#3



STORMSHIELD

Transformation numérique des entreprises :

La maturité à l'épreuve du réel ?

Baromètre de la transformation numérique des entreprises
réalisé en collaboration avec l'Usine Digitale
Édition 2020

Comme chaque année depuis trois ans maintenant, nous interrogeons **les entreprises et les organisations**, grandes, petites et moyennes, afin d'en savoir plus sur leurs projets numériques et leur sécurisation.

Comme chaque année ? Pas vraiment, vous vous en doutez. 2020 est déjà et restera une année particulière à tous les niveaux.

C'est pourquoi, dans cette troisième édition du baromètre de la transformation numérique, nous décryptons plus précisément les effets à court et moyen terme de l'actualité.

Sommaire

4 **Préambule : la transformation numérique « à marche forcée » a-t-elle eu lieu ?**

8 **Quand l'actualité affecte notre perception de la transformation numérique**

13 **Cybersécurité : des automatismes en place malgré les difficultés**

19 **Une stratégie de moyens contrastée**

25 **Conclusion**

Préambule

La transformation numérique « à marche forcée » a-t-elle eu lieu ?

Entre la grève massive dans les transports français fin 2019, la crise sanitaire internationale de la Covid-19 ou les enjeux organisationnels et sécuritaires liés au(x) confinement(s), les douze derniers mois ont mis les entreprises et les organisations à rude épreuve.

Nous avons cherché à mettre en lumière les dernières avancées en termes de transformation numérique de ces structures, et questionné le lien avec les événements de cette année, qui ont dans un même mouvement freiné beaucoup d'activités et engendré un télétravail massif.

Nous avons beaucoup parlé d'une transition numérique « à marche forcée », mais cette expression décrit-elle fidèlement ce que nous avons vécu ? Pour les entreprises réputées « matures » numériquement, ne s'agissait-il pas plutôt d'un test ?

Les résultats de notre enquête et les différentes interviews menées pour les éclairer dépeignent en effet des réalités très différentes. Difficile donc de plaquer sur 2020 une étiquette homogène, encore moins définitive.

Nous espérons néanmoins apporter des clés de compréhension pour tirer les premiers enseignements d'une crise toujours en cours à l'heure où nous écrivons ces lignes.

Les principaux chiffres 2020

Quels sont les projets de transformation numérique les plus déployés ?

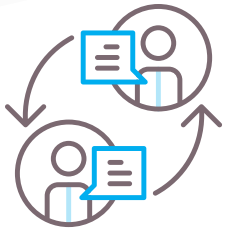
- **87 %** — **Les outils bureautiques** *(contre 79 % en 2019)*
- **77 %** — **Les outils de travail collaboratif** *(contre 62 % en 2019)*
- **75 %** — **Les services de communications unifiées** *(contre 63 % en 2019)*

Qui pilote les projets numériques au sein des entreprises ?

- **61 %** — **La direction des systèmes d'information** *(contre 55 % en 2019)*
- **44 %** — **La direction générale** *(contre 30 % en 2019)*
- **31 %** — **La direction R&D et innovation** *(contre 20 % en 2019)*

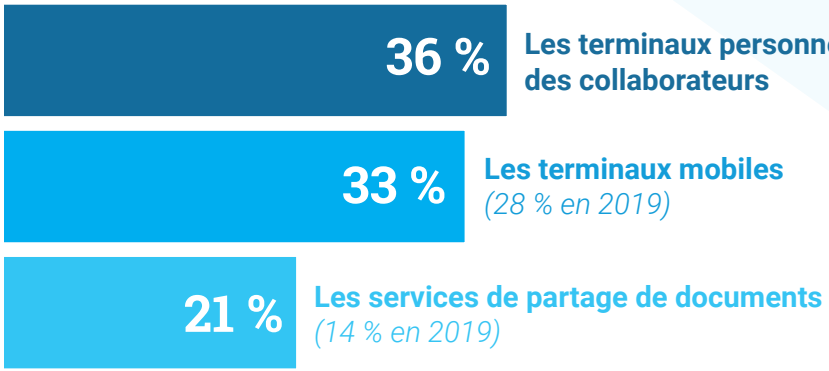
L'administration publique investit (enfin) dans le collaboratif

37 % des sondés de l'administration publique ont déclaré avoir déployé en urgence des outils de travail collaboratif pendant les événements (contre 20 % de l'échantillon global). Cet écart s'explique par **un retard important de la transformation numérique du secteur public français** de l'aveu d'un agent public sur trois.

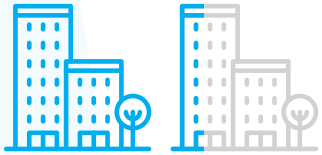


Les principaux chiffres 2020

Quels sont les éléments les plus vulnérables en matière de cybersécurité ?



Quelles solutions de sécurité sont en place dans les entreprises ?



Plus d'1 entreprise sur 2
déclare bénéficier d'une solution de Web Application Firewall (WAF)



Plus de la moitié de l'échantillon
dispose d'une solution de chiffrement de fichiers. Le chiffrement de mails est en place chez 39 % des répondants quand 17 % y réfléchissent.

90 %

Le taux de déploiement en antivirus, antispam ou anti-phishing, protection réseau et VPN avoisine ou dépasse désormais 90 %.

Les principaux chiffres 2020



La vulnérabilité des terminaux personnels des collaborateurs

Le besoin urgent de recourir au télétravail a forcé certaines entreprises à accepter que les terminaux personnels des collaborateurs soient utilisés. Un véritable sujet de sécurité, partagé par 36 % des personnes interrogées.



Les infrastructures industrielles et opérationnelles sur la bonne voie

Alors qu'elles figuraient parmi les éléments considérés les plus vulnérables dans notre précédente édition, la sécurisation de ces infrastructures progresse de 13 points cette année, portant à 66 % la part de répondants qui les estiment plutôt ou tout à fait sécurisées.

Vous souhaitez en savoir plus sur les solutions de sécurité à l'étude ou en cours de déploiement dans les entreprises et les organisations?

Rendez-vous en page 17 !

Partie 1

Quand l’actualité affecte notre perception de la transformation numérique

L'actualité de ces douze derniers mois aura mis en lumière les inégalités sociales et économiques qui traversent notre société. Parmi ces difficultés, il faut composer, selon le Forum Économique Mondial[1], avec une fracture numérique toujours plus profonde : la réalité des confinements aura en effet été bien différente en fonction du niveau d'équipement informatique, de la qualité de la connexion Internet ou tout simplement de la possibilité ou non d'exercer une activité professionnelle à distance.

Notre étude révèle que les inégalités se situent également au niveau des perceptions. Interrogés sur l'évolution de leur entreprise ou de leur organisation en matière de transformation numérique cette année, 70 % des répondants estiment que celle-ci a progressé. Particulièrement dans le secteur du commerce, forcé à se réinventer par l'enchainement des crises, en France avec les mouvements sociaux et grèves des transports, et à l'échelle internationale avec la crise de la Covid-19.

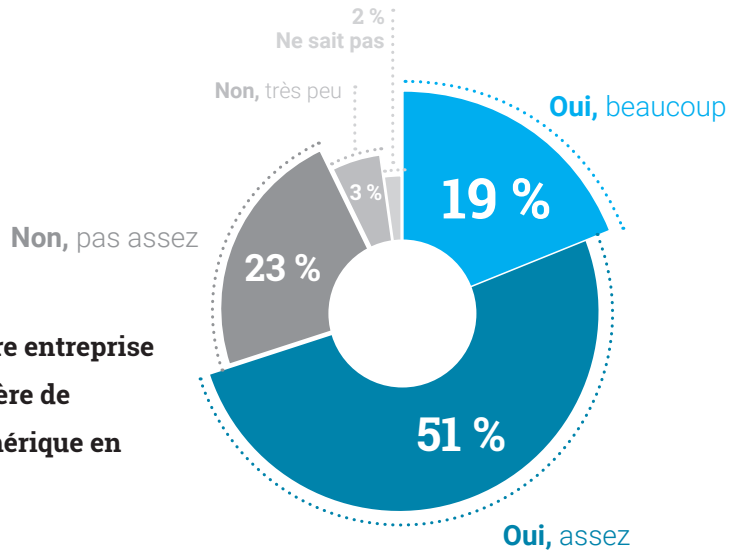
Ce n'est pas cependant le cas pour l'administration publique, où 44 % des sondés ont répondu par la négative. À l'exception de l'enseignement, où une majorité des sondés a perçu une progression que certains qualifieront de rattrapage ou de mise à niveau.

70 %

des répondants estiment que leur entreprise ou organisation a progressé en matière de transformation numérique

La proportion de répondants s'estimant en avance en matière de transformation numérique progresse de presque 10 points par rapport à l'an dernier, portée par les directions générales (51 %) plus que par les DSI qui restent plus prudentes (25 %). Parmi ces optimistes, 44 % opèrent dans l'industrie. Et si les confinements, véritables crash-test de la transformation numérique, n'avaient pas permis aux entreprises de ce secteur d'évaluer leur niveau de transformation et de se rassurer quant à leur préparation ?

Diriez-vous que votre entreprise a progressé en matière de transformation numérique en 2019 et début 2020 ?



[1] www.weforum.org/agenda/2020/08/5-things-covid-19-has-taught-us-about-inequality/

Quand l'actualité affecte notre perception de la transformation numérique

Tout n'est pas dû au virus ou aux grèves

61 % des personnes interrogées reconnaissent que les événements récents (mouvements sociaux, crise sanitaire) ont changé la perception de l'importance de la transformation numérique pour assurer la continuité des activités. Une prise de conscience qui n'est pas sans lien avec les messages passés par les DSI lors de la mise en place du télétravail par exemple.

La crise sanitaire aurait donc fait progresser la transformation numérique dans l'administration publique, la santé et l'action sociale. Côté industrie, Yann Bourjault, Directeur Transformation Digitale et Cybersécurité France de Schneider Electric, précise que « *le contexte sanitaire a surtout permis de prendre conscience du fait que la plupart des industriels n'avaient pas la capacité de superviser leurs usines à distance* ».

Charles Blanc-Rolin, Responsable des Systèmes d'information (RSSI) & *Data Protection Officer* (DPO) du Groupement Hospitalier du Territoire Cantal, pondère : « *pour un certain nombre de directions générales, notamment dans la fonction hospitalière, la priorité 2020 n'était clairement pas aux projets numériques ou à leur sécurisation* ».

On note également cette année un renforcement de la **perception de la fonction sécurité comme un « gendarme »**. Alors que près de la moitié des directions métiers interrogées en 2019 considérait la fonction sécurité comme un conseiller, cette proportion a chuté de 11 points en 2020. Elles sont maintenant 37 % à lui attribuer un rôle de gendarme (contre 26 % en 2019).

Néanmoins, 57 % des sondés ont déclaré que la progression de leur structure en matière de transformation numérique n'était pas due à la crise sanitaire. Gardons-nous donc d'imputer toutes les évolutions de l'année à l'actualité sociale ou sanitaire.

À titre d'exemple, Frédéric Leblond, RSSI du Port Boulogne Calais, a déployé une nouvelle solution VPN dès la fin d'année dernière. « *Nous avions les outils pour faire face à la situation du printemps 2020* », explique-t-il.

Comment se matérialise cette progression ?

Au classement des types de projets déployés, le trio de tête reste inchangé par rapport à notre baromètre 2019 : bureautique, communications unifiées et collaboratif.

Parmi les plus belles progressions, il faut souligner :

- les applications mobiles, dont le déploiement a augmenté de 18 points,
- la dématérialisation numérique, devenue réalité pour 54 % des répondants (+ 18 points également),
- la numérisation de la relation client, qui progresse quant à elle de 16 points.

L'exploitation de la donnée (39 %) et les plateformes métier (36 %) sont les solutions à l'étude ou en cours de déploiement les plus populaires.

Rappelons-nous que les entreprises et les organisations doivent composer avec un manque de visibilité accru par l'actualité incertaine, ce qui n'est pas sans conséquence sur les choix d'investissement. Pour Frédéric Leblond, RSSI du Port Boulogne Calais, cela signifie par exemple « *se concentrer en 2021 sur la mise en place d'un réseau informatique local dans le cadre des travaux d'extension du port* ».

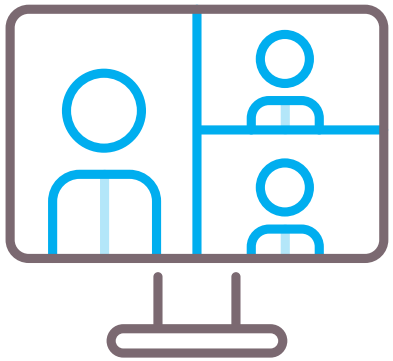
Yann Bourjault, Directeur Transformation Digitale et Cybersécurité France de Schneider Electric, a pu observer bon nombre d'investissements circonstanciels dans l'informatique bureautique pour permettre le télétravail. « *En informatique industrielle, les entreprises ont aussi investi pour permettre la prise en main à distance de l'usine, car la connectivité des outils de production est non seulement un enjeu pour la continuité d'activité, mais aussi pour la compétitivité. Cela se traduit par la mise en place d'accès distants sécurisés notamment à travers un VPN, un pare-feu, une solution de PAM* (Privileged Access Management), *etc.* ».

Quand l'actualité affecte notre perception de la transformation numérique

La transformation numérique est-elle linéaire ?

Pas à en croire les experts interrogés qui soulignent que l'on peut rapidement revenir en arrière. Sébastien Viou, Consultant Cyber-évangéliste chez Stormshield, ne décrit pas d'adoption massive du tout numérique. « *La généralisation du télétravail est vite retombée en France. Il y a eu une libération au niveau du télétravail, parfois subie par les DSI, mais en entreprise comme à l'école, beaucoup ont fait machine arrière dès qu'ils ont pu.* »

Frédéric Leblond, RSSI du Port Boulogne Calais, confirme : « *nous avons été contraints à mettre en place le télétravail pour garantir la continuité d'activité, mais ce n'est toujours pas dans les mœurs* ».



Toutefois, la transformation numérique ne se limite pas au télétravail, et certains changements pourraient s'inscrire dans la durée. Sébastien Viou souligne ainsi une « *accélération dans les secteurs peu poussés au changement par la concurrence. Par exemple, certains conseils municipaux ont pu se tenir en visioconférence, de même pour les assemblées générales des syndicats de copropriété. La signature d'actes notariés à distance a également été autorisée* ».

Partie 2

Cybersécurité : des automatismes en place malgré les difficultés

État des lieux de(s) menace(s)

« *Le cybercrime et les cyberattaques sont en croissance, motivés par l'appât du gain. La hausse des achats en ligne ou le télétravail ont augmenté la surface d'attaque, mais les cyber-criminels jouent également sur la fébrilité des utilisateurs en cette période anxiogène* », déplore Sébastien Viou, Consultant Cyber-évangéliste chez Stormshield.

En effet, malgré les crises, les cyberattaques ont continué d'augmenter et de se sophistiquer en 2020. L'ANSSI décrit ainsi deux fois plus de rançongiciels qu'en 2019, avec un pic de 28 cas en une semaine au mois de juin.

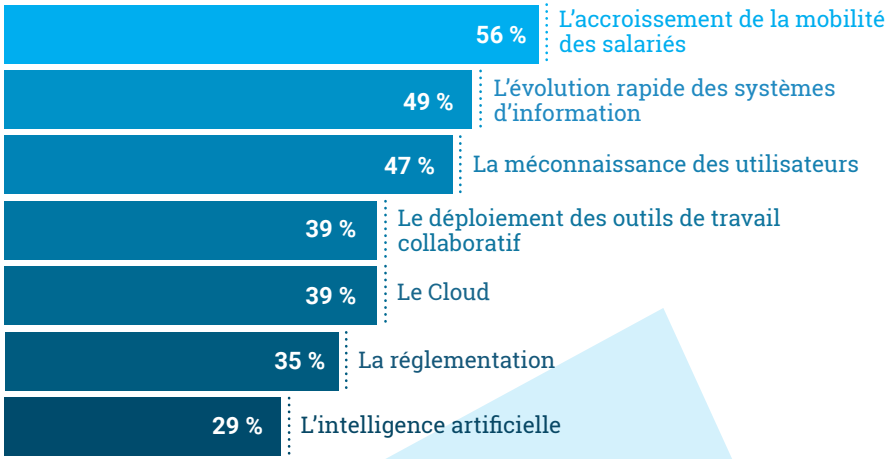
Le phishing reste un grand classique, même si Charles Blanc-Rolin, RSSI & DPO du GHT Cantal, insiste sur la forte adaptation au contexte : « *Les attaquants surfent clairement sur l'actualité. Entre les statistiques fantaisistes sur la progression de l'épidémie, les fausses boutiques en ligne de masques ou les escroqueries à la vente de vaccins, il a fallu que chacun soit particulièrement vigilant à sa boîte mail !* ».

En parallèle de ces attaques plutôt opportunistes, Jérémy, DSI d'un groupe agroalimentaire en Afrique de l'Ouest, complète : « *les cyberattaquants sont de plus en plus organisés. Ils disposent de plus de moyens et multiplient les exploits Zero-day* ».

Yann Bourjault, Directeur Transformation Digitale et Cybersécurité France de Schneider Electric, observe quant à lui que les cyberattaques en milieu industriel « *se rapprochent des machines. Les structures de toute taille redoutent les dégâts de ces attaques toujours plus complexes sur les outils de production, mais aussi sur la réputation de la victime* ».

En dehors des attaques, d'autres défis cyber préoccupent les entreprises

La **mobilité des salariés** est citée comme le 1er défi en matière de cybersécurité pour les prochaines années, en hausse de 11 points par rapport à l'an dernier. 49 % de répondants évoquent également l'évolution rapide des systèmes d'information (+ 9 points). La **méconnaissance des utilisateurs** arrive en 3e position, suivie par le déploiement d'outils de **travail collaboratif** à égalité avec le **cloud** (39 % des réponses).



Quels sont les défis principaux en matière de cybersécurité auxquels votre entreprise devra faire face dans les années à venir ?

Les résultats laissent apparaître dans l'administration publique plus qu'ailleurs **une difficulté à définir le rôle de chacun** (40 % contre 26 % dans l'échantillon complet). En parallèle, 21 % de l'échantillon global fait état d'**un manque de moyens financiers** (un chiffre qui grimpe à 41 % pour les répondants s'estimant en retard en matière de transformation numérique).

À ces défis cyber à moyen terme, se sont ajoutées cette année des difficultés très concrètes :

- connexion Internet inadaptée pour près de 40 % des sondés,
- problèmes d'accès aux applications métiers pour plus d'un répondant sur cinq,
- problèmes d'accès, de maîtrise des outils de communication et d'organisation du travail pour un tiers des répondants (46 % sur ce dernier item pour les directions générales).

Sans oublier la délicate articulation du travail à distance et de la vie personnelle, notamment la garde des enfants.

L'étude révèle qu'¼ des organisations n'a eu d'autre choix que de faire des concessions en matière de cybersécurité pour assurer la continuité d'activité.

Parmi elles figure une majorité d'administrations publiques. Charles Blanc-Rolin, RSSI & DPO du GHT Cantal, confirme que « *certains établissements de santé se sont retrouvés dans des situations critiques après avoir ouvert leurs infrastructures en urgence. Heureusement, notre secteur pratique la veille collaborative et nous avons pu remonter un grand nombre de vulnérabilités à l'Agence du Numérique en Santé (ANS)* ».

Autre indicateur encourageant, la proportion de sondés déclarant voir la dimension « sécurité » toujours intégrée en amont d'un projet est passée de 70 % en 2019 à 82 % cette année. Certains automatismes se mettent donc en place.

1 entreprise sur 4

déclare avoir fait des concessions en matière de cybersécurité pour assurer la continuité d'activité

Quelles sont les solutions déployées pour sécuriser les projets de transformation numérique ?

L'accroissement de la mobilité des salariés cette année n'est sans doute pas étranger à l'accélération de l'approche « **Zero Trust** », en réflexion ou en déploiement dans près d'une structure interrogée sur cinq. Cette stratégie repose sur le principe de ne jamais accorder sa confiance par défaut et donc de systématiquement vérifier l'identité des personnes avant de leur octroyer un accès quel qu'il soit.

Les courtiers en sécurité d'accès cloud (ou CASB pour *cloud access security brockers*) avaient su séduire près de 20 % des répondants en 2019. L'enthousiasme est beaucoup plus modéré cette année avec seulement 7 % cette année (contre 43 % de sondés qui ne prévoient pas son déploiement).

En revanche, les organisations et entreprises réfléchissent à la mise en place de l'**authentification avancée double facteur** (29 %), de la protection contre la fuite de données (Data Loss Prevention - **DLP**, 22 %) et du **chiffrement des emails** (17 %).



Pour Jérémy, DSI d'un groupe agroalimentaire en Afrique de l'Ouest, les projets ne manquent pas : « *nous allons mettre en place de nouveaux pare-feux, l'authentification à plusieurs facteurs (MFA), le scan de vulnérabilités et un SOC* ».

Les déploiements en urgence sont peu nombreux, à l'exception des VPN, et encore dans une moindre mesure (4 %). Cela s'explique sans doute par le fait que le temps du projet sécurité n'est pas celui de la gestion de crise. Seule certitude à ce stade, celle-ci n'est pas derrière nous, d'où l'importance d'anticiper et de se préparer à différents scénarios afin de réduire la menace que représentent une mobilité accrue des salariés et l'utilisation de leur matériel personnel.

La note attribuée au degré de préparation aux cyber-risques par l'ensemble de l'échantillon est de 6,6 sur 10, stable par rapport à l'an dernier (6,5). Il est même rassurant de remarquer que sur la population DSI, celle-ci est en hausse (de 6,1 à 6,6).

6,6/10

comme note moyenne de d'évaluation du degré de préparation des entreprises et organisations pour faire face aux cyber-risques induits par la transformation numérique

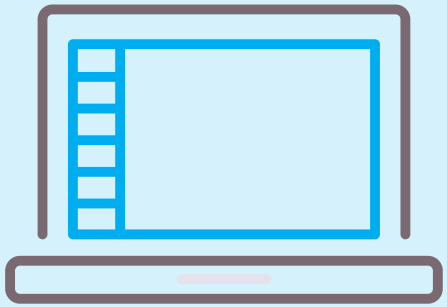
Partie 3

Une stratégie de moyens contrastée

De nouveaux outils numériques à sécuriser

Déjà pointés du doigt l'an dernier, les terminaux mobiles et les services de partage de documents ne sont toujours pas suffisamment sécurisés pour respectivement 33 et 21 % du panel. Cependant, **les craintes se concentrent cette année sur un nouvel item : les terminaux personnels des collaborateurs (36 %)**. À travers ces résultats, nous percevons que la mobilité des collaborateurs, forcée la plupart du temps cette année, demeure un sujet pour la sécurisation des outils numériques.

Au chapitre des améliorations, il faut noter que la sécurité de l'infrastructure industrielle ou opérationnelle aurait progressé de 13 points et celle de l'infrastructure réseau de 19 points tout comme celle des applications métiers.



Le SOC, future star des moyens déployés pour garantir la sécurité informatique ?

La **sensibilisation à la sécurité informatique** reste l'action prioritaire préconisée par les sondés pour améliorer la cybersécurité au sein des entreprises et des organisations. Elle est déjà à l'œuvre dans 68 % des structures interrogées et prévues dans 17 %.

En revanche, la proportion d'entreprises qui ne prévoient pas d'actions de sensibilisation à la sécurité informatique est passée de 2 % en 2019 à 9 %. Faut-il y voir le reflet des priorités de cette année hors du commun ou l'impact de l'annulation de formations en présentiel ?

Près de la moitié des répondants disent réfléchir ou avoir opté pour le Security Operations Centre (SOC). Comme l'explique Sébastien Viou, Consultant Cyber-évangéliste Stormshield, « *le SOC intervient dans la phase de détection : il s'agit d'une organisation, au sens process, qui supervise la sécurité du système d'information et repère les menaces. Elle conseille les équipes de réponses sur les possibles corrections* ».

Ces tours de contrôle SI ont été largement déployées dans les grands groupes et pour les infrastructures critiques dans la foulée de l'adoption du Règlement Général de Protection des Données (RGPD), de la loi de programmation militaire française (LPM) et de la directive NIS sur la sécurité de l'information et des réseaux. Mais les plus petites structures peuvent également bénéficier des services d'un SOC mutualisé.

Le recours à des **entreprises de conseil spécialisées** dans la cybersécurité a plus que doublé pour atteindre 46 % des répondants. À l'inverse, les prévisions de **recrutement de profils spécialisés** baissent de 13 points par rapport à l'an dernier. Au-delà de la question des budgets, nous pouvons y voir la manifestation d'un secteur toujours en manque de talents. Des difficultés de recrutement confirmées par Yann Bourjault, Directeur Transformation Digitale et Cybersécurité France de Schneider Electric : « *il n'est déjà pas simple de trouver des experts en cybersécurité et en cybersécurité industrielle encore moins ! La compréhension du monde de l'industrie, de la priorité à la production, au fonctionnement d'un automate, représente une double compétence particulièrement rare* ».

Enfin, près d'un tiers des répondants prévoit de **repenser les process de mise à jour** des postes de travail. Une entreprise sur cinq prévoit d'intégrer la sécurité dès la réflexion des nouveaux projets de transformation numérique, de mettre en place une **plateforme d'automatisation** de la cybersécurité ou encore de **redéfinir l'architecture** réseau et sécurité.



Une stratégie de moyens contrastée

Le budget, toujours au cœur du sujet sécurité

Les tendances budgétaires sont très dépendantes du secteur d'activité et bien sûr de la façon dont celui-ci est impacté par la crise. Certains secteurs ont continué d'investir à l'image de l'agroalimentaire, du moins les segments qui distribuent des produits essentiels aux foyers français, ou de l'automobile, qui a connu un rebond net au sortir du 1er confinement. En revanche, nous comprenons aisément qu'il n'y ait pas eu ou peu d'investissements de la part des acteurs de l'hôtellerie-restauration ou des aéroports par exemple.

Yann Bourjault, Directeur Transformation Digitale et Cybersécurité France de Schneider Electric, complète : « *les entreprises ont alloué leur budget à la sécurisation de l'informatique bureautique dans le cadre de la généralisation du télétravail. Du point de vue des technologies industrielles, les seuls budgets en hausse sont ceux de la cybersécurité des usines* ».

Un témoignage qui fait écho aux 27 % de répondants qui ont déclaré que leur entreprise avait débloqué des fonds exceptionnels importants pour le numérique et sa sécurisation dans ce contexte.

La priorité a été donnée à la transformation numérique à court terme, mais la volonté d'investir plus dans la sécurité à moyen terme semble présente avec 49 % des répondants qui assurent que le budget cybersécurité va augmenter.



Reste à espérer que les entreprises et les organisations aient réellement les moyens de passer à l'acte.

Face aux problématiques de financement du secteur public, en particulier pour le monde hospitalier, il est clair que la gestion du vieillissement de ses architectures informatiques ou de l'obsolescence de ses logiciels ne se classe pas en tête des priorités. Il faut donc apprécier l'investissement de 2 milliards prévus par le Ségur de la Santé pour le numérique. Un enthousiasme modéré par Charles Blanc-Rolin, RSSI & DPO du GHT Cantal : « *c'est certes historique, mais ces accords ne prévoient rien pour la maintenance de ces investissements* »[1].

Les difficultés budgétaires touchent également le secteur privé. En juillet, près de la moitié des entreprises du CAC 40[2] s'apprêtaient à stabiliser leurs budgets cybersécurité et 25 % à les diminuer.

Jérémy, DSI d'un groupe agroalimentaire en Afrique de l'Ouest, fait donc plutôt figure d'exception. « *Là où d'autres ont vu l'intégralité de leur budget consommé par des tentatives de sécurisation et/ou de remédiation, mon budget a très peu été impacté et nous allons pouvoir maintenir la feuille de route d'investissement* » confie-t-il, conscient de sa chance.

[1] esante.gouv.fr/node/3641

[2] www.lesechos.fr/tech-medias/hightech/cybersecurite-en-difficulte-le-cac-40-reduit-ses-budgets-1221700

Conclusion

Dans le numérique comme dans d'autres sphères de nos sociétés, les crises ont accentué les inégalités d'accès, de moyens et de compétences numériques entre les différents acteurs. Yann Bourjault, Directeur Transformation Digitale et Cybersécurité France de Schneider Electric, le confirme : « *les menaces cyber augmentent et se complexifient bien plus vite que la sécurité informatique ne s'améliore : l'écart se creuse* ».

2020 aura aussi été un « *laboratoire extraordinaire pour le travail hors bureau et le télétravail à grande échelle* »[1]. Selon Jérémy, DSI d'un groupe agroalimentaire en Afrique de l'Ouest, « *beaucoup de sociétés ont pris conscience cette année grâce au télétravail que l'informatique était vitale et que les budgets IT et cyber mériteraient d'être réévalués en conséquence* ».

Au niveau individuel, l'infrastructure personnelle du salarié devient la préoccupation de l'entreprise. Avec la généralisation du travail à distance, la responsabilité cyber tend à se déporter sur les collaborateurs. Ces derniers sont-ils prêts à l'endosser ?

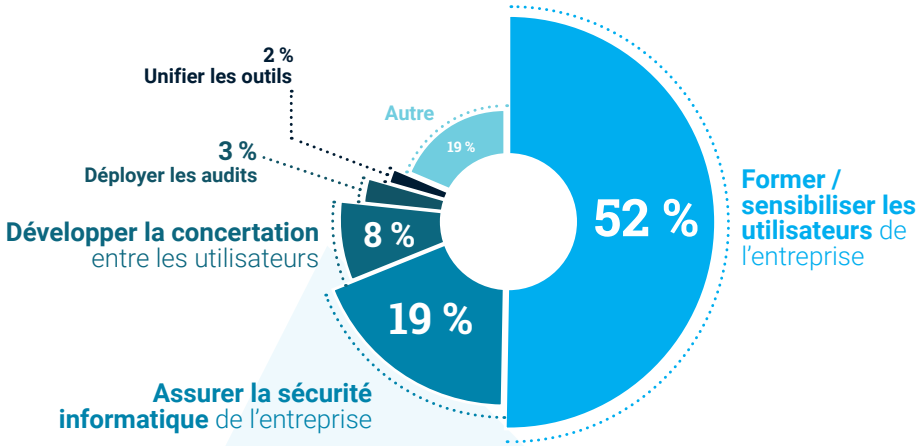
C'est en tout cas le cap que fixe Sébastien Viou, Consultant Cyber-évangéliste Stormshield : « *l'ensemble de l'entreprise doit être partie prenante dans l'amélioration de la cybersécurité. L'équipe IT pourrait par exemple mettre en place les outils puis déléguer aux managers la gestion du quotidien* ». Un modèle qui nécessite de maintenir les efforts de sensibilisation auprès de tous les publics.

[1] CLUSIF, *Télétravail, cybersécurité et collaborateurs : les nouveaux équilibres*, octobre 2020

Continuer d'expérimenter pour améliorer la cybersécurité

Charles Blanc-Rolin, RSSI & DPO du GHT Cantal, poursuit donc sa mission : « *faire passer des messages pour faire évoluer les pratiques* ». Pour cela, il communique sur l'actualité, les menaces et les incidents observés dans son secteur. « *Malgré le contexte, nous avons des retours utilisateurs, des alertes… C'est positif.* »

Et il n'est pas le seul à avoir fait le choix de la communication.



Quelles seraient vos principales idées pour améliorer la cybersécurité de votre entreprise ?

Depuis près d'un an, Frédéric Leblond, RSSI du Port Boulogne Calais, diffuse une newsletter mensuelle qui a su trouver ses lecteurs. Enfin, les webinaires ont permis à Schneider Electric de poursuivre sa mission d'évangélisation pour améliorer le niveau de sécurité de l'ensemble de l'écosystème, et ce, malgré les annulations de formations en présentiel.

C'est sans doute là le point positif de cette année particulière : le nombre incroyable de ressources partagées pour construire une intelligence collective et le monde de demain.

Sources et références

Baromètre de la transformation numérique et de la cybersécurité 2020 Stormshield/L'UsineDigitale

Méthodologie :

Questionnaire auto administré en ligne, rempli entre les 16 juillet et 07 septembre 2020 par 217 décideurs issus de directions SI/Digital/Numérique et de directions métiers, de tous secteurs d'activité et de toutes tailles d'entreprise.

STORMSHIELD

Partout dans le monde, les entreprises, les institutions gouvernementales et les organismes de défense ont besoin d'assurer la cybersécurité de leurs infrastructures critiques, de leurs données sensibles et de leurs environnements opérationnels. Les technologies Stormshield, certifiées et qualifiées au plus haut niveau européen, répondent aux enjeux de l'IT et de l'OT afin de protéger leurs activités. Notre mission : cyber-séréniser nos clients pour qu'ils puissent se concentrer sur leur cœur de métier, si cruciale pour la bonne marche de nos institutions, de notre économie et des services rendus aux populations. Choisir Stormshield, c'est privilégier une cybersécurité européenne de confiance.

www.stormshield.com