

Future Ready Days - Christophe Bianco : « On traite des cyberattaques tous les jours »



Quinze minutes et des poussières, soit le temps imparti à Christophe Bianco pour son intervention aux Future Ready Days : « Pour ceux qui me connaissent, un quart d'heure, c'est un challenge... » Le co-founder d'Excellium Services a pourtant relevé le défi. Ce grand nom de la cybersécurité a fait un passage remarqué, le 11 mars dernier à la Luxexpo, cadre de la 1^{ère} édition de l'évènement co-organisé par le ministère de l'Economie, la House of Entrepreneurship de la Chambre de Commerce et la Chambre des Métiers.

Axé sur la digitalisation des PME, ce rendez-vous a mis l'accent sur un domaine familier de l'expert, que l'on pourrait résumer par cette question volontairement naïve : les voies de l'intelligence artificielle sont-elles impénétrables ? Evidemment, pour les **cybercriminels**, non...

Pouvez-vous vous présenter en quelques mots et décrire votre parcours ?

J'évolue dans l'univers de la **cybersécurité** depuis 1996. Ces douze dernières années, j'ai cofondé [la société luxembourgeoise Excellium](#). Elle compte un peu plus de 200 personnes réparties sur le Luxembourg et la Belgique. Parce que c'est un monde qui nécessite énormément d'investissement et de capacité, nous avons rejoint le groupe de défense français, Thales, en 2022. Dans notre volonté de rejoindre un acteur d'importance internationale, nous avons également pris en compte l'environnement géopolitique. Non seulement nous souhaitons rejoindre un acteur européen mais aussi un industriel car notre domaine est avant tout un domaine d'expertise. C'est nécessaire qu'ils s'emparent de ces sujets, il en va de notre confiance dans nos environnements numériques.

L'actualité, qui remet la souveraineté européenne sur le devant de la scène, vous donne raison...

Oui, il semblerait... Nous avons donc fait cette opération de cession mais je suis resté dans la société en tant que responsable des ventes au niveau mondial. **L'expertise** développée au Luxembourg a été reconnue par [Thales, un groupe qui emploie tout de même 80.000 personnes](#)... En tant qu'entrepreneur, c'est toujours valorisant de voir que ce que tu as construit se développe. En parallèle, j'exerce comme professeur associé à l'école d'ingénieurs Telecom Nancy. J'encourage aussi mes collaborateurs à intervenir dans une dizaine de cursus au Luxembourg et dans la grande région.

"Notre problème dans les métiers de la cybersécurité, c'est que tout le monde pense que le job c'est pull à capuche, Red Bull et hacking"

C'est important de transmettre ?

Ce n'est pas juste une histoire de transmission. Notre business dépend de compétences et ces compétences, il faut les infuser car nous sommes sur des métiers nouveaux, qui n'existent pas. Il faut motiver les jeunes à embrasser ces **carrières technologiques**. Notre problème, dans les métiers de la **cybersécurité**, c'est que tout le monde pense que le job c'est « pull-capuche, Red Bull et hacking » ; or il y a autant de métiers que de sujets dans le cyber. Autant l'avenir est incertain dans plusieurs métiers, autant dans la cybersécurité, le champ est vaste.

Selon vous, quelles sont les trois grandes tendances qui vont transformer l'entrepreneuriat d'ici 2030 ?

Je ne suis pas voyant...

Contrairement à l'IA, basée sur la prédiction comme vous le souligniez lors de votre intervention...

Je crois que l'on va se calmer rapidement avec tout l'argent dépensé dans l'IA. Aujourd'hui, on a du mal à valoriser le volume de data produit. Or **l'IA est basée sur l'analyse de ces data**, donc tant que nous n'aurons pas des gens qui pensent data, ce sera compliqué de développer des modèles économiques viables.

Ces trois tendances, donc ?

En premier lieu, la recherche de modèles économiques soutenables et résiliants favorisant la flexibilité et l'adaptabilité. Monter un business en posant un plan sur cinq ans est de plus en plus difficile, le marché bouge trop vite. Ce qui va faire la différence d'ici 2030, c'est la capacité à piloter en temps réel, à tester rapidement et à ajuster en fonction des données. Le monde des affaires est de plus en plus imprévisible, avec des crises économiques, sanitaires et géopolitiques qui se succèdent. Les entrepreneurs devront être agiles et capables de s'adapter rapidement aux changements. La deuxième tendance tient à la bataille pour les talents du fait de la digitalisation accrue. Le recrutement et la rétention sont déjà des challenges pour de nombreuses entreprises. D'ici 2030, il sera de plus en plus dur de recruter des salariés. J'ai l'impression qu'il faudra jongler entre collaborateurs fixes, freelances, experts à la demande, et miser sur des valeurs fortes pour attirer les bonnes personnes. Les entreprises qui ne s'adapteront pas perdront la **guerre des talents**. Enfin, je pense que l'on se dirige vers une révolution des business models : vendre un produit ne suffira plus, on vendra une expérience, une communauté et un impact. Les consommateurs et les entreprises clientes deviennent de plus en plus exigeants. Il faudra proposer un écosystème, une expérience et une relation durable. Cela passera par des modèles par abonnement (SaaS, services à la demande, offres évolutives), l'intégration des clients dans la création du produit (co-crétation, personnalisation) et un engagement sur des valeurs fortes (impact écologique, transparence, responsabilité sociale).



L'intervention de Christophe Bianco a constitué l'un des temps forts de cette première édition des Future Ready Days (crédit : Charly Petit/Chambre de Commerce).

Un message clé que vous aimeriez faire passer aux lecteurs de Merkur.lu ?

L'importance de la digitalisation, un élément majeur pour les entrepreneurs. Mais cela requiert la prise en compte de ces trois impératifs : piloter l'adoption et ne pas la subir, investir dans la formation et le développement des compétences (les entreprises devront former leurs employés aux nouvelles technologies et aux compétences du futur) et renforcer la cybersécurité du fait de la dépendance accrue au digital. Avec la digitalisation croissante, la protection des données et des systèmes est cruciale.

Sur ce point, comment convertir des PME à ces systèmes de protection souvent très coûteux ?

C'est compliqué... Lorsque j'ai cofondé la société il y a douze ans, nos cibles étaient les PME et PMI. Mais un modèle économique basé sur l'expertise avec de forts besoins d'investissement amène à des coûts de prestation qui peuvent être un peu dissuasifs pour une PME ou PMI qui ne peut pas englober son budget annuel dans une simple prestation ponctuelle. Donc je pense, là, que la posture du gouvernement est assez exemplaire. Les grosses entreprises ont les moyens mais ce sont les PME/PMI qui font le tissu économique de notre pays. Donc il faut une collaboration secteur privé – secteur public pour développer des capacités et essayer de créer des synergies. Et d'avoir des incitatifs pour que des gros, comme nous, reversent un peu à la communauté. L'idée, c'est d'accompagner, a minima, à la sensibilisation aux bonnes pratiques. Mais encore faut-il que les dirigeants de PME trouvent du temps dans leur agenda surchargé.

"L'IA est un outil, que l'on peut challenger mais dont il faut toujours vérifier la pertinence"

Face à une cybercriminalité toujours mieux organisée, ce minimum requis n'apparaîtrait-il pas comme presque vital ?

Je peux vous donner les statistiques, on traite **des cyberattaques tous les jours**. Cela m'arrive régulièrement de dire à des dirigeants de PME que je ne peux pas les aider, parce que c'est trop tard. Un exemple récent ? Un entrepreneur a réglé 15.000 euros à un artisan. C'était une fausse facture numérique. Ces 15.000 euros, il ne les retrouvera jamais. Aujourd'hui, on utilise de la nouvelle technologie sans en avoir la moindre compréhension. On n'a pourtant pas idée de conduire une voiture sans avoir le permis...

Cette conduite dangereuse n'est-elle pas induite par la facilité de prise en main de l'IA ?

En effet, on essaie de la rendre la plus abordable et utilisable pour les néophytes, mais on occulte les problématiques liées à son usage. Quand quelqu'un télécharge son résultat financier dans ChatGPT pour obtenir une synthèse, est-ce qu'il a conscience de transférer des données confidentielles à une boîte qui va les utiliser de manière publique ? Pas besoin d'être expert pour se prémunir de ces risques. Il faut garder à l'esprit que l'IA est un outil, que l'on peut challenger mais dont il faut toujours vérifier la pertinence. Le piège, c'est que quand on reçoit une information de **ChatGPT**, c'est tellement bien écrit qu'on a toujours l'impression que c'est vrai...

Quels conseils donneriez-vous aux entrepreneurs qui souhaitent se lancer dans la cybersécurité, un secteur qui paraît déjà fortement congestionné ?

Quand j'ai lancé Excellium, nous étions déjà en nombre sur le marché. Pour sortir du lot, nous avons pris le parti de l'expertise, en nous positionnant comme experts à disposition d'une clientèle spécifique dans une approche de partenariat. Aujourd'hui, nous aurions du mal à le refaire. Plus que la compétitivité, la difficulté tient aux investissements initiaux nécessaires et aux besoins de

compétences à aligner pour répondre aux besoins de nos clients. La taille critique et les capacités sont de mon point de vue indispensables aujourd'hui pour se positionner comme un partenaire cyber de ces entreprises. Malgré tout, j'encouragerais mes camarades qui veulent s'engager dans la cybersécurité à accompagner la sécurisation de l'IA dans son adoption. C'est un nouveau champ de compétences, un nouveau type de technologie qui nécessite des profils. L'IA est un excellent domaine pour développer ses compétences.