HOFFMAN NEWSLETTER

Leadership en cybersécurité : un échange avec le Professeur Georges Ataya sur les 6 Étapes Clés pour construire une Résilience Organisationnelle

Mars 2025

À une époque où les menaces numériques évoluent constamment, la cybersécurité est devenue une préoccupation cruciale pour les organisations de tous les secteurs. J'ai récemment eu l'opportunité de m'entretenir avec le Professeur Georges Ataya, expert renommé en gouvernance numérique et cybersécurité, pour discuter des étapes essentielles que les dirigeants devraient suivre pour protéger leurs entreprises. Notre discussion a mis en lumière six facteurs clés dans le domaine de la cybersécurité, repris ci-dessous.

Nous avons commencé notre discussion avec Georges en évoquant "le concept du 'Paradoxe de la Connaissance', qui suggère qu'une moindre connaissance des risques de cybersécurité conduit souvent à un excès de confiance. Cela peut entraîner une sous-estimation des risques lors des efforts de transformation numérique."

Faits sur la Cybersécurité

Fait 1: Les Mythes de la Cybersécurité

Selon Georges, les entreprises luttent souvent pour atteindre le bon équilibre entre des dépenses adéquates en cybersécurité, et une protection raisonnable. Toutes les dépenses en outils, systèmes de protection et méthodes de défense ne sont pleinement productives que si elles sont basées sur une analyse de risque validée par la direction. En examinant les statistiques d'incidents, cet équilibre recherché ne semble pas être atteint dans la plupart des organisations, des plus grandes aux plus petites. Il existe en effet plusieurs mythes courants sur la cybersécurité, comme celui de la considérer uniquement comme un problème technique.

Fait 2: La Dette de Securité

Comme la Dette Technologique, une Dette de Sécurité est une accumulation de déficiences dans une entreprise et ses éléments d'architecture IT, y compris les processus métier et les technologies. Le coût d'une Dette de Sécurité correspond à des paiements récurrents causés par une mauvaise planification et mise en œuvre des protections, ainsi que par l'absence d'une démarche intégrant la sécurité dès la conception (« security-by-design »). Elle a des dimensions à la fois commerciales et technologiques.

Fait 3: Le Besoin de Gouvernance

La Gouvernance de la Cybersécurité, comme la Gouvernance Numérique, définit des processus qui permettent des prises de décision et des actions efficientes. L'optimisation des

risques et l'optimisation des ressources doivent avoir comme objectif d'atteindre les objectifs stratégiques tout en optimisant l'équilibre entre risques et dépenses.

Notre discussion s'est poursuivie sur ce que les dirigeants d'entreprise devraient faire. Et, sur la base de son expérience très importante et largement reconnue, Georges a résumé le tout en proposant six étapes clés :

La Check-list du Leadership en Cybersécurité

Étape 1 : Risques Commerciaux

Les dirigeants doivent identifier et évaluer les risques de sécurité liés à l'entreprise, au-delà des seules préoccupations du département informatique. "On nous a fait croire que la cybersécurité implique de dépenser de l'argent principalement pour protéger le département informatique", dit Georges. Et, en effet, les entreprises à faible maturité confinent les activités de cybersécurité au département IT.
En bref, "le retour sur investissement des dépenses occasionnées pour atténuer les risques commerciaux liés à la cybersécurité est mieux estimé lorsqu'on compare les coûts des protections supplémentaires à la perte de réputation, au service au client, et à l'impact financier."

Étape 2 : Risques Technologiques

Cette étape implique d'évaluer les protections technologiques existantes et de les aligner sur les priorités de l'entreprise. Elle couvre l'examen des protections Techniques, Organisationnelles, Humaines et Physiques.

Étape 3 : Feuille de Route de Cybersécurité

La transformation digitale visant à protéger l'entreprise entraîne le lancement d'un ensemble de programmes et de projets de construction et de mise en place. Il s'agit de développer une feuille de route complète, qui priorise les projets de mise en œuvre sur la base de l'atténuation des risques. Elle implique la mise en œuvre de technologies nouvelles ou améliorées, la modification de processus métiers, la sensibilisation des employés, la contractualisation d'un service externe, un changement majeur dans l'architecture de l'entreprise, ou simplement la signature d'un contrat d'assurance.

Les projets de mise en œuvre sont priorisés en fonction des risques qu'ils sont censés éviter. Ces risques présentent un impact élevé ou faible et peuvent se voir attribuer une probabilité élevée ou faible. La priorisation implique de sélectionner un bon équilibre entre les protections qui atténuent les risques les plus probables, et les plus impactants. On pourrait arriver à un investissement annuel de 2 à 5% du budget opérationnel total de l'entreprise, en fonction de la Dette Technologique. Pour l'anecdote, les pays de l'Otan ne dépensent pas moins pour leur propre défense.

Étape 4 : Tableau de Bord de Cybersécurité

Vu le niveau et l'importance des budgets concernés et des risques à éviter, un tableau de bord constitue un outil indispensable pour le suivi de cette transformation stratégique. Il

offrira des chiffres réels et des rapports de statut de diverses postures de risques, de l'avancement des projets, des données financières et de tout autre élément nécessaire pour guider les différentes parties prenantes. Georges et son équipe ont développé un modèle à quatre dimensions, basé sur la pratique du « Balanced Scorecard », appliqué aux besoins de gestion de la cybersécurité. Les quatre dimensions sont : Finance, Processus métier, Clients, et Apprentissage et croissance.

Étape 5 : Un leader effectif en Cybersécurité

Georges souligne l'importance d'une responsabilité managériale claire pour les activités de cybersécurité, même dans les petites entreprises. Tout en insistant sur le fait qu'il existe un besoin critique de compétences multiples, allant le plus souvent bien au-delà des capacités d'une "seule personne". À cet égard, le Groupe HTP offre une proposition assez unique, soutenant ses clients avec divers modèles de leadership en cybersécurité, du placement de talents permanents au "as a service".

Étape 6 : S'engager dans un Programme de Cybersécurité

Cette étape souligne la nécessité d'une implication à tous les niveaux de l'organisation, y compris le Conseil d'Administration, le CEO, les managers commerciaux, les leaders technologiques et le RSSI (CISO).

Conclusion

Lorsque j'ai demandé à Georges ce qu'il conseillerait aux entreprises de faire, de manière très concrète, il n'a pas hésité à souligner l'importance de réaliser un audit pour déterminer la valeur potentielle et les améliorations qu'un programme complet de cybersécurité pourrait apporter. Ces évaluations structurées ont été développées pour les petites, moyennes et grandes entreprises et leur permettent, pour un coût très limité, d'atteindre une hygiène de base complète en matière de cybersécurité.

Comment le Groupe HTP peut il vous aider

Le Groupe HTP offre une combinaison de services assez unique, assurant que les besoins de nos clients sont entièrement couverts, de la définition et la mise en œuvre d'une gouvernance numérique globale, à la réalisation d'un audit et à l'assistance aux entreprises pour répondre à toutes les exigences de DORA, RGPD, NIS2, ISO27001 et autres réglementations et normes. Mais aussi en soutenant ses clients avec divers modèles de leadership en cybersécurité, du placement de talents permanents, intérimaires ou "as a service".

N'hésitez pas à nous contacter pour une discussion exploratoire.

Georges Ataya, Founder & Member of the Board
ga@atayapartners.com
Michel Grisay, Partner, Hoffman
mg@hoffman.be