

# Revenir plus forts : les priorités pour les dirigeants d'entreprises en matière de communication

Malgré les nombreuses transitions et transformations, désirées ou subies, par les organisations ces derniers mois, la communication est restée un élément clé de la vie professionnelle. Dès le début de la pandémie, les entreprises ont cherché à s'appuyer sur différentes technologies pour garder le contact avec leurs employés, collègues et clients, et ont fait de leur mieux pour maintenir leurs niveaux de productivité aussi élevés que possible.

Naturellement, pendant cette crise, les organisations se sont efforcées de mettre en place les technologies adéquates pour permettre à leurs salariés de travailler depuis leur domicile. Cependant, avec l'évolution de la situation sanitaire et le retour progressif dans les bureaux, chacun doit continuer à s'organiser en attendant une sortie de crise.

## Des solutions visuelles pour les salles de réunion

Bien que cela soit actuellement difficile à imaginer, bientôt, des groupes d'individus pourront se rassembler dans une même pièce pour participer à des réunions. C'est donc le moment idéal pour réfléchir à ces espaces et à la meilleure façon de les optimiser, en y intégrant les solutions visuelles les plus appropriées pour soutenir la collaboration et favoriser des présentations incluant l'ensemble des collaborateurs (qu'ils travaillent en présentiel ou à distance).

Un des points importants sera de donner la priorité aux technologies les plus adaptées, pas seulement par rapport à l'espace, mais aussi pour les collaborateurs amenés à les utiliser. Les produits surdimensionnés ne sont pas forcément meilleurs, de même qu'une technologie trop complexe peut être source d'appréhension et engendrer de la résistance au sein des équipes. Les décideurs gagneront donc à consulter les utilisateurs clés de leur entreprise, afin de veiller à installer la solution adéquate dans un espace où elle pourra être utilisée en toute simplicité.

Certains écrans collaboratifs sont idéals pour des réunions collaboratives en visioconférence via Skype for Business et Teams. Ils peuvent également fournir des informations relatives à la température, à la qualité de l'air, à l'humidité, à l'occupation et à la luminosité des pièces dans lesquels ils sont installés. Les fonctionnalités de ce type seront essentielles dans l'environnement professionnel de demain, et offrent aux entreprises l'opportunité de prendre une longueur d'avance.

## Des systèmes d'impression pour faciliter le partage d'informations

Bien que les entreprises soient, à juste titre, inquiètes quant à l'impact sur l'environnement des impressions inutiles, investir dans un appareil économe en énergie est une autre façon de contribuer à cet effort tout en disposant des documents importants sur papier.

Les systèmes d'impression font partie des équipements ayant trouvé un nouveau souffle dans les bureaux connectés d'aujourd'hui ; cependant leurs nouvelles applications sont également à l'origine de risques accrus en matière de sécurité. Ainsi, une étude publiée récemment a révélé que près de

la moitié (45%) des PME françaises couraient le risque de subir de graves pertes ou corruption de leurs données à cause de systèmes d'impression mal sécurisés. La menace que représentent les imprimantes et MFP connectés pour un réseau reste sous-estimée par les organisations locales.

Si les entreprises comptent de plus en plus sur leur fournisseur bureautique pour se procurer leurs systèmes multifonctions connectés, cette pratique est également l'opportunité pour elles de profiter d'une approche plus unifiée en matière de sécurité de leurs infrastructures. Recevoir des services de sécurité de la part de leur fournisseur d'équipements est une solution bien plus simple, et les dirigeants pourront même se tranquilliser en sachant que ces prestataires possèdent déjà l'expertise et les technologies nécessaires pour les protéger.

### Sécuriser les équipements pour protéger les données des clients et d'entreprises

Les dirigeants d'entreprise ont l'obligation de veiller à la sécurité de leurs équipements, données clients, et actifs numériques. Nous savons que le cybercrime représente une menace immédiate pour toutes les organisations, quelles qu'en soient la forme ou la taille. Cette menace a d'ailleurs été particulièrement manifeste au premier trimestre 2020, où le nombre d'attaques a augmenté de 30% par rapport à la même période, l'année dernière.

Aujourd'hui, les cybercriminels disposent d'une multitude de points d'entrée pour pirater l'infrastructure d'une entreprise, tout en restant presque impossibles à détecter ; À l'heure où les appareils IoT sont de plus en plus répandus en entreprise, ce problème concerne non seulement les programmeurs, mais aussi les équipements connectés à Internet.

L'environnement professionnel d'aujourd'hui, en dépit de ses nombreuses nouvelles opportunités de gestion intelligente et de rationalisation, présente donc clairement des risques de sécurité non négligeables pour les dirigeants. Des ordinateurs aux imprimantes en passant par les télévisions et les smartphones, l'adoption de technologies connectées toujours plus sophistiquées augmente également le nombre de faiblesses susceptibles d'être exploitées.

Les vulnérabilités des PME sont déjà nombreuses, et cette liste de points faibles est amenée à s'allonger avec la multiplication des équipements de bureau intégrés et connectés. L'IoT étant désormais une réalité en entreprise, les opportunités offertes aux pirates ne peuvent qu'augmenter.

Dans les prochaines années, les dirigeants devraient se rendre compte que leurs objets connectés nécessitent tout autant de protection que leurs ordinateurs. Tout appareil connecté doit désormais être considéré comme un potentiel maillon faible. Les fabricants d'équipements ont donc une excellente occasion d'offrir davantage de tranquillité et de prendre une place plus importante auprès de leurs clients.

Après des mois de confinement, le retour sur le lieu de travail est le moment idéal pour se décider à protéger l'ensemble des potentiels points d'entrée laissés aux pirates. Ces initiatives devront couvrir l'ensemble des appareils connectés à Internet. Pour gérer le retour de leurs salariés sur le lieu de travail, les dirigeants ont donc tout intérêt à faire du choix d'un fournisseur offrant une sécurité renforcée leur priorité.