ESSEC
Solutions Entreprises

Rapport

Étude des enjeux actuels de la cybersécurité pour les entreprises

Novembre 2022

Sommaire

Executive Summary

1

ESSEC
Solutions Entreprises

Le marché de la cybersécurité est en évolution et les entreprises doivent s'adapter afin de garantir la sécurité de leur système d'information

Le marché de la cybersécurité est en pleine croissance…

> Le marché de la cybersécurité est en forte croissance depuis de nombreuses années et cette dynamique ne semble pas se tarir : on prévoit une **croissance de 12% par an jusqu'en 2030**
> Malgré cela, c'est un secteur qui manque de spécialistes et dans lequel certaines entreprises sont parfois **réticentes à investir**

… Il est porté par des événements de différentes natures…

> **La crise du Covid-19** a bouleversé les habitudes informatiques des entreprises. Elles se sont très rapidement adaptées aux confinements en mettant en place le **télétravail**
> Cela a désorganisé les réseaux et a engendré une hausse des attaques. Plus généralement, la cybersécurité évolue et se réinvente au gré des crises, des tensions, **notamment géopolitiques**, et des différents événements qui touchent au secteur
> Les risques étant **plus nombreux et virulents**, les entreprises ont tendance à investir plus, donc la demande augmente, forçant le secteur à innover et proposer des offres adaptées aux nouvelles menaces

… Et fait face à des évolutions structurelles

> Dans un premier temps, ce sont les **cyberattaques qui évoluent**. En effet, les outils et les manières d'attaquer changent au **fil des crises** mais également avec la **professionnalisation des cyberdélinquants** qui sont de plus en plus organisés
> Cependant, la **technologie évolue elle aussi**, pour offrir une plus grande précision de ciblage et une réactivité en cas d'attaque pour permettre aux entreprises de **sécuriser leurs réseaux**. C'est le cas notamment de l'accélération de la protection des drives après l'augmentation du télétravail ou au développement de l'intelligence artificielle

“ Verbatims ”

*« Il n'y a **aucune raison que le marché de la cybersécurité soit en décroissance**, déjà, lorsqu'il sera en stagnation il s'agira d'un tremblement de terre. Actuellement je suis dans une entreprise qui vise une **croissance de 30 à 50% par an**. »*

Un leader d'une grande entreprise de la cybersécurité

*« Nos critères de choix des solutions de cybersécurité sont l'**efficacité**, le **coût**, la **crédibilité**, le **retour d'expérience**, la **notoriété**, les **certifications** et les **référencements** auprès d'acteurs majeurs (ANSSI). »*

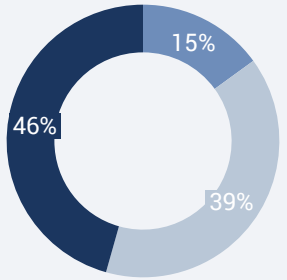
Un RSSI interrogé

L'objectif de l'étude est d'interroger des RSSI et des entreprises de la cybersécurité afin de comprendre les enjeux de la cybersécurité pour les entreprises

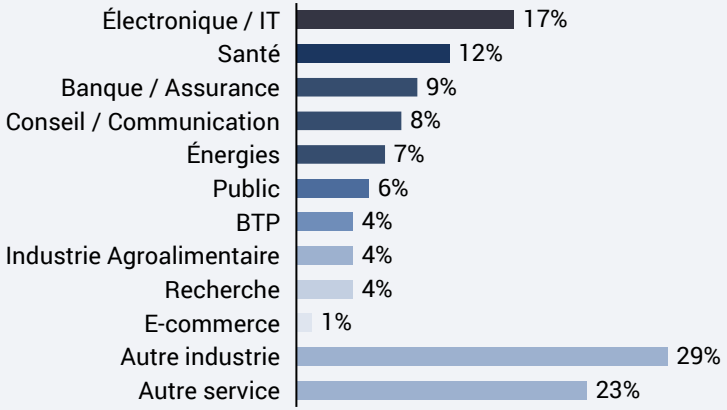
160

questionnaires administrés à des Responsables de la Sécurité des Systèmes d'Information (RSSI)

Profil des entreprises ayant répondu à l'enquête



- TPE / Start-up
- PME
- Grande Entreprise



Exemples d'entreprises ayant répondu à l'enquête

AIRBUS · Allianz · Agence régionale Grand Est du tourisme · cnrs · accenture · suez · Avocats Barreau de Paris

4

entretiens réalisés avec des professionnels de la cybersécurité

Les entreprises interrogées

Cisco · proofpoint · Trend Micro · paloalto Networks

Le renforcement de son système d'information passe par 5 étapes clés qui, réunies, permettent de diminuer les risques d'attaques

Protéger son système

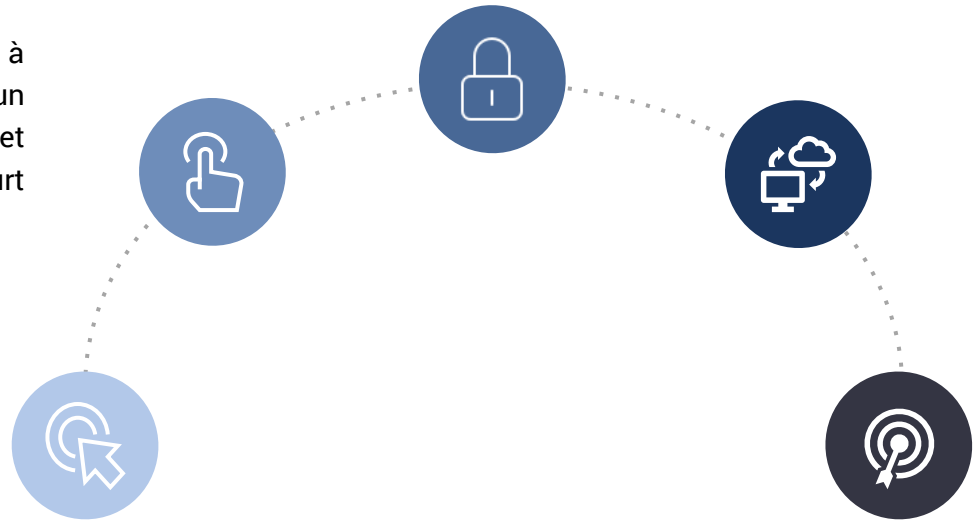
Adopter les bons réflexes **en interne grâce à la formation** et renforcer son système IT en ayant recours à des **prestataires et des nouvelles technologies**

Identifier les failles

Avoir recours à des audits et faire appel à des cabinets de conseil pour établir un **état des lieux du système de défense** et des risques que l'entreprise encourt

Détecter les menaces entrantes

Mettre en place **une surveillance des flux** pour être alerté en cas d'incident. Cette veille peut être **réelle ou virtuelle** (recours à l'intelligence artificielle par exemple)



Anticiper les menaces

Mettre en place des **veilles technologiques** pour connaître les menaces et anticiper les risques. Se renseigner sur les **tendances en termes d'attaque et d'innovation**

Réagir efficacement

Adopter les bons réflexes en cas de cyberattaque. Tester l'efficacité de son SOC (Security Operation Center) en temps de crise pour contrer les prochaines

Les enjeux de la cybersécurité

ESSEC
Solutions Entreprises

Le marché de la cybersécurité est en pleine croissance

2.1

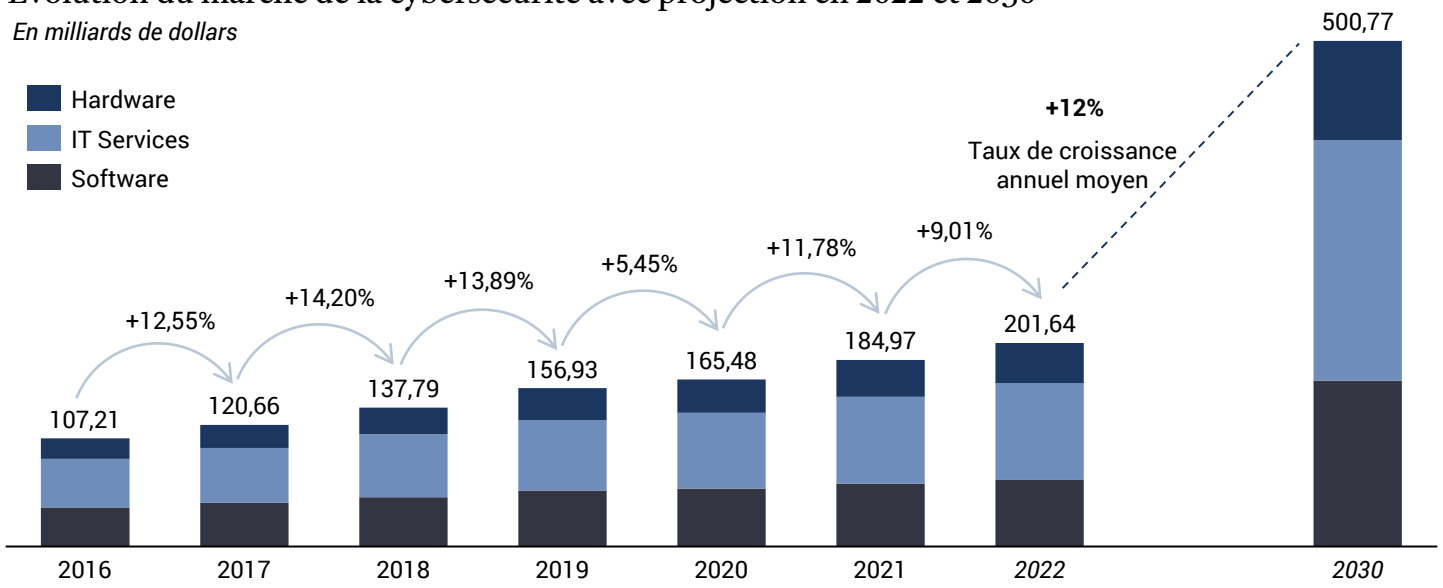
ESSEC
Solutions Entreprises

Le marché de la cybersécurité devrait connaître une croissance annuelle de 12% d'ici 2030…

- Une croissance de l'ordre de **12%** est attendue entre 2022 et 2030, faisant passer le marché de **184,97 milliards de dollars** en 2021 à **500,7 milliards** en 2030
- Cette croissance s'explique en partie par le **coût croissant des attaques** sur les données, par les tendances émergentes en matière de **mobilité des systèmes** (télétravail par exemple) et par les **réglementations gouvernementales** restrictives qui commencent à se mettre en place
- Le marché devrait être confronté à des défis liés au **manque de personnel qualifié au sein des entreprises** et à l'utilisation de **logiciels de cybersécurité sans licence** à cause du coût élevé de ces solutions, notamment pour les PME

Évolution du marché de la cybersécurité avec projection en 2022 et 2030

En milliards de dollars



Source : Statista, Financial Statements of Key Players

Source : Grand View Research

Les principaux acteurs de la cybersécurité en France…

Orange Cyberdefense — *838M€*

Capgemini — *N/a*

THALES — *1Md€*

TEHTRIS — FACE THE UNPREDICTABLE — *5,8M€*

… Et dans le monde

CISCO — *42Mds€*

paloalto NETWORKS — *3,6Mds€*

Check Point SOFTWARE TECHNOLOGIES LTD. — *2Mds€*

BROADCOM — *23Mds€*

JUNIPER NETWORKS — *4Mds€*

FORTINET — *3Mds€*

Tous les chiffres d'affaires datent de 2021

… Cependant, il est au cœur de défis multiples, à la tête desquels la recrudescence des cyberattaques

Il y a de plus en plus d'attaques

> **72% des entreprises** ont subi entre **un et dix** cyber-incidents et fuites de données au cours de 2021 d'après une étude de Deloitte

> Cette augmentation découle en grande partie de l'opportunité que le **télétravail et la désorganisation entrepreneuriale** ont été pour les cybercriminels durant la crise du Covid-19, mais également à la professionnalisation des cyberattaques qui sont de plus en plus rentables

“ Verbatim ”

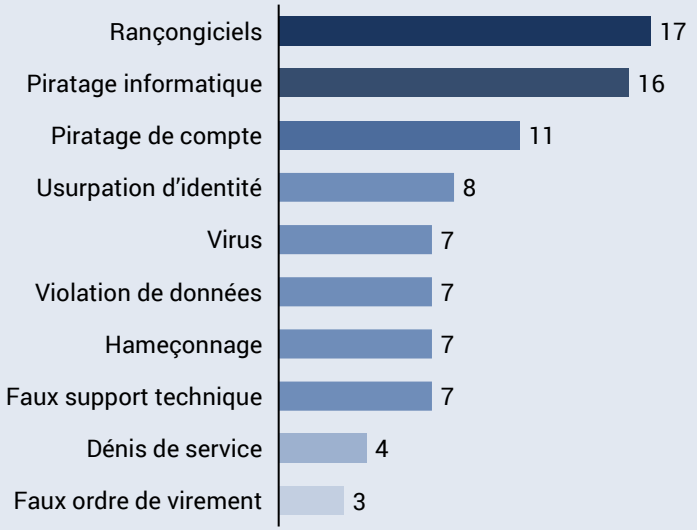
*« Notre société est de plus en plus **dépendante du digital.** Les impacts (et leviers de croissance pour les hackers) sont donc plus importants. Ajoutez à cela que la sensibilisation à ces sujets ne suit pas et nous arrivons dans la situation, **qui ira de mal en pis**. »*

Un RSSI interrogé

Qui se diversifient…

> Même si **l'hameçonnage** reste l'attaque la plus connue, celles-ci se sont **diversifiées** et ciblent tous les secteurs des entreprises

Le top 10 des recherches d'assistance effectuées par les entreprises et associations



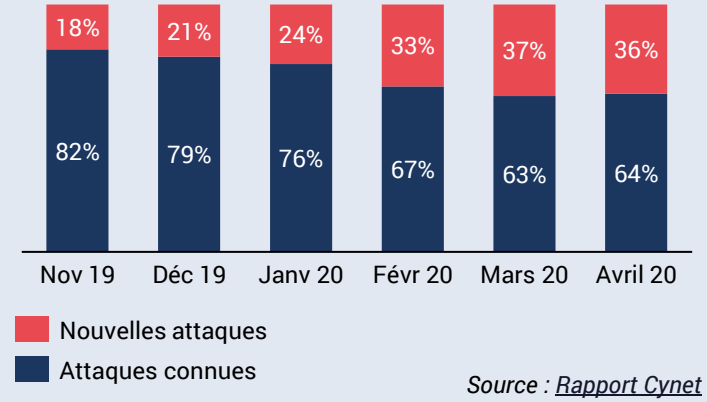
Source : Cybermalveillance.gouv.fr

… Et se complexifient

> L'augmentation du nombre de cyberattaques découle également de **l'innovation en termes d'attaques**

> Au début de la crise sanitaire, dès février 2020, **une part non négligeable de nouvelles attaques** encore non recensées a été observée. Cela fait état de la **réactivité** et de **l'inventivité** des cybercriminels

Évolution de la part des nouvelles cyberattaques au début de la pandémie



Source : Rapport Cynet

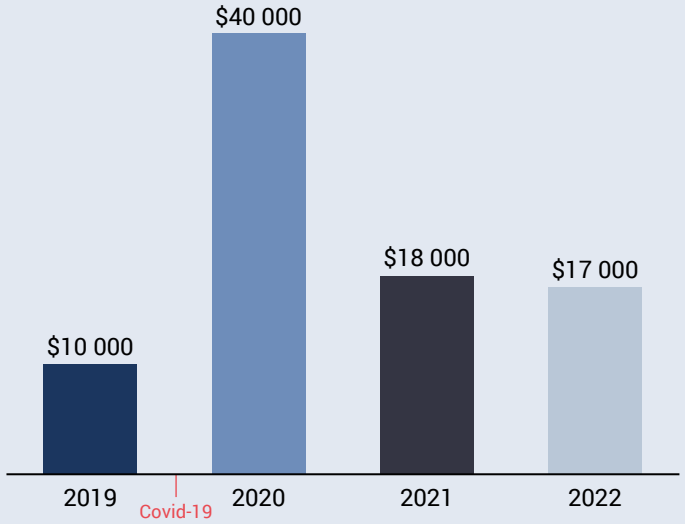
Le marché est en **constante évolution** pour répondre aux nouvelles problématiques posées par les **technologies innovantes** en termes d'attaques et **leur augmentation**

Les conséquences des cyberattaques peuvent être lourdes

ESSEC
Solutions Entreprises

Les conséquences des cyberattaques sont avant tout financières, et les pertes engendrées ont tendance à croître au fil des années

L'évolution du coût médian des cyberattaques qu'ont subies les entreprises en France au cours des 4 dernières années :



Source : Hiscox Cyber Readiness Reports

> Le **Covid-19** semble avoir eu un **impact** immédiat sur les **pertes financières** liées aux cyberattaques qui ont explosé **au cours de l'année 2020**

> Mais si l'impact de la crise semble s'être résorbé rapidement, elle **a instauré** une **tendance de long terme** induisant des pertes globalement plus importantes

58%

des entreprises ayant subi au moins une cyberattaque au cours des 12 derniers mois devaient faire face à des attaques relevant pour la plupart de **l'escroquerie.**

Or, quand bien même les cyberattaques ne relèvent **pas de l'escroquerie**, elles **induisent toujours un coût** croissant en fonction des dommages subis.

Les cyberattaques peuvent également impacter le chiffre d'affaires et la valorisation des entreprises :

> En 2021, **Bénéteau** a été victime d'une cyberattaque très violente qui a contraint l'entreprise à **fermer toutes ses usines** du jour au lendemain. L'impact en **perte de chiffre d'affaires est estimé à 45M€**

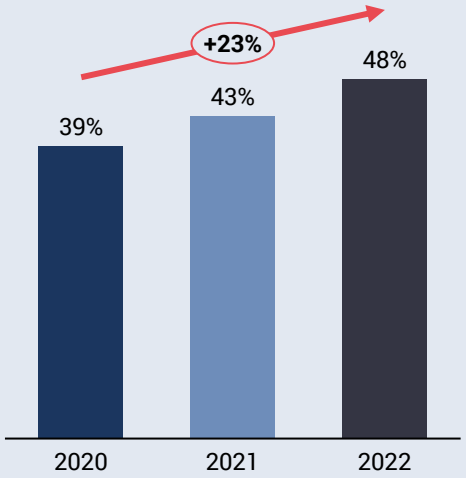
> Pour les **sociétés françaises cotées**, on observe un **recul moyen de 9% du cours de Bourse** suite à une cyberattaque *(source : Bessé)*

> En France, les **ETI** voient leur **risque de défaillance augmenter de 80%** à la suite d'une cyberattaque *(source : Bessé)*

Toutes les entreprises sont confrontées à ces risques

Une tendance mondiale…

L'évolution du pourcentage d'entreprises touchées par au moins une cyberattaque au cours des 12 derniers mois



Source : Hiscox Cyber Readiness Reports

… à laquelle la France n'échappe pas :

- Parmi les **160 entreprises interrogées**, **41%** ont subi **au moins une** cyberattaque au cours des **12 derniers mois**
- **17%** des entreprises ont été touchées par **plus de 3** cyberattaques au cours des **12 derniers mois**

Et bien que les entreprises ne soient pas touchées avec la même intensité, la menace plane sur chacune d'entre elles :

21%

des **TPE / start-ups** interrogées ont subi **au moins une** attaque au cours des **12 derniers mois** alors que ce sont les entreprises **les moins touchées.**

*« Les entreprises réalisant un **chiffre d'affaires entre 100 000 et 500 000$** subissent maintenant **autant d'attaques** que celles qui réalisent entre **1 et 9 millions de $ de chiffre d'affaires**. »*
(Hiscox Cyber Readiness Reports)

Verbatim

« Toutes les entreprises ont compris que la cybersécurité était un enjeu important de leur activité, malgré les disparités induites par leur secteur et leur taille. »

Proofpoint

Les dégâts matériels des cyberattaques peuvent être majeurs, il s'agit donc pour les entreprises de réagir en conséquence afin de les limiter

Les cyberattaques sont **particulièrement dommageables** pour les entreprises. Face à une cyberattaque la **réaction à avoir** pour limiter les dégâts doit **être rapide** et s'articule en **3 temps :**

1

Détecter les intrusions

- Lorsqu'une entreprise se fait attaquer, l'un des risques majeurs est qu'elle **ne détecte pas l'intrusion**
- Or, si tel est le cas, les dégâts risqueront d'être **décuplés**, les cyberattaquants pouvant exploiter les brèches plus longtemps

“ Verbatim ”

« Certaines entreprises ne savent pas qu'elles ont été victimes d'une cyberattaque, ou ne la considèrent pas comme tel. »

Proofpoint

2

Stopper l'attaque

- La première réaction suite à une cyberattaque doit être de **stopper le cyberattaquant** ou bien de s'assurer qu'il ne puisse plus faire de dégâts
- Or, afin de stopper l'invasion du cyberattaquant, le réseau peut être **temporairement hors service**, ce qui impacte l'activité de l'entreprise
- Les dégâts infligés par une cyberattaque seront d'autant plus importants que le temps de réaction sera long. Or, le **temps moyen de réponse à une cyberattaque** atteint **20,9 heures** *(Source : Deep Instinct)*

3

Évaluer les dégâts

Parmi les **65** entreprises interrogées ayant été **touchées** par au moins une cyberattaque au cours des 12 derniers mois, **17%** d'entre elles ont fait face à du **vol de données** et **14%** à de la **destruction de données.**

Les attaques sont-elles plus susceptibles de menacer vos données ou les données de vos clients ?

20 répondants - %

La crise du Covid a fragilisé les systèmes d'information des entreprises

2.3

ESSEC
Solutions Entreprises

Si la crise sanitaire a fortement augmenté le risque de cyberattaques pour les entreprises…

Le Covid-19

Le Covid-19 a été à l'origine **d'une refonte de la structure du réseau d'entreprise**.

L'imprudence

Dans un contexte de crise, **l'efficacité du phishing s'est accrue**. Le Covid-19 a en effet été un **prétexte des cyberattaquants visant à convaincre les victimes de cliquer sur les liens** (en insinuant par exemple que leur contenu était lié à des mesures sanitaires).

Le télétravail

Son usage s'est imposé dans toutes les sociétés, et a eu 2 effets majeurs :

> **Une exposition plus importante** aux cyberattaques du fait du passage en ligne induit par le télétravail
> **Une augmentation de la vulnérabilité** des systèmes du fait du manque de protection des outils à distance

> Le **nombre de cyberattaques** envers les entreprises a **augmenté de 13%** en **2021** *(Source : Orange Cyberdefense Security Report)*

> Les **méthodes des cyberattaquants** se sont améliorées

> Le télétravail a mis a mal la **continuité numérique** des entreprises, augmentant parfois les dégâts des cyberattaques

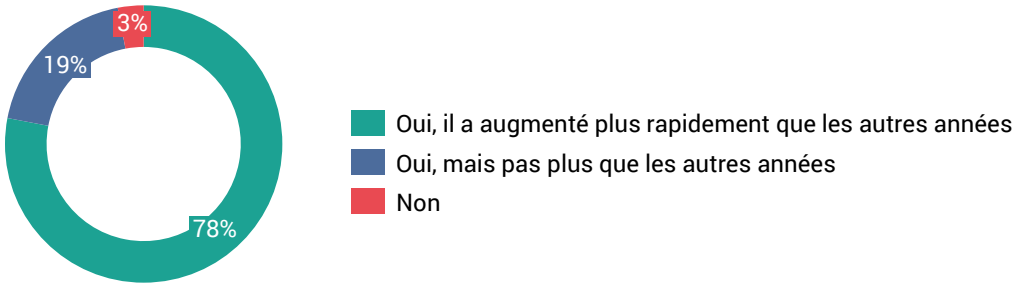
« L'impact de la pandémie Covid-19 sur la cybercriminalité a été le plus visible et le plus frappant par rapport à d'autres activités criminelles »

Rapport d'Europol

… Elles n'ont pas toutes pris conscience de son impact

Le risque de cyberattaques a-t-il augmenté au cours de ces 3 dernières années selon vous ?

160 répondants - %



> Parmi les **125 RSSI** ayant répondu « Oui, il a augmenté plus rapidement que les autres années », **70%** d'entre eux estiment que cette augmentation est **due en majeure partie à la crise sanitaire**

> Ainsi, sur les **160 RSSI** interrogés, **seulement 54%** d'entre eux estiment que le risque de cyberattaques **s'est accru plus rapidement ces dernières années, du fait de la crise sanitaire**

46%

des RSSI interrogés n'estiment pas que le risque de cyberattaques s'est accru ces dernières années, du fait de la crise sanitaire. Presque **une entreprise sur deux** n'a donc **pas conscience de l'impact du Covid-19**.

Les raisons de l'augmentation du risque qui ressortent le plus, outre les récentes crises :

155 répondants - %

Nouvelles technologies

Facilité des attaques

Hausse de la rentabilité

Professionnalisation des cyberattaquants

Digitalisation des entreprises

Tensions géopolitiques

“ Verbatim ”

*« Les entreprises **n'appréhendent pas suffisamment** bien l'augmentation du risque liée aux récentes crises. »*

Un Major Account Manager chez Proofpoint

L’infogérance : un enjeu stratégique pour les entreprises

ESSEC
Solutions Entreprises

2.4

L'infogérance : un enjeu majeur des années à venir sur le marché de la cybersécurité

L'infogérance c'est :

L'externalisation
appliquée au domaine des systèmes d'information

31,6
milliards de dollars à l'échelle mondiale

8%
de croissance annuelle prévue jusqu'en 2025

Elle est classée en 3 catégories :

La gestion d'infrastructures
Par exemple la maintenance d'un parc informatique, de l'hébergement de serveurs, de la supervision d'équipements réseau ou de solutions de sauvegarde, etc.

La gestion des applications
Cela correspond aux activités de support fonctionnel, de maintenance préventive ou corrective, et de gestion des évolutions.

L'hébergement de service
Le prestataire héberge pour le compte de son client une application utilisée comme un service (site web par exemple). Le client perd la gestion de l'application et de ses données.

Les étapes pour réaliser un appel d'offre réussi et sécurisé d'après l'ANSSI :

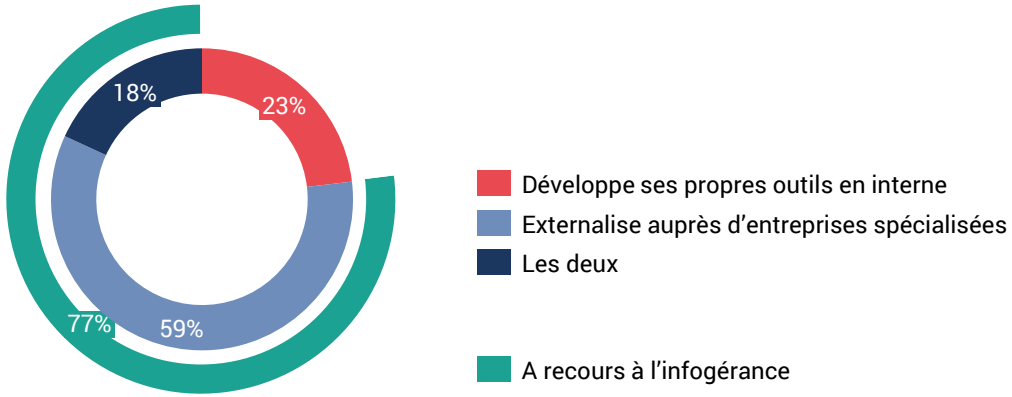
- **Apprécier les risques et déterminer les objectifs de sécurité** grâce à une étude préalable sur son propre système d'information
- **Rédiger le cahier des charges** concernant les exigences et les clauses de sécurité et récupérer les **Plans d'Assurance Sécurité** des différents candidats (il engage l'entreprise à exécuter ses obligations en termes de sécurité des systèmes d'information)
- **Choisir le prestataire**. Il appartient au donneur d'ordres de s'assurer de la recevabilité du Plan d'Assurance Sécurité fourni par les candidats
- **Mettre en place des audits de sécurité** réguliers pour s'assurer que les exigences de sécurité soient satisfaites par les dispositions prises par le prestataire

Malgré la tendance à l'externalisation des services de cybersécurité, les décisions sont toujours majoritairement prises en interne

Ne pouvant pas complètement maîtriser les risques cyber, les entreprises se tournent vers l'externalisation…

Votre entreprise :

147 répondants



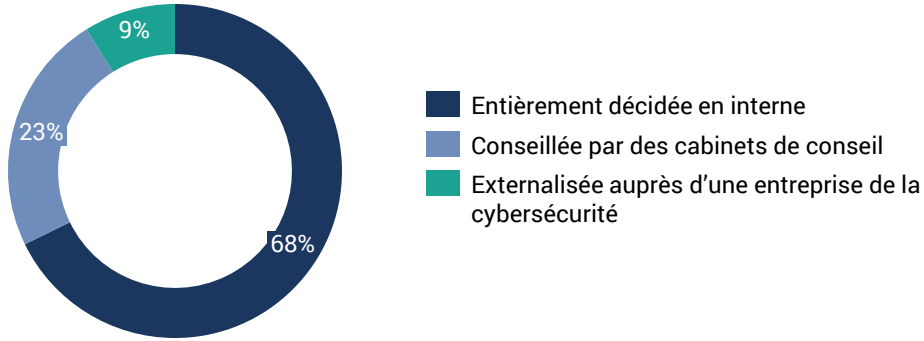
> **77%** des RSSI interrogés ont déclaré payer des licences auprès d'entreprises de cybersécurité pour avoir accès à leurs outils et à leurs services

> Ce résultat confirme la tendance à **l'accroissement du recours à l'infogérance** au sein des directions des services informatiques. **59%** des entreprises externalisent au complet leur cybersécurité

… Cependant, le cœur des décisions stratégiques en termes de sécurité informatique est maintenu en interne

L'orientation de la politique de cybersécurité de votre entreprise est :

147 répondants



> L'un des risques majeurs du recours à l'externalisation est **la perte de la gouvernance** de ce secteur pourtant stratégique

> Cependant, nous avons pu observer qu'à **68%** la politique de cybersécurité était **entièrement décidée en interne**. On retrouve dès lors un équilibre sain entre infogérance et décisions stratégiques prisent en interne

« L'internalisation et l'externalisation ne sont pas antinomiques, elles sont complémentaires. » Palo Alto Networks

Internalisation des pratiques de cybersécurité au sein de la sécurité des systèmes d'information

- Relève le niveau de **compétence interne** en sécurité
- **Contrôle stratégique** de la sécurité du réseau
- **Permet une indépendance technologique**

- **Engagement humain trop important** pour la majorité des entreprises
- **Incapacité d'utilisation** de certaines technologies
- Trop **onéreux**

Externalisation de la gestion de la cybersécurité auprès d'entreprises spécialisées

- Remédie au **manque de ressources humaines** et de compétences
- Permet une **maitrise des coûts**
- Propose l'utilisation de **technologies complexes**

- **Perte du savoir-faire** des équipes en interne
- **Perte de maîtrise** du système d'information
- **Risque de l'hébergement mutualisé** qui lie les différents services

- **L'infogérance s'impose de plus en plus** aux directions des systèmes d'information car elle présente de nombreux avantages. Cependant, il est nécessaire de **ne pas en confier la totalité à des sociétés extérieures** car cela serait risquer une **perte directe de pouvoir** sur la gestion des risques stratégiques

- Ainsi, pour se diriger vers l'externalisation, il est nécessaire d'être **précautionneux**. Pour cela, **l'Agence Nationale de la Sécurité des Systèmes d'Information** (ANSSI) propose un **guide de l'externalisation** qui aide à maîtriser les aspects de sécurité dans les choix des prestataires extérieurs

L’impact sur les entreprises et leurs réponses face aux risques

3

ESSEC
Solutions Entreprises

Toutes les entreprises sont confrontées aux risques de cyberattaques

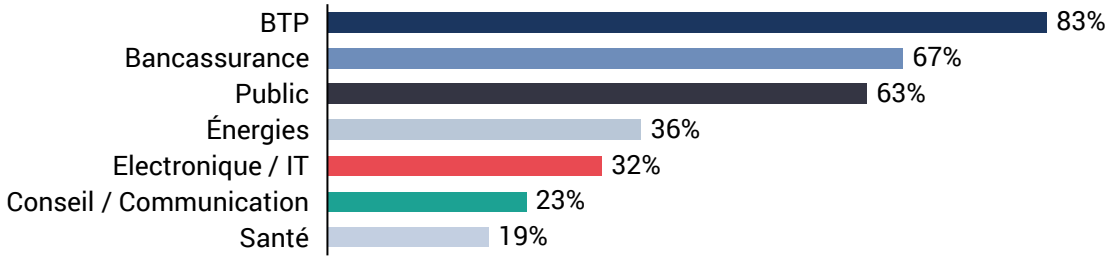
3.1

ESSEC
Solutions Entreprises

Si l'on observe des disparités entre les secteurs d'activité, aucun n'est épargné par les cyberattaques

Les entreprises dont l'activité est liée au BTP ou à la bancassurance et les entreprises du secteur public semblent être plus confrontées aux cyberattaques

Pourcentages d'entreprises interrogées ayant subi au moins 1 cyberattaque au cours des 12 derniers mois par secteur :



> Le choix de ces cibles privilégiées s'explique en grande partie par **l'appât du gain** des cyberattaquants, choisissant des secteurs dans lesquels il est possible de **voler des données sensibles** en grande quantité et où la **liquidité** est importante

> En outre, les entreprises qui exercent une activité au sein d'un **secteur stratégique** doivent avoir une cybersécurité très renforcée : les cyberattaques touchent souvent toute la **chaîne de logistique**, il faut donc en particulier que **les PME fournisseuses**, qui peuvent être un point d'entrée « facile » pour les cyberattaquants, aient une **part importante de leur budget consacrée à la cybersécurité**

Mais le secteur d'activité n'est pas nécessairement corrélé au nombre de cyberattaques subies : le risque 0 n'existe pas, quelle que soit l'activité de l'entreprise

40%

des entreprises interrogées du **secteur secondaire** ont été victimes d'**au moins une cyberattaque** au cours des 12 derniers mois

des entreprises interrogées du **secteur tertiaire** ont été victimes d'**au moins une cyberattaque** au cours des 12 derniers mois

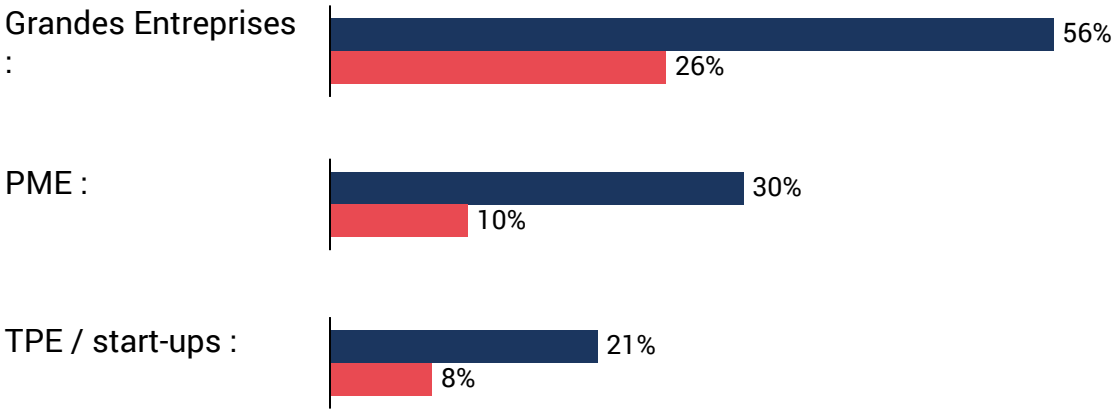
Verbatim

*« Toutes les entreprises, **quel que soit leur secteur d'activité**, sont confrontées à la problématique de la **cybersécurité**. »*

Un Major Account Manager chez Proofpoint

Les grandes entreprises restent plus touchées par les cyberattaques que les plus petites structures

Des différences marquées en fonction de la taille des entreprises…



Bien que **toutes les entreprises** soient **touchées**, il existe une **corrélation positive** entre la **taille** d'une entreprise et le **nombre de cyberattaques** qu'elle subit.

- Au moins 1 cyberattaque
- Plus de 3 cyberattaques

… Qui cachent toutefois une hausse de la vulnérabilité des petites entreprises

> **81%** des RSSI de **PME** interrogés estiment **que le risque de cyberattaques a augmenté** plus rapidement qu'habituellement au cours de ces **3 dernières années** pour leur entreprise contre **77%** pour les RSSI de **Grandes Entreprises**. On observe généralement une hausse des attaques envers les PME

> Or, ce sont aussi les entreprises qui investissent le moins dans la cybersécurité : **82%** des RSSI de **Grandes Entreprises** interrogés affirment que leur entreprise **investit de manière non négligeable** dans la cybersécurité (politique de cybersécurité développée, recherche des équipements les plus performants possibles) **contre seulement 62%** pour ceux de **PME** et **33%** pour les **TPE / start-ups**

Ce que les entreprises mettent en place

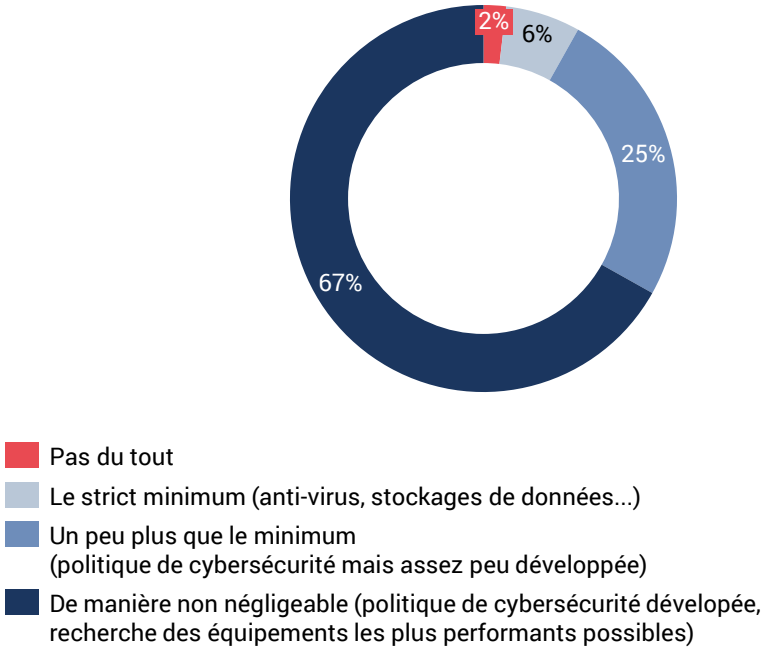
ESSEC
Solutions Entreprises

3.2

Les entreprises investissent de plus en plus dans la cybersécurité…

Votre entreprise investit-elle dans la cybersécurité ?

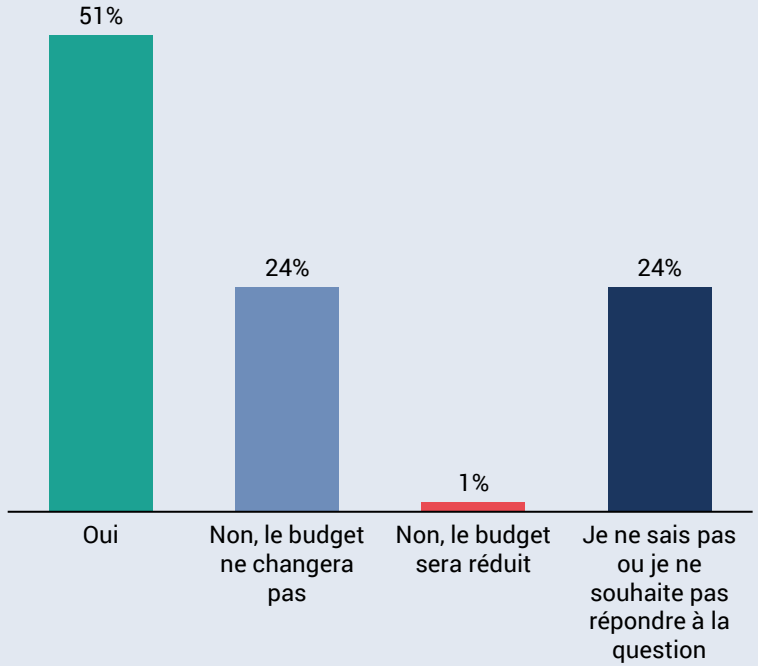
160 répondants - %



> **67%** des RSSI interrogés estiment **investir de manière non négligeable** dans la cybersécurité. Si on élargit aux entreprises ayant une politique cyber, cette proportion monte à **92%**

Votre entreprise a-t-elle prévu une hausse de ce budget cette année par rapport à 2021 ?

160 répondants - %



> En 2022, **51%** des entreprises comptaient augmenter leurs dépenses en cybersécurité contre **45% en 2020** (*IDC France*)

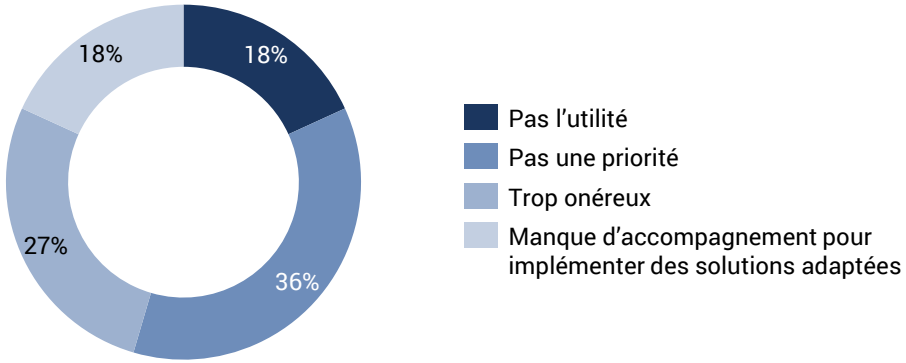
> Ces résultats font état d'une **conscience accrue des risques** encourus par les dirigeants et **surtout depuis la crise sanitaire**

… Cependant, entre réticence à l'investissement et manque de moyen, toutes les entreprises ne sont pas préparées face aux risques cyber

> Malgré l'augmentation des investissements dans la majorité des entreprises, une étude de IDC France révèle que **40%** des entreprises restent toujours « **non armées** » face aux cyberattaques : **38%** des entreprises interrogées n'ont **pas défini de procédures** dans le cas où elles seraient attaquées

Pourquoi ne pas investir plus dans ce domaine ?

160 répondants - %



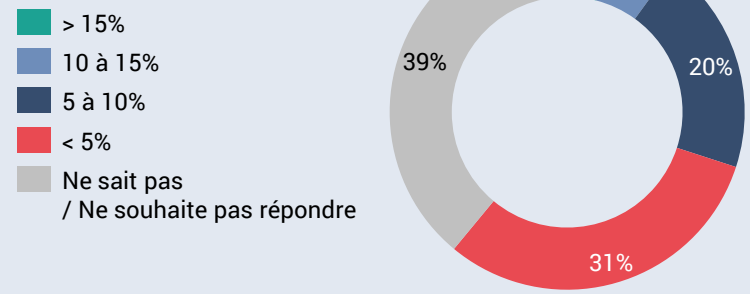
> Ceci s'explique par les choix des entreprises de ne **pas se protéger**
> Les résultats nous indiquent que **les raisons sont multiples** et il est donc nécessaire que les entreprises qui proposent des solutions soient multi-spécialisées pour **favoriser l'investissement** dans la cybersécurité

La problématique du budget

> Le manque d'investissement s'explique également par un **manque de budget** alloué à la cybersécurité. Pour 27% des RSSI interrogés, les solutions sont **trop onéreuses**

Quelle part du budget de votre DSI est allouée à la cybersécurité ?

160 répondants - %



> De plus, selon les recommandations de l'ANSSI, les entreprises devraient allouer au **moins 5% de leur DSI** à la cybersécurité mais encore aujourd'hui **31% des sociétés n'atteignent pas ce chiffre**

Source : Étude par Infopro Digital pour Stormshield, 2021

Comment réagir à une cyberattaque

3.3

ESSEC
Solutions Entreprises

Les bons gestes à adopter en cas de cyberattaques

1

Qualifier le signalement pour définir une vision de la situation fiable

> La première étape du traitement d'un incident est de **le qualifier**

> Pour ce faire, il est nécessaire **d'identifier les sources d'informations et les anomalies** qui peuvent y être associées

> L'objectif de cette étape est de **définir une vision de la situation la plus fiable possible**

> Une fois les dysfonctionnements identifiés, il est nécessaire de **s'orienter pour identifier les impacts potentiels de l'attaque et les actions à mener**

2

Réagir de manière efficace à la menace entrante

> Lors d'une attaque, il est nécessaire **d'établir un plan d'action clair afin d'être le plus efficace**

> Dans un premier temps, il faut **synthétiser le sûr et l'incertain** sous une forme concise afin de notifier les décideurs puis de **prendre conseil auprès de spécialistes** pour prendre des décisions éclairées

> Il faut ensuite **agir** en prenant les **premières mesures : préserver les traces** de l'attaque, **mobiliser les équipes internes,** etc.

3

Obtenir de l'aide auprès d'organismes spécialisés

> **L'ANSSI** et le **CERT-FR** (Centre gouvernemental de veille, d'alerte et de réponse aux attaques informatiques) peuvent apporter **leur expertise** en cas d'attaque

> Mais généralement ils redirigent vers des **prestataires de confiance spécialisés**. Si le problème persiste il faudra se diriger également vers des **prestataires de solutions SI**

> Si vous bénéficiez d'une **assurance, il faut signaler au plus vite l'incident**

4

Faire une déclaration des faits afin de les répertorier et de s'en protéger dans le futur

> Les cyberattaques sont en grande majorité **des infractions** qu'il faut **signaler aux autorités compétentes**

> **L'ANSSI** répertorie les attaques au travers d'un **formulaire** disponible sur son site

> Il est possible de **déposer plainte** afin de déclencher une enquête auprès de **la Police ou de la Gendarmerie**

> Les incidents affectant les **données personelles** doivent être **signalés à la CNIL**

Source : Recommandations de l'ANSSI

Les leviers d’action des entreprises pour gagner en sécurisation de leurs SI

4

ESSEC
Solutions Entreprises

Se renseigner sur les cyberattaques ainsi que les nouvelles tendances

4.1

ESSEC
Solutions Entreprises

Se renseigner sur les cyberattaques et les évolutions pour mieux appréhender sa propre sécurité

Il existe des **moyens simples de se renseigner** sur les récentes évolutions dans le domaine de la cybercriminalité. Cela permet de **se prémunir contre les nouvelles attaques** et de déceler **les tendances** pour mieux s'en protéger.

Les indices

Des indices ont été créés ces dernières années pour **mesurer le niveau et la perception de l'insécurité dans les entreprises**. Ils sont très différents les uns des autres dans leur méthode de calcul et dans ce qu'ils mettent en avant, il faut donc **bien les sélectionner**.

Exemples d'indices :

> **Global Cybersecurity Index –** C'est une référence fiable qui mesure l'engagement des pays en matière de cybersécurité

> **IBM 2020 cyber security intelligence index –** Cet indice analyse des milliards de données pour exposer les statistiques et les tendances les plus urgentes en matière de sécurité

> **Cybersecurity Index (WTCBR) –** C'est un indice qui vise à suivre les innovations en matière de cybersécurité réalisées par des entreprises sur les marchés publics

Les rapports

Les rapports d'activité sont des éléments **revenant en général sur l'année précédente**, mettant en avant les **incidents majeurs, les tendances observées, les récents développements,** etc.

Les rapports de dispositifs gouvernementaux :

> **Chiffres et tendances des cybermenaces, rapport d'activité 2021 de Cybermalveillance.gouv.fr**

> **Rapport d'activité 2021 de l'ANSSI**

> **Rapport d'activité 2021 de la CNIL**

Les rapports d'initiatives privées :

> **2022 Thales Data Threat Report**

> **Multiple rapports de Cisco**

Les tableaux de bord

Les tableaux de bord permettent de **visualiser les cyberattaques en temps réel**. Leur intégration dans les campagnes de formation est une approche à la fois **ludique et pédagogique** pour sensibiliser les équipes.

Exemples de cartes interactives :

> **Kaspersky Cyberthreat Real-Time Map**

> **Arbor Networks DDoS Digital Attack Map**

> **SonicWall Live Cyber Attacks Map**

> **NetScout Omnis Theat Horizon**

> **Bitdefender Live CyberThreat Real-Time Map**

> **Talos Cyber Attack Map Top Spam & Malware Senders**

Faire appel à des organismes spécialisés pour établir un diagnostic

4.2

ESSEC
Solutions Entreprises

Le choix des solutions à adopter doit être guidé par un audit de cybersécurité

Les écueils des entreprises lorsqu'elles commencent à investir

> La **mauvaise orientation des investissements** en cybersécurité est un écueil qui ressort des entretiens avec les professionnels du secteur. Les entreprises ont trop tendance à être victimes d'un **« effet de mode »** en investissant dans **les solutions les plus utilisées** par les autres acteurs de leur marché

> Or, s'il peut exister des **« indispensables »** en matière de cybersécurité, **les besoins ne sont pas les mêmes** selon les entreprises (utilisation d'un cloud, données sensibles etc.), et chacune d'entre elles doit investir dans des solutions qui lui sont **adéquates**

> Les entreprises doivent donc avant tout **réaliser un audit de cybersécurité** afin de prendre conscience des failles potentielles et existantes et d'investir sur des **solutions adaptées**

Les étapes à suivre pour investir dans la cybersécurité

Audit de cybersécurité

Il est essentiel de réaliser un audit afin de **comprendre** quels sont les **besoins spécifiques** à l'entreprise et **d'éviter les investissements caducs**.

Choix d'une solution adaptée

Suite à un audit, une entreprise peut faire appel soit à un **cabinet de conseil spécialisé**, soit à un **éditeur** afin d'orienter en conséquence son investissement.

Formation des collaborateurs

Il s'agira de former ses collaborateurs non seulement à **l'utilisation des nouveaux outils**, mais aussi aux **réflexes à adopter en cas de cyberattaque**.

L'Agence Nationale de la Sécurité des Systèmes d'Information, une référence gouvernementale en termes de cybersécurité à l'écoute des entreprises

Une intervention efficace en cas d'attaque

- Le site de l'ANSSI propose des **conseils pratiques** à mettre en place lors d'une cyberattaque
- Il oriente directement vers les **prestataires susceptibles de répondre aux problèmes rencontrés**. Ainsi, il est facile d'identifier les solutions pour remédier à cette attaque et pour se reconstruire
- Suite aux attaques ou en prévention, l'ANSSI propose également des **audits** qui sont essentiels avant d'entamer tout investissement dans la cybersécurité

Elle dirige un programme d'incubation

- L'ANSSI est à la tête d'un **programme de création régionale de CSIRT**
- Un **CSIRT régional** (Computer Security Incident Response Team) est un centre de **réponse aux incidents cyber** au profit des entités implantées sur le territoire régional
- Cet accompagnement est **méthodologique**, **financier** et dure 5 mois. Le but final étant de **mettre en réseau** les nombreux CSIRT français pour bénéficier de l'expertise des pairs

Elle pilote le volet cybersécurité du plan France Relance

- À l'échelle nationale, **136 millions** d'euros ont été mobilisés pour renforcer le **niveau de cybersécurité** des acteurs publics en 2020
- L'ANSSI a pour mission de proposer des offres de **services personnalisés** en fonction des organismes et ainsi **renforcer la sécurité** de leurs systèmes d'information
- Actuellement **828 organismes** en sont bénéficiaires mais il est encore possible d'y participer

“ Verbatim ”

*« Si je devais donner un conseil, ce serait de **se rapprocher de ces organismes pros** qui parlent un **langage simple**, qui assurent un suivi et qui sont une source de veilles et de **recommandations inépuisables.** »*

Jacques Barbezange, Directeur général des services SMICA

Choisir une solution adaptée à son entreprise et oser de nouvelles technologies

ESSEC
Solutions Entreprises

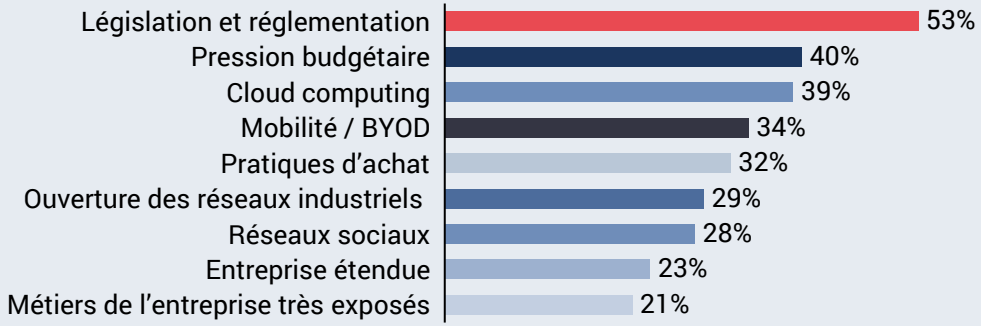
4.3

Si la pression budgétaire dicte souvent les stratégies de cybersécurité, les solutions ne sont pas choisies selon leur prix mais selon leur efficacité

- **68%** des entreprises interrogées qui ont une réelle **politique de cybersécurité** affirment que son **orientation** est **entièrement décidée en interne**
- À l'inverse, **23%** des RSSI interrogés affirment que l'orientation de la politique de cybersécurité de leur entreprise est **conseillée par des cabinets de conseil** et **9%** que la leur est **externalisée auprès d'une entreprise de cybersécurité**

- **77%** des RSSI interrogés dont l'entreprise investit de manière non négligeable dans la cybersécurité ont **recours à l'infogérance** en payant des licences auprès d'entreprises de cybersécurité pour avoir accès à leurs outils, parmi lesquels **59%** ne développent **aucune solution** de cybersécurité **en interne**

Quels sont les trois éléments qui influencent le plus votre stratégie de cybersécurité ?



Source : Le nouveau paradigme de la cyber sécurité de PAC

Quel est le critère le plus important selon vous pour choisir sa solution de cybersécurité ?

157 répondants - %

Les essentiels de la cybersécurité : protéger sa messagerie, son réseau, détecter les menaces et réparer les dégâts

Sécurité de messagerie

> La **première étape** dans la constitution d'une cybersécurité pour une entreprise doit être la **protection de la messagerie**

> En effet, l'e-mail professionnel est une des méthodes d'entrée les plus courantes pour les cyberattaquants. En **2022**, **40% des intrusions** se faisaient par l'**e-mail professionnel** (*Source : Hiscox 2022 Cyber Readiness Report*)

> Il est préférable de renforcer la protection qu'octroie une **sécurité de messagerie** en réalisant des **formations** auprès des collaborateurs

Firewall

> La mise en place d'un **Firewall** constitue souvent une **base** à la **protection de son réseau**

> Le Firewall agit comme un **filtre** sur le trafic des données entre les différentes zones de confiance d'une entreprise (**réseau interne** et **internet**)

EDR

> La mise en place d'un **EDR** (**Endpoint Detection and Response**) a pour objectif de **détecter les menaces** quant à la sécurité informatique des équipements numériques d'une entreprise

> Or, la **détection des menaces** est essentielle afin de **stopper les cyberattaques**. En effet, certaines cyber-intrusions ne sont **pas visibles** et donc plus vite elles sont détectées, moins elles causeront de dégâts

> Toutefois, une cybersécurité n'est pas infaillible, un **risque résiduel** persiste. Il peut donc être préférable de souscrire à une **cyber-assurance**

> Face à l'**augmentation** effrénée du nombre de **cyber-attaques**, les cyber-assurances exigent désormais que leurs clients mettent en place des solutions de cybersécurité considérées comme essentielles telles que la **double authentification**

Le Cloud, dont l'usage est de plus en plus primordial, nécessite d'être sécurisé

La protection du cloud d'une entreprise doit prendre une part de plus en plus importante dans sa politique de cybersécurité…

79%

des **victimes de ransomware** indiquent que ces attaques ont été le résultat d'une **vulnérabilité** et d'une **mauvaise configuration** du **Cloud** *(2019 IDC Info).*

« Le cloud est désormais la première porte d'entrée des cyberattaques ». **41%** des cyberattaques de **2022** venaient d'une **intrusion** via le **Cloud** *(Hiscox).*

… Alors qu'elle est encore trop souvent négligée

44%

des RSSI **ne considèrent pas** la sécurité du Cloud comme une **priorité forte** *(2019 IDC Info).*

La sécurisation d'un Cloud relève souvent d'une responsabilité partagée entre client et fournisseur :

> Dans la plupart des cas, il s'agit de faire confiance à un fournisseur **Iaas** qui prendra **en charge** en grande partie la **sécurité** des données du Cloud, et qui sera responsable du **chiffrement des informations**. Il s'agira de choisir un fournisseur **de confiance** ainsi que de **comprendre** le modèle de responsabilité partagée associé

> Mais quand bien même la sécurisation d'un Cloud est souvent prise en charge par un fournisseur, **certaines bonnes pratiques doivent être maintenues** : **formation** des utilisateurs, contrôle étroit de l'**accès** des utilisateurs, sécurisation des **Endpoints**, politique de sécurité de **mots de passe forts**

La stratégie Zero Trust, une manière efficace de prévenir les attaques

La statégie Zero Trust, qu'est-ce que c'est ?

> La sécurité Zero Trust part du principe que **les menaces sont permanentes en interne et externe** et que donc tout doit être contrôlé (les terminaux, utilisateurs, flux réseau) et ce, à toutes les étapes (authentification, autorisation, transactions, accès aux données) grâce à des mécanismes comme **l'authentification multi-facteurs**

> La confiance est vue comme un risque. Ainsi, toutes les demandes sont traitées comme si elles provenaient d'un **réseau ouvert non sécurisé**

Les avantages d'une sécurité Zero Trust

> **Défense fiable** contre les attaques en tout genre

> **Protection solide des données,** qu'elles soient stockées dans les bases de données internes ou dans le cloud

> **Amélioration de la sécurité des appareils connectés** utilisés lors du télétravail

> **Réduction de la superficie** de la zone de menace

> **Amélioration de la collaboration** avec les clients et **gagner leur confiance**

L'authentification multi-facteurs

Les solutions apportées par la stratégie Zero Trust peuvent **accorder ou refuser l'accès** en fonction des critères suivants :

> **L'identité** de l'utilisateur

> **L'emplacement géographique** de l'utilisateur

> La **demande d'accès** effectuée

> **L'heure de connexion**

> Le **système d'exploitation** utilisé et la version du firmware

> **La posture** de l'appareil

Les étapes pour construire un réseau solide

1

> **Cartographie du SI** et identification des faiblesses des réseaux-clés

2

> **Identification de la surface à protéger**

3

> Mise en œuvre de **technologies spécifiques**

4

> **Surveillance continue** du réseau afin de garder un œil sur les activités suspectes

> La stratégie Zero Trust est une solution particulièrement adaptée à la **digitalisation des systèmes d'information** et à leur **nouvelle mobilité**, notamment depuis la démocratisation du télétravail et l'accès aux logiciels professionnels depuis les smartphones

> Cependant, **il faut rester prudent** car la mise en place de cette solution est longue et nécessite **d'importants changements** qui, effectués partiellement, peuvent **fragiliser les systèmes d'informations** et donner un **faux sentiment de sécurité**

Le recours à l'Automatisation Robotisée des Processus (RPA) dans la cybersécurité : une révolution en devenir

De plus en plus de DSI se tournent vers **l'automatisation des processus** afin d'éliminer les tâches fastidieuses, de rationaliser les opérations et de réduire les coûts dans le but de **gagner en efficacité**. Le RPA peut également être vu comme une solution transitoire vers **l'automatisation intelligente** (l'intelligence artificielle), grâce à des outils d'apprentissage automatique (Machine Learning), qui peuvent **résoudre de nombreux problèmes.**

Les avantages du RPA

- Les employés peuvent **se concentrer sur d'autres activités**
- L'automatisation **complète des contrôles et applications de sécurité existants** en détectant les menaces émergentes
- Elle permet également de **mettre en évidence les récurrences** dans les attaques et les failles pour mieux s'en protéger
- Elle améliore le ciblage des attaques en **collectant, corrélant et analysant** de nombreuses **données de sécurité**
- Les modèles les plus avancés mettent en place des **stratégies de défense en prenant en compte l'actualité, les menaces,** etc.

Quelques étapes pour mettre en place l'Automatisation Robotisée des Processus dans son entreprise

1. **Informez-vous** et formez vos équipes aux **nouveaux enjeux de l'utilisation des nouvelles technologies** dans la cybersécurité
2. **Comprenez l'impact des nouvelles technologies** et développez des réponses appropriées en matière de gestion des risques
3. Évaluez comment les **changements dans l'environnement opérationnel** affecteront le **panorama des menaces** et les contrôles nécessaires, puis **adaptez les rôles et responsabilités de votre équipe** .
4. **Encouragez la conception** de nouveaux systèmes, technologies et cadres de contrôle afin de réduire les contrôles inutiles et **favoriser la prévention**
5. Développez une **stratégie progressive de mise en place des technologies d'IA** simples et efficaces en identifiant les opportunités
6. **Repensez votre stratégie cyber** en investissant dans l'expertise de professionnels en **interne ou en externe**

Source : Smart Cyber, Deloitte, 2019

Mettre en place des formations et sensibilisation auprès de ses employés

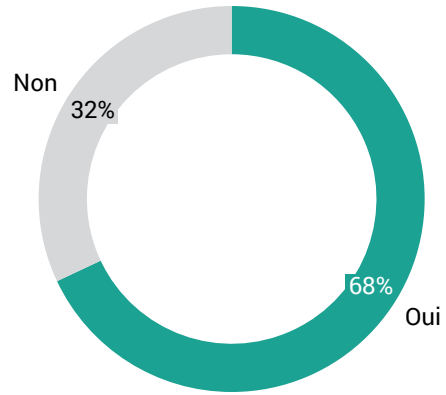
4.4

ESSEC
Solutions Entreprises

« La menace vient aussi de l'intérieur » : les collaborateurs au sein des entreprises ne sont pas assez formés pour se prémunir contre les menaces en ligne

Les salariés de votre entreprise sont-ils selon vous assez sensibles aux enjeux de la cybersécurité ?

160 répondants



> **32%** des RSSI pensent que les employés de leur entreprise ne sont pas assez sensibles à ce sujet

> **Parmi les 32%** d'entreprises n'organisant pas de formations en interne, **48%** considèrent que **leurs employés ne sont pas assez sensibles** aux enjeux de la cybersécurité

> Cependant des initiatives sont mises en place car **84%** des entreprises disent avoir **mis en place des formations** ou campagnes de sensibilisation dans ce domaine

“ Verbatims ”

*« **La formation est fondamentale** car l'espace de liberté laissé aux employés **est utilisé par les hackeurs** notamment pour faire du phishing. Il y a très peu d'attaques qui se déclenchent automatiquement. Très souvent **elles sont le résultat d'une action humaine** ayant débouchée sur une faille du système. »*

PaloAlto

*« L'homme est le **point de faiblesse** de la cybersécurité. »*

Proofpoint

*« **La sensibilisation des utilisateurs est l'un des plus grands enjeux à venir** car le risque est là. On peut anticiper tant bien que mal les nouvelles menaces mais tant que les utilisateurs ne sont pas conscients qu'il y a un vrai risque cyber, on ne peut pas se protéger correctement. **La menace vient aussi de l'intérieur**. »*

Cisco

« Mettre l'humain au cœur du dispositif de cybersécurité » : comment développer une culture interne de cybersécurité

Plusieurs moyens existent pour accéder à la formation contre les risques

Utiliser les ressources internes

Faire appel au personnel de l'entreprise déjà qualifié dans le domaine permet de faciliter l'accès à la formation, la personnaliser et de réduire les coûts d'intervention.

Faire appel à des entreprises spécialisées

Cette solution est plus onéreuse et demande plus de temps mais permet de bénéficier de supports de formation variés et originaux ainsi que d'une expertise dans le domaine.

Des thèmes simples et variés à aborder pour renforcer la sécurité informatique de son entreprise

Éviter le ransomware

Apprendre à reconnaître et se protéger des menaces

Reconnaître le phishing

Concevoir un mot de passe fort

Protéger les données de l'entreprise

Être prudent avec l'utilisation d'appareils connectés en dehors de l'espace de travail

Gérer ses mots de passe

Sécuriser ses applications

- La formation et la sensibilisation des collaborateurs aux enjeux de la cybersécurité est un **élément fondamental de la protection de l'entreprise**
- La grande majorité du temps, **les erreurs qui débouchent sur des cyberattaques** sont issues **d'erreurs humaines en interne. Les opérations « zero click » sont rares**
- La sensibilisation de tous les collaborateurs, **quel que soit leur degré de responsabilité** dans l'entreprise, permet de réduire les erreurs possibles et les responsabilisent face à leur utilisation des dispositifs numériques de l'entreprise

Expertise et références

5

ESSEC
Solutions Entreprises

Qu’est-ce qu’ESSEC Solutions Entreprises ?

ESSEC Solutions Entreprises est le 1er cabinet de conseil étudiant indépendant, composé de 10 étudiants du programme Grande École de l’ESSEC Business School

Le cabinet en chiffres

1er Cabinet de conseil étudiant en France

10 Chefs de projet et consultants

80 Études par an

36 Années d’expérience et de transmission

700 000 € De CA annuel

Nos partenaires

Une équipe de chefs de projet dédiés à vos projets

Étudiants à l’ESSEC, nos chefs de projet mettent leurs études entre parenthèses et consacrent une année à l’accompagnement de leurs clients.

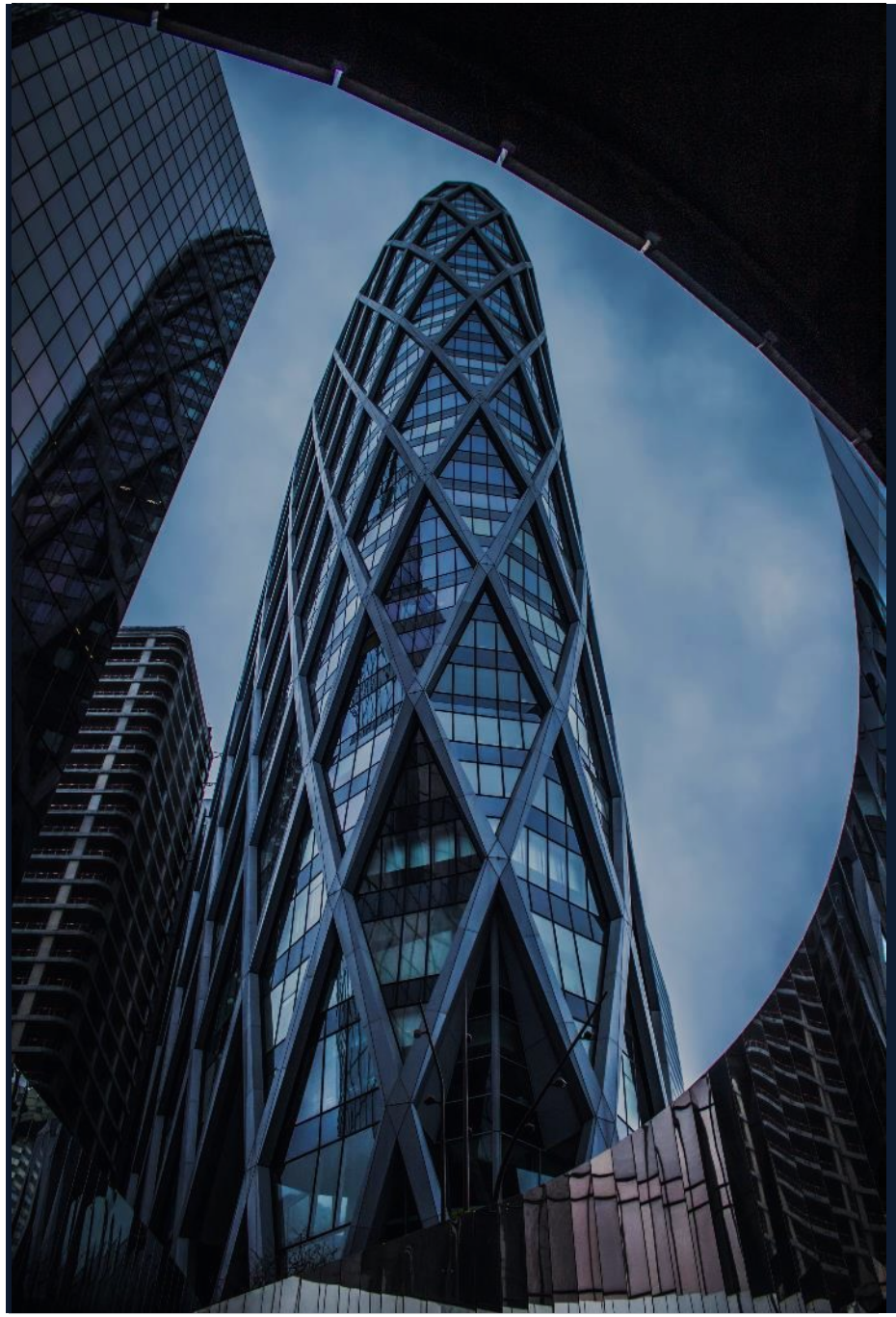
Un accompagnement complet, des données aux recommandations

Pour répondre à vos besoins, ESSEC Solutions Entreprises met en place un accompagnement complet, de la récolte et l’analyse de données à l’élaboration de recommandations stratégiques sur vos problématiques.

Une structure de l’ESSEC Business School

Tous nos chefs de projet sont étudiants en Master à l’ESSEC, et travaillent dans un milieu innovant, au contact de milliers d’étudiants et professeurs renommés.

Ils ont travaillé avec nous cette année



ESSEC
Solutions Entreprises

Rapport

Étude sur les enjeux actuels de la cybersécurité pour les entreprises

JULIEN GODARD
Chef de projet & Community Manager
+33 (0)7 87 87 87 87
j.godard@essecsolutionsentreprises.com

PAULINE TABOURET
Cheffe de projet & Responsable alumni
+33 (0)6 86 23 43 19
p.tabouret@essecsolutionsentreprises.com