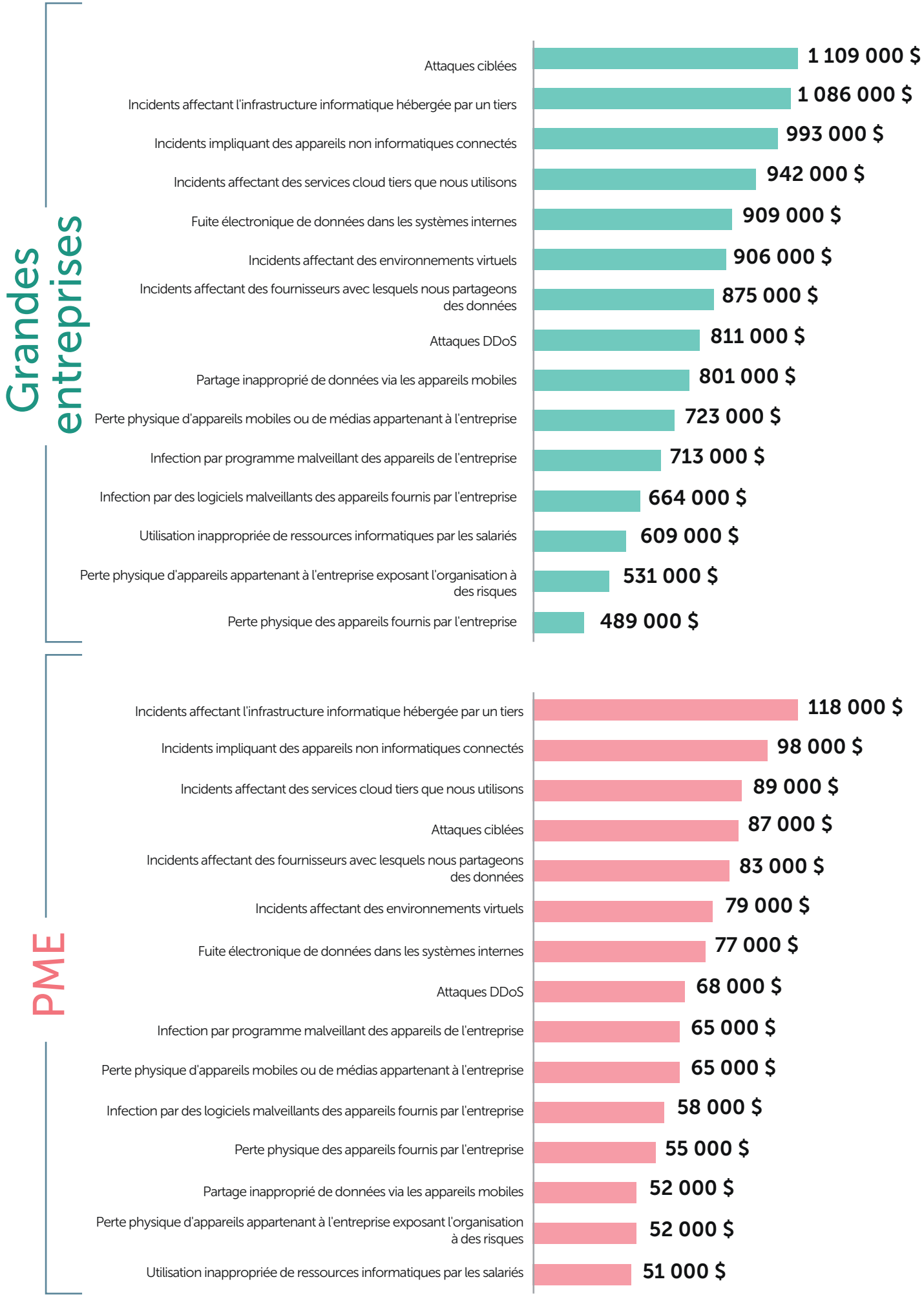


Figure 10 : types d'incidents de cybersécurité et leur impact financier

La sécurité informatique doit être abordée lors des conseils d'administration

Étant donné que les violations de données et les incidents de sécurité coûtent de plus en plus cher aux entreprises, il devient de plus en plus important de mettre en place des outils et des processus pour se défendre contre les activités cybercriminelles. Cette tendance se reflète dans le montant que les grandes entreprises et les PME consacrent à la sécurité informatique.

En effet, les budgets de sécurité informatique ont augmenté dans toutes les tailles d'entreprises au cours des 12 derniers mois. Pour les grandes entreprises, le pourcentage du budget informatique global consacré à la sécurité est passé de 23 % en 2017 à plus d'un quart (26 %) en 2018, soit une moyenne de 8,9 millions de dollars.

Une tendance similaire peut également être observée dans les PME et les TPE. Les PME dépensent maintenant en moyenne 246 000 $ par année pour la sécurité informatique, ce qui représente 23 % du budget informatique global, contre 20 % en 2017. Les TPE affichent la plus forte augmentation en pourcentage, les budgets de sécurité passant de 16 % (2 000 $) à 20 % (4 000 $) du total des dépenses informatiques.

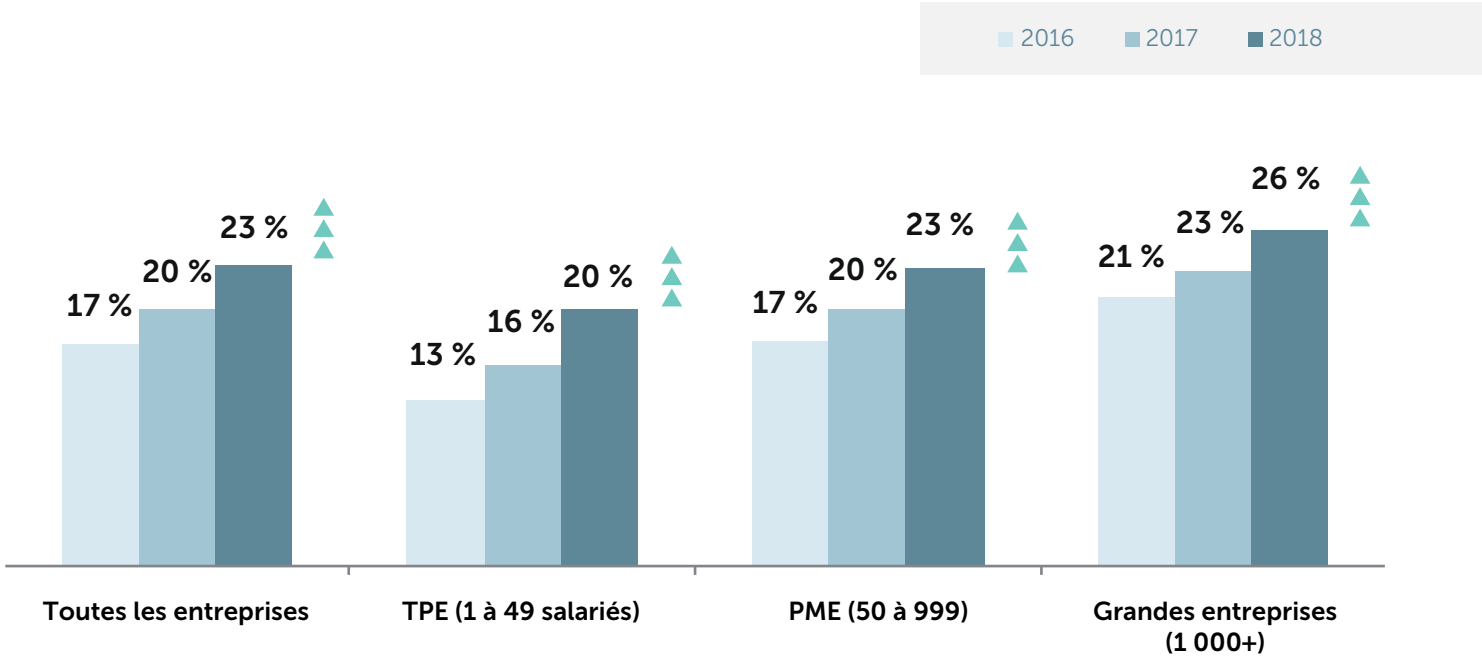


***Figure 11** : suivi du pourcentage des budgets informatiques consacrés à la sécurité*

Ces résultats sont cohérents dans presque toutes les régions, mais il est intéressant de noter qu'il y a quelques anomalies, en particulier parmi les grandes entreprises en Amérique du Nord et dans la région META où les proportions du budget informatique consacrées à la sécurité ont connu les plus fortes augmentations à partir de 2017. Les budgets des grandes entreprises en Amérique du Nord ont augmenté de 9 points pour atteindre 28 % du budget informatique total, tandis que celui des grandes entreprises dans la région META a augmenté de 8 points pour atteindre 27 %.

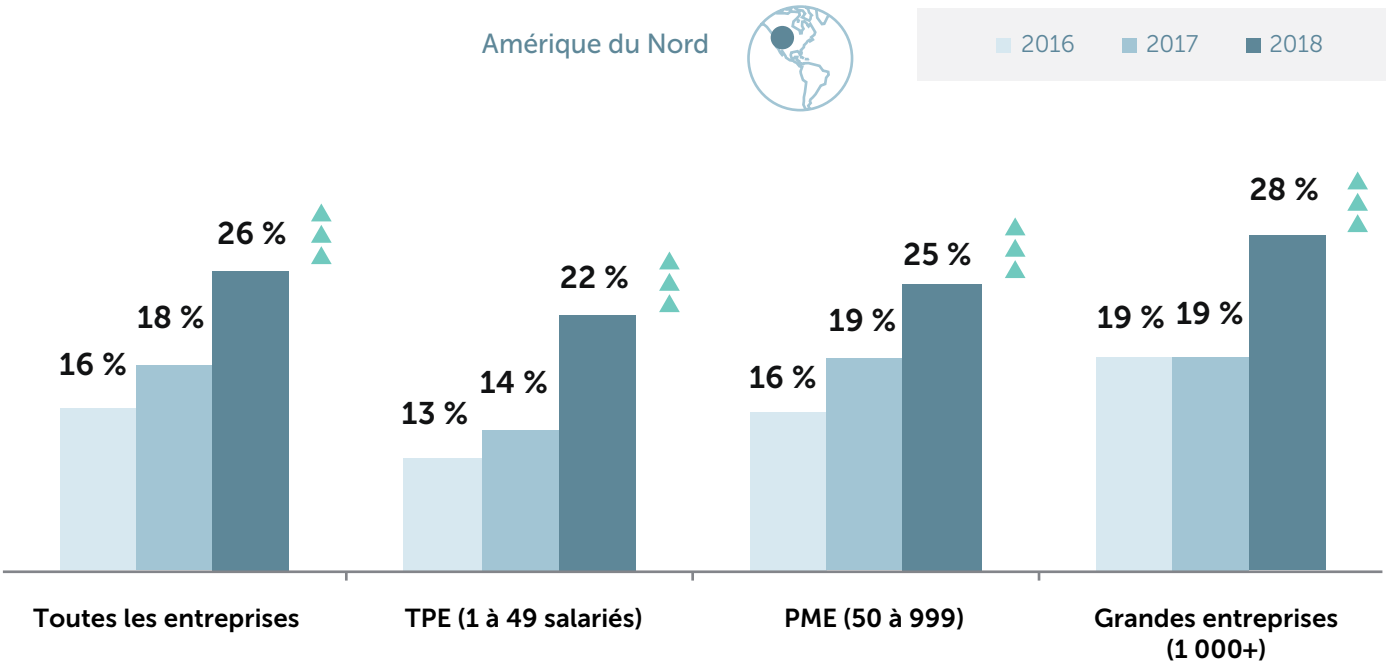


***Figure 12** : suivi du pourcentage des budgets informatiques consacrés à la sécurité en Amérique du Nord*

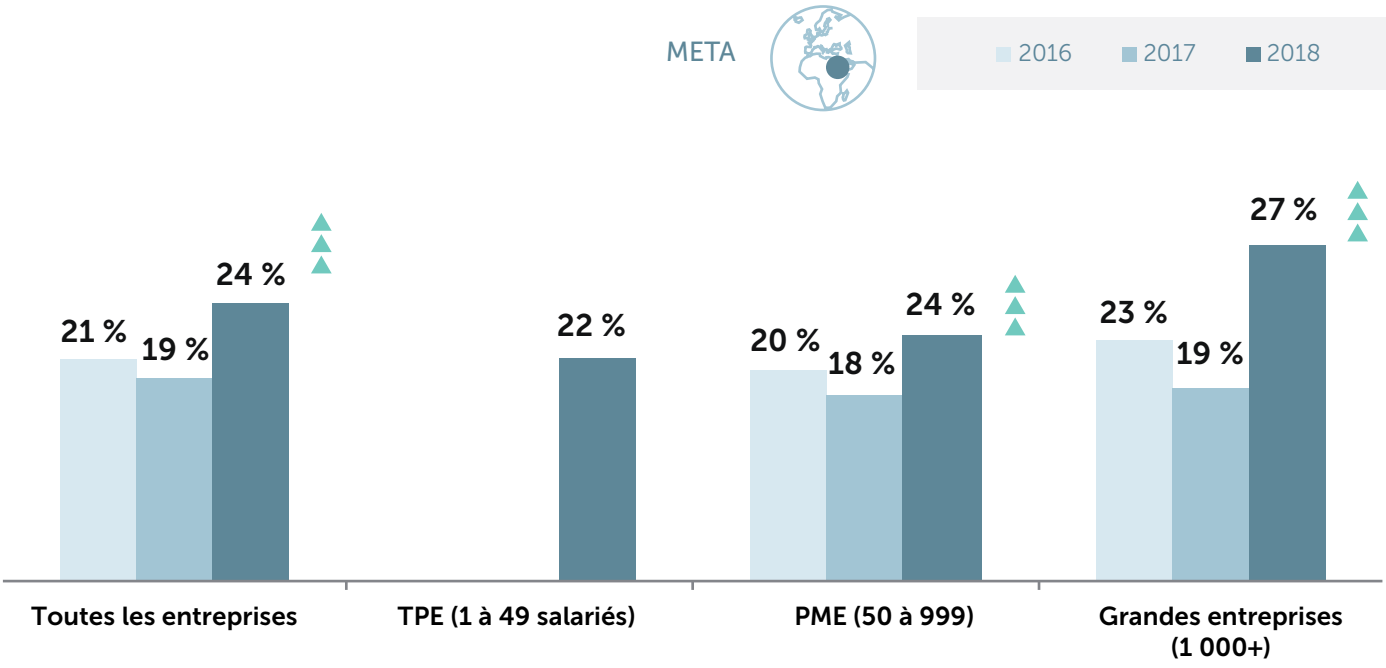


***Figure 13** : suivi du pourcentage des budgets informatiques consacrés à la sécurité dans la région META*

En comparaison, le pourcentage des budgets de sécurité informatique est demeuré le même pour les PME et les grandes entreprises de l'Asie-Pacifique et de la Chine (23 % et 26 % respectivement) et les grandes entreprises du Japon (26 %). Cette absence de mouvement pourrait s'expliquer par le fait que les grandes entreprises japonaises dépensent en moyenne 31,1 millions de dollars, ce qui est nettement plus élevé que dans les autres régions.

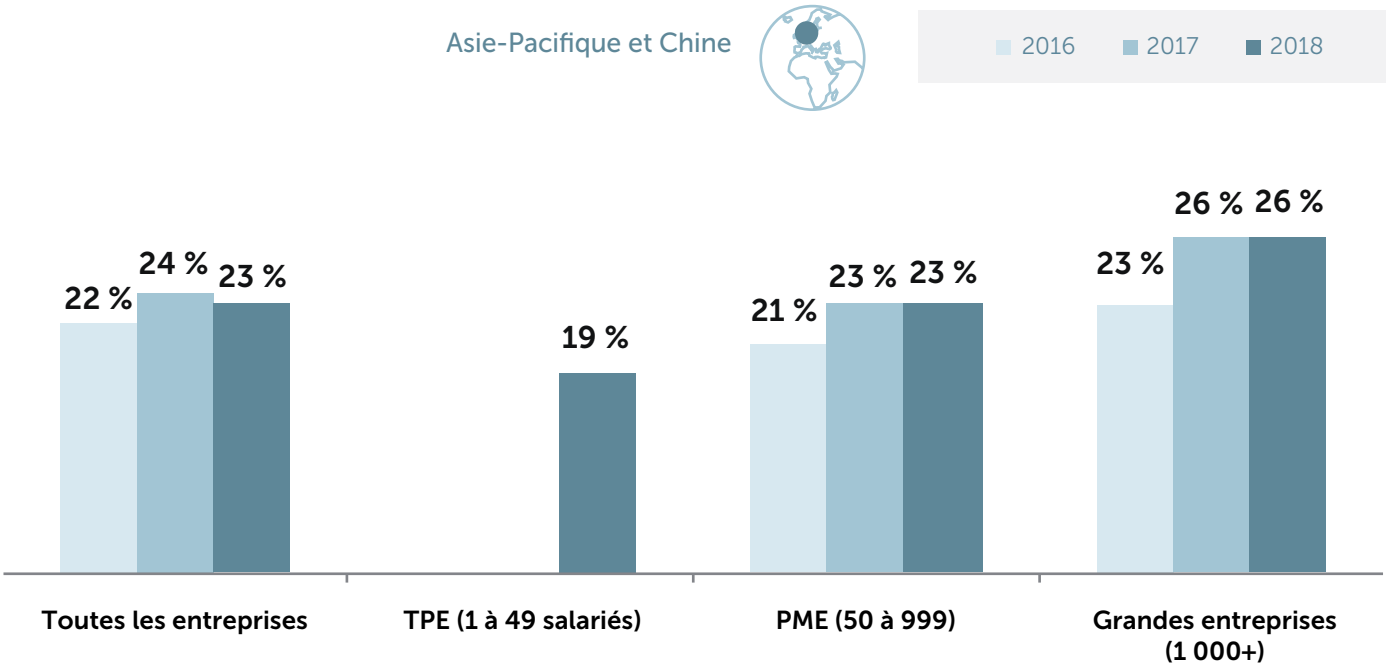


***Figure 14** : suivi du pourcentage des budgets informatiques consacrés à la sécurité en Asie-Pacifique/Chine*

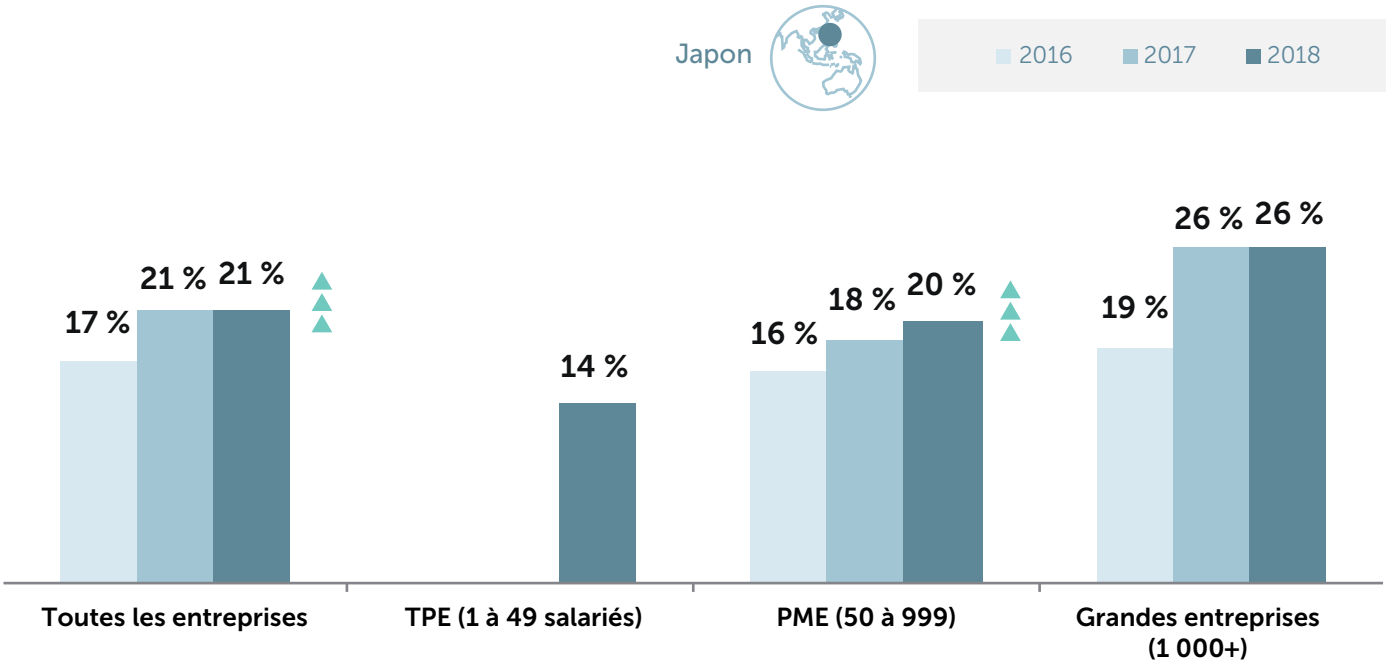


***Figure 15** : suivi du pourcentage des budgets informatiques consacrés à la sécurité au Japon*

De plus, les entreprises s'attendent toujours à ce que leurs budgets de sécurité informatique augmentent à l'avenir. Globalement, tant les TPE que les grandes entreprises prévoient que la somme qu'elles dépenseront pour la cybersécurité augmentera de 15 % au cours des trois prochaines années, tandis que les PME prévoient une augmentation de 14 %.

Là encore, il existe des différences régionales, comme les PME japonaises qui prévoient la plus faible augmentation (7 %) de leur budget de sécurité informatique. À l'autre extrémité de l'échelle, les TEP d'Amérique latine prévoient une augmentation de 22 % de leurs budgets de sécurité, devant les grandes entreprises et les PME de la région META (19 %) et de Russie (18 %).

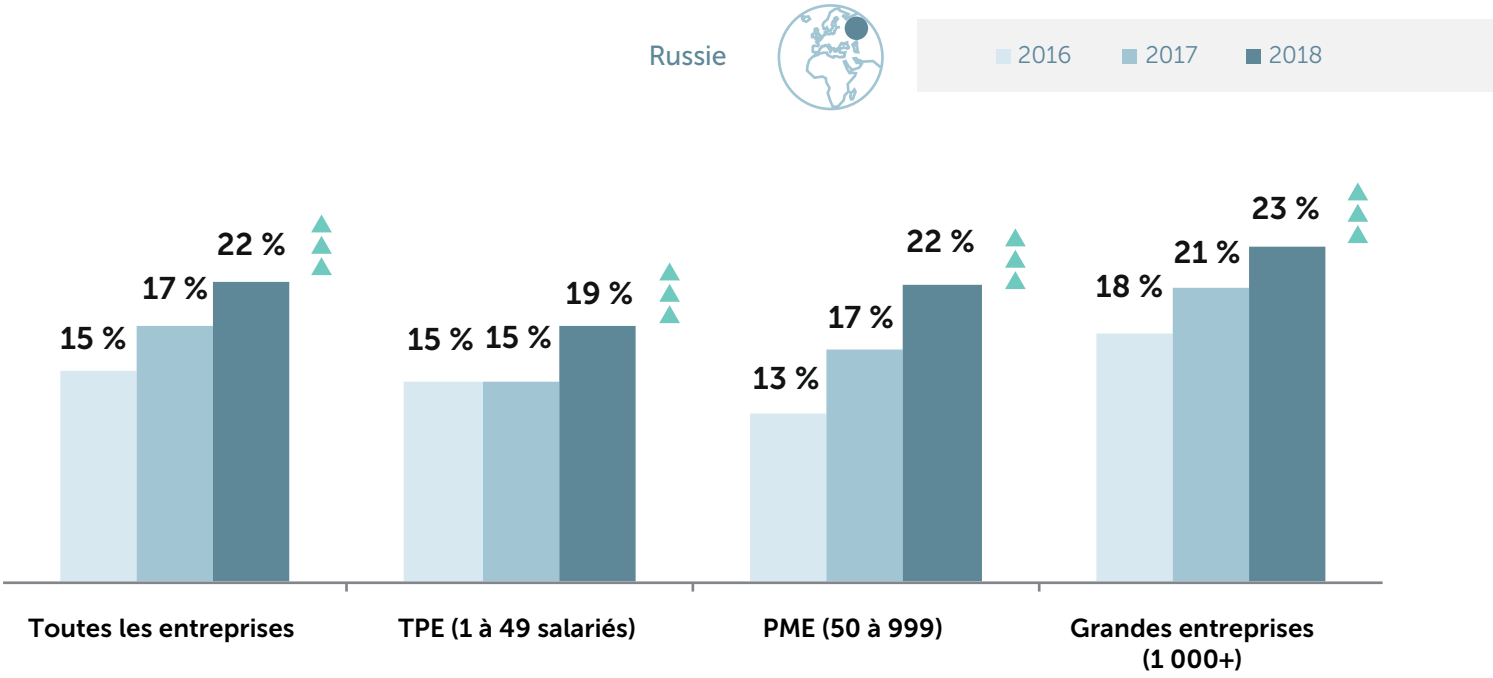


***Figure 16** : suivi du pourcentage des budgets informatiques consacrés à la sécurité en Russie*

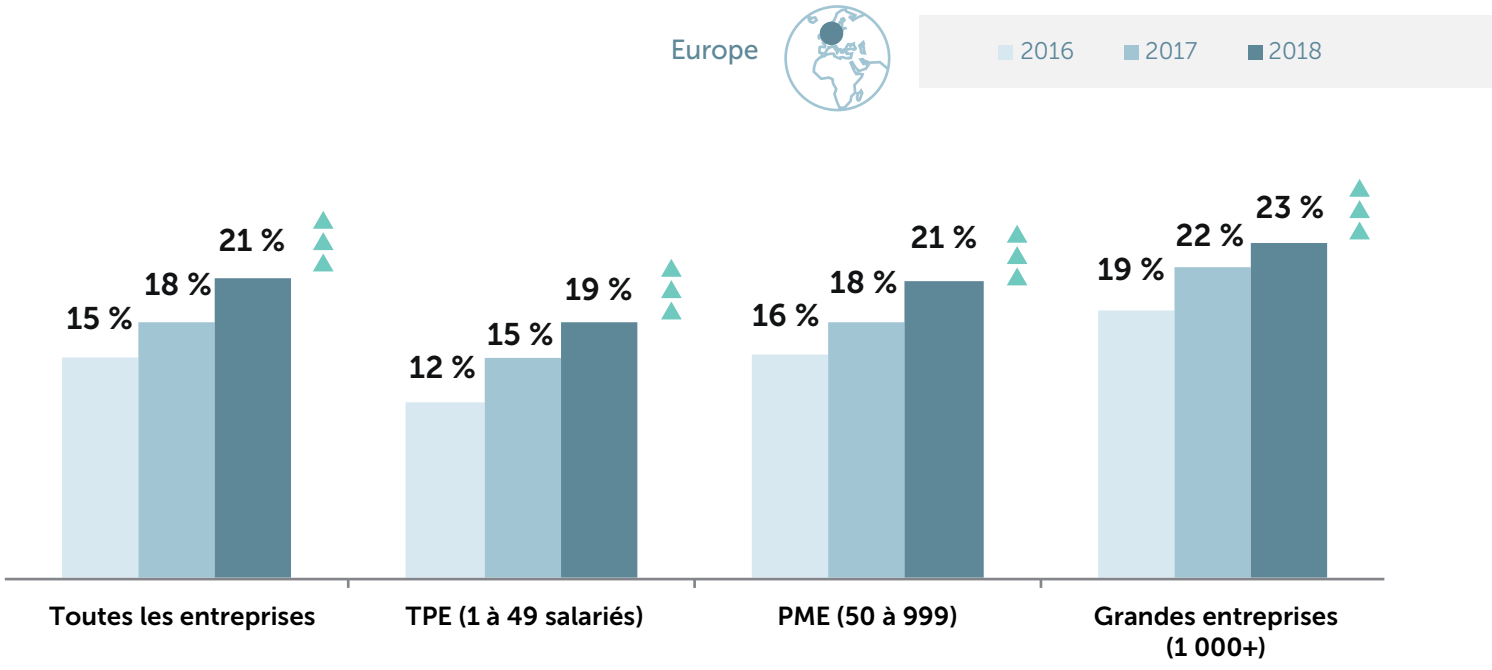


***Figure 17** : suivi du pourcentage des budgets informatiques consacrés à la sécurité en Europe*

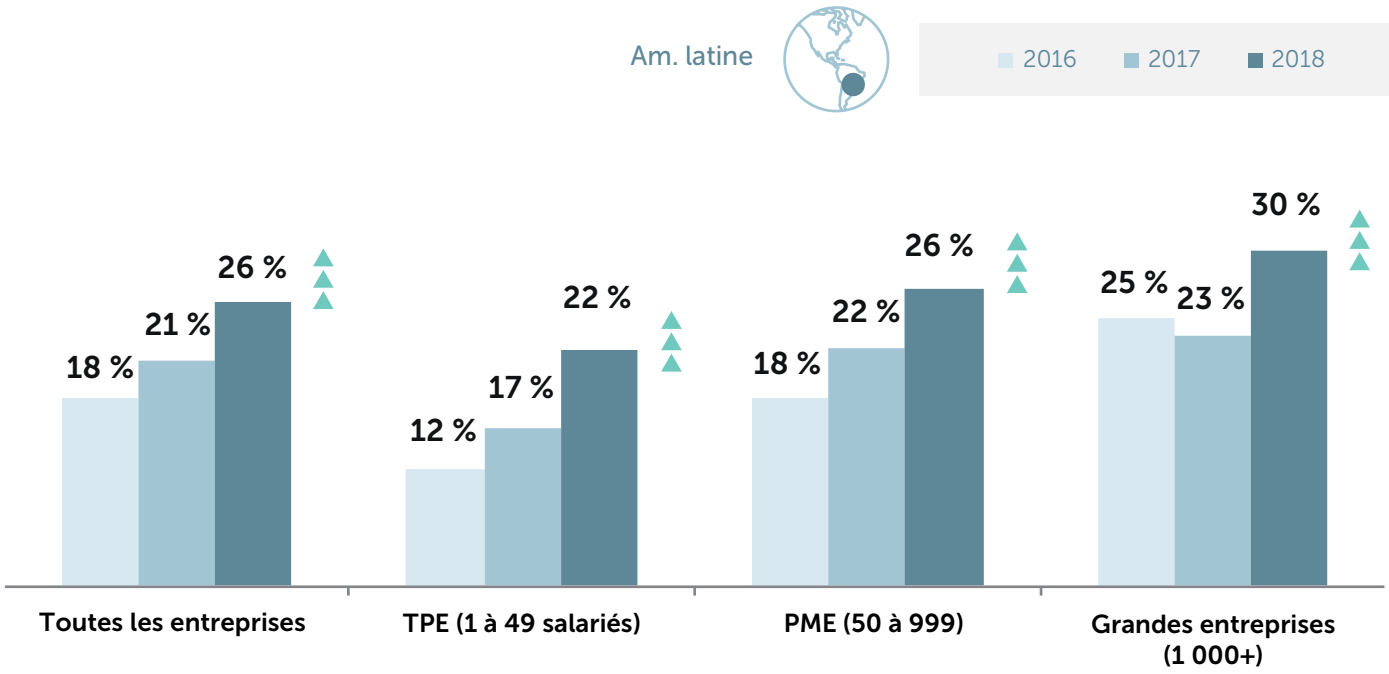
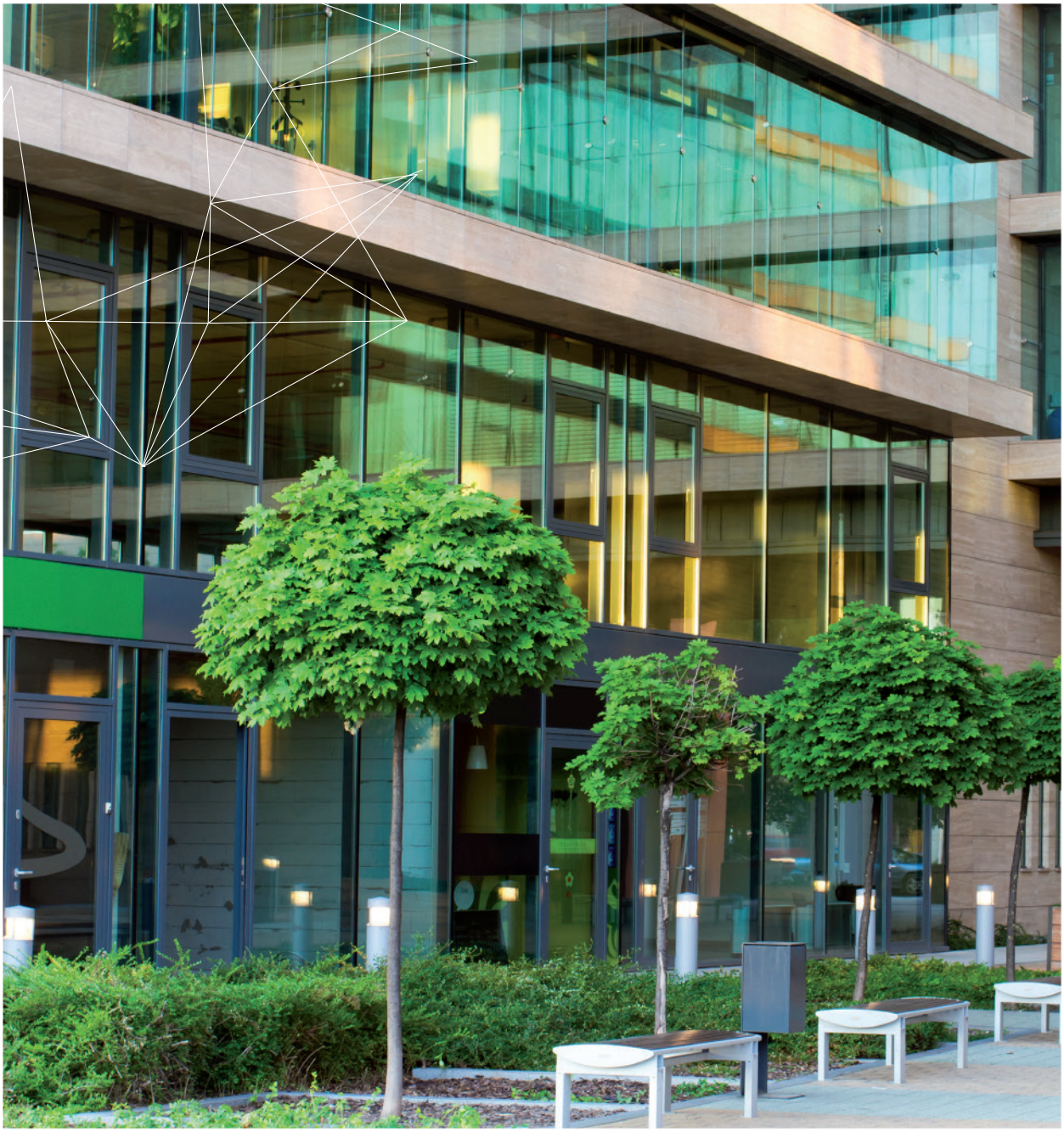


***Figure 18** : suivi du pourcentage des budgets informatiques consacrés à la sécurité en Amérique latine*

Les motivations pour investir dans la sécurité informatique



Avec des entreprises de tailles différentes, des industries différentes et des besoins divers à prendre en considération, la question clé que nous voulions poser aux entreprises était de savoir exactement ce qui les motive à investir dans la cybersécurité.

Alors que les budgets informatiques devraient continuer à croître au cours des trois prochaines années, les entreprises sont clairement conscientes de la nécessité d'investir dans la sécurité informatique, aujourd'hui et à l'avenir. Comme notre étude l'a révélé, il existe des facteurs évidents qui incitent les entreprises à investir leur argent là où c'est nécessaire.

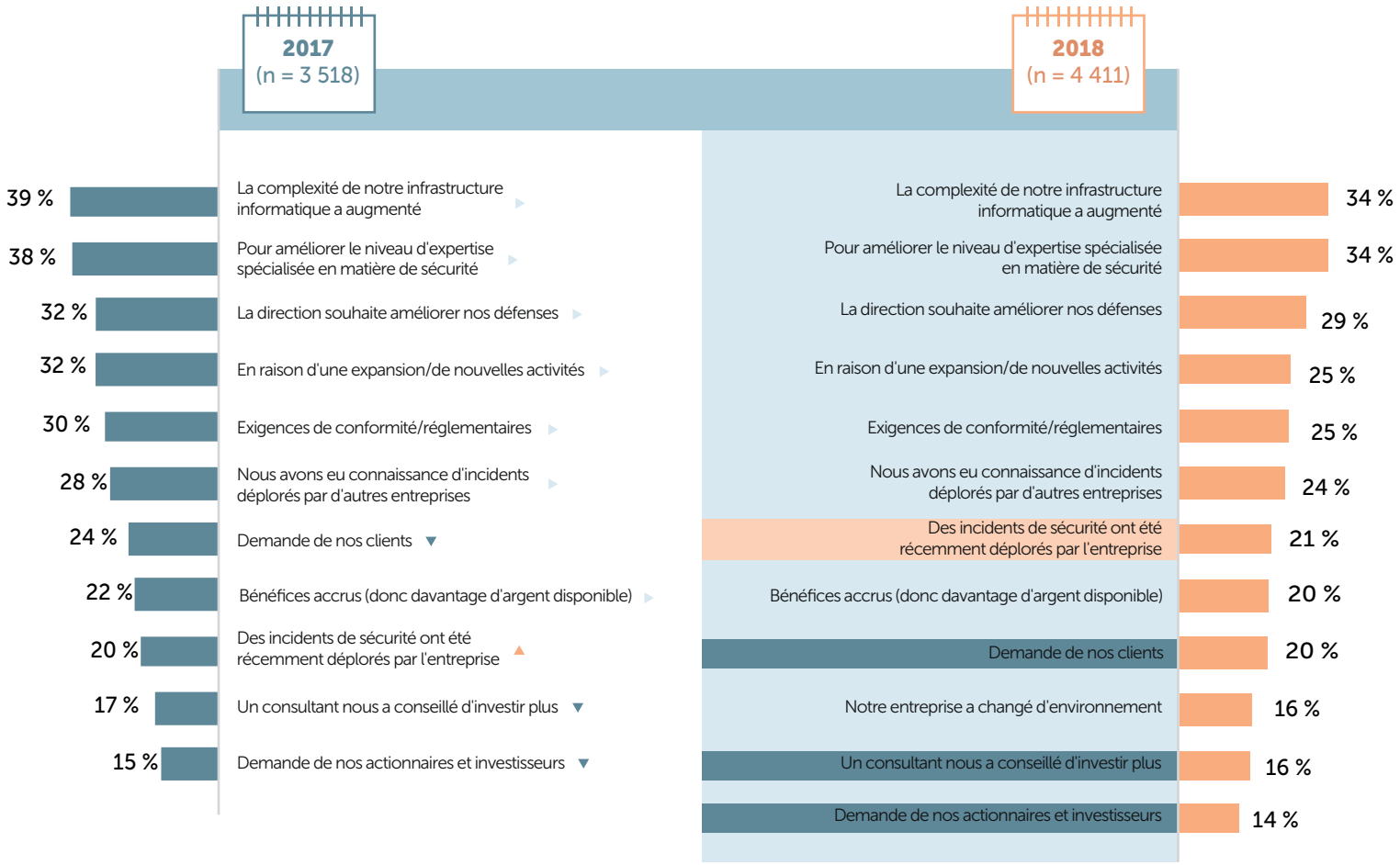


***Figure 20** : trois principales motivations d'investir dans la sécurité informatique dans toutes les régions*

Comme le montre le tableau ci-dessus, la complexité accrue de l'infrastructure informatique a conservé sa position au sommet et s'est classée conjointement avec l'amélioration du niveau d'expertise en sécurité spécialisée (34 % dans les deux cas) comme étant la plus grande motivation pour investir dans la sécurité informatique dans toutes les régions. Elles sont suivies de près par les pressions de la direction (29 %), ce qui suggère que les chefs d'entreprise s'intéressent de plus en plus à la cybersécurité, et l'impact des nouvelles activités commerciales ainsi que les exigences de conformité (25 % dans les deux cas).

La demande des actionnaires et des investisseurs (14 %) a été identifiée comme le plus petit facteur de motivation de l'investissement en sécurité informatique, juste derrière les entreprises auxquelles un consultant a conseillé d'augmenter les dépenses de sécurité (16 %).

Comme il s'agit d'un domaine où les facteurs régionaux peuvent avoir une influence significative, nous avons également examiné les trois principaux facteurs de motivation pour chaque région afin d'identifier les similitudes ou différences qui pourraient servir à expliquer comment les différentes entreprises perçoivent l'importance de la cybersécurité.

Comme on pouvait s'y attendre, la complexité accrue de l'infrastructure informatique est apparue parmi les trois principaux facteurs de motivation dans toutes les régions, mais c'est aussi le principal facteur de motivation en Amérique du Nord (34 %), en Amérique latine (33 %) et en Europe (29 %). L'amélioration du niveau d'expertise des spécialistes de la sécurité était tout aussi importante et représente le principal facteur de motivation des investissements dans quatre des régions incluses dans l'étude : le Japon (48 %), l'Asie-Pacifique et la China (41 %), la région META (37 %) et la Russie (36 %). Cela s'explique probablement par le manque de compétences largement débattu dans le secteur de la cybersécurité. Les experts en sécurité sont toujours en nombre insuffisant, ce qui signifie que les entreprises de tous les secteurs ont du mal à trouver des personnes ayant les compétences nécessaires pour contrer les cyberattaques les plus sophistiquées d'aujourd'hui.

	Russie ++	Amérique du Nord	META	Asie-Pacifique	Japon	Am. latine	Europe
TOP-1	Pour améliorer le niveau d'expertise spécialisée en matière de sécurité **(36 %)**	La complexité de notre infrastructure informatique a augmenté **(34%)**	Pour améliorer le niveau d'expertise spécialisée en matière de sécurité **(37%)**	Pour améliorer le niveau d'expertise spécialisée en matière de sécurité **(41%)**	Pour améliorer le niveau d'expertise spécialisée en matière de sécurité **(48%)**	La complexité de notre infrastructure informatique a augmenté **(33 %)**	La complexité de notre infrastructure informatique a augmenté **(29%)**
TOP-2	La complexité de notre infrastructure informatique a augmenté **(33 %)**	Pour améliorer le niveau d'expertise spécialisée en matière de sécurité **(31%)**	La direction souhaite améliorer nos défenses **(29%)**	La complexité de notre infrastructure informatique a augmenté **(41%)**	La complexité de notre infrastructure informatique a augmenté **(34%)**	Pour améliorer le niveau d'expertise spécialisée en matière de sécurité **(28%)**	Pour améliorer le niveau d'expertise spécialisée en matière de sécurité **(27%)**
TOP-3/4	La direction souhaite améliorer nos défenses **(29%)**	La direction souhaite améliorer nos défenses **(30 %)**	La complexité de notre infrastructure informatique a augmenté **(29%)** Nous avons eu connaissance d'incidents déplorés par d'autres entreprises **(28 %)**	La direction souhaite améliorer nos défenses **(35%)**	Exigences de conformité/réglementaires **(26 %)**	En raison d'une expansion/de nouvelles activités **(26 %)** La direction souhaite améliorer nos défenses **(25%)**	Exigences de conformité/réglementaires **(25%)** La direction souhaite améliorer nos défenses **(24%)**

Figure 13 : *suivi du pourcentage des budgets informatiques consacrés à la sécurité dans la région META*

Le rôle croissant de la sécurité informatique lors des réunions du conseil d'administration est également évident. Les pressions de la direction sont arrivées en deuxième position pour la motivation des entreprises dans la région META (29 %) et en troisième ou quatrième position dans cinq autres régions : l'Asie-Pacifique et Chine (35 %), l'Amérique du Nord (30 %), la Russie (29 %), l'Amérique latine (25 %) et l'Europe (24 %).

Les résultats indiquent également que les changements réglementaires ont un impact financier sur les entreprises dans certaines régions. Un quart (25 %) des entreprises européennes ont identifié les exigences réglementaires/de conformité comme étant un moteur clé de l'investissement dans la cybersécurité, ce qui n'est pas surprenant compte tenu de l'attention portée au RGPD qui entre en vigueur en mai 2018.

Les entreprises européennes adoptent probablement une vision à long terme lorsqu'il s'agit de se conformer aux règlementations. Avec des amendes du RGPD pouvant atteindre un maximum de **20 millions d'euros**, soit 4 % du chiffre d'affaires annuel global de l'entreprise, investir dans la sécurité informatique pourrait permettre aux entreprises de réaliser d'énormes économies à long terme.

Il en va de même pour les entreprises japonaises. Le gouvernement japonais a récemment mis à jour sa loi sur la protection des données personnelles (l'une des plus anciennes lois sur la protection des données en Asie) et a établi une nouvelle Commission de protection des données personnelles (PPC) pour régir la conformité des entreprises.

Conclusion

Notre étude a démontré de manière catégorique que la sécurité informatique joue un rôle plus stratégique dans le paysage commercial moderne.

L'une des raisons en est que les coûts liés aux violations de données et aux incidents de sécurité sont toujours en hausse et n'ont jamais été aussi élevés, soit **1,23 million de dollars** pour les grandes entreprises et **120 000 $** pour les PME. Ce seul fait devrait suffire à faire comprendre aux entreprises la valeur financière de la mise en place d'outils de cybersécurité.

Mais nos recherches montrent clairement que la menace des coûts n'est pas le seul facteur qui inscrit la sécurité à l'ordre du jour des conseils d'administration. L'informatique joue également un rôle de plus en plus important dans les affaires, les entreprises se tournant de plus en plus vers les stratégies de transformation numérique pour faire face à la concurrence et aux attentes des consommateurs. Dans cet environnement, un dysfonctionnement du système ou un incident informatique pourrait avoir un impact rapide et direct sur les flux de revenus.

Les chefs d'entreprise comprennent de mieux en mieux que si leur stratégie de transformation numérique (c'est-à-dire leur passage au cloud, leur migration vers une nouvelle plate-forme ou leur bouleversement des pratiques de travail existantes) est mise en danger, il en va de même pour l'entreprise elle-même.

En fin de compte, pour beaucoup d'entreprises, cela se résume à une simple question : est-ce que faire de la sécurité informatique un investissement plus stratégique finira par payer les dividendes de l'entreprise à long terme ?

La réponse, semble-t-il, est un « oui » retentissant.