Deloitte.

Pointer du doigt les coupables est futile. Les parties prenantes des services, des TI et de la TO peuvent-elles faire équipe?

Pour assurer leur cyberrésilience, les organisations doivent se doter d'un cadre de gouvernance de la sécurité et l'infuser à tous les niveaux de l'entreprise – de la salle du conseil à l'usine.

La transformation du secteur de l'énergie, des ressources et des produits industriels (ER&PI) est spectaculaire. L'industrie 4.0 et l'émergence de systèmes autonomes propulsés par les données, l'analytique et l'IA sont les moteurs d'une vague inégalée de transformations. L'augmentation des fusions, des acquisitions et des désinvestissements jette un éclairage cru sur les failles des systèmes, tout comme la multiplication des cyberincidents et l'attention plus soutenue que les conseils d'administration portent à la cybermaturité.

La nécessité impérieuse de trouver des solutions innovatrices à des problèmes endémiques – allant de l'amélioration du rendement environnemental à une collaboration plus étroite dans les relations avec la collectivité – change les réalités de l'exploitation. De plus, la propagation de la COVID-19 n'a fait qu'accélérer cette tendance, contraignant les organisations à passer au télétravail à une vitesse fulgurante.

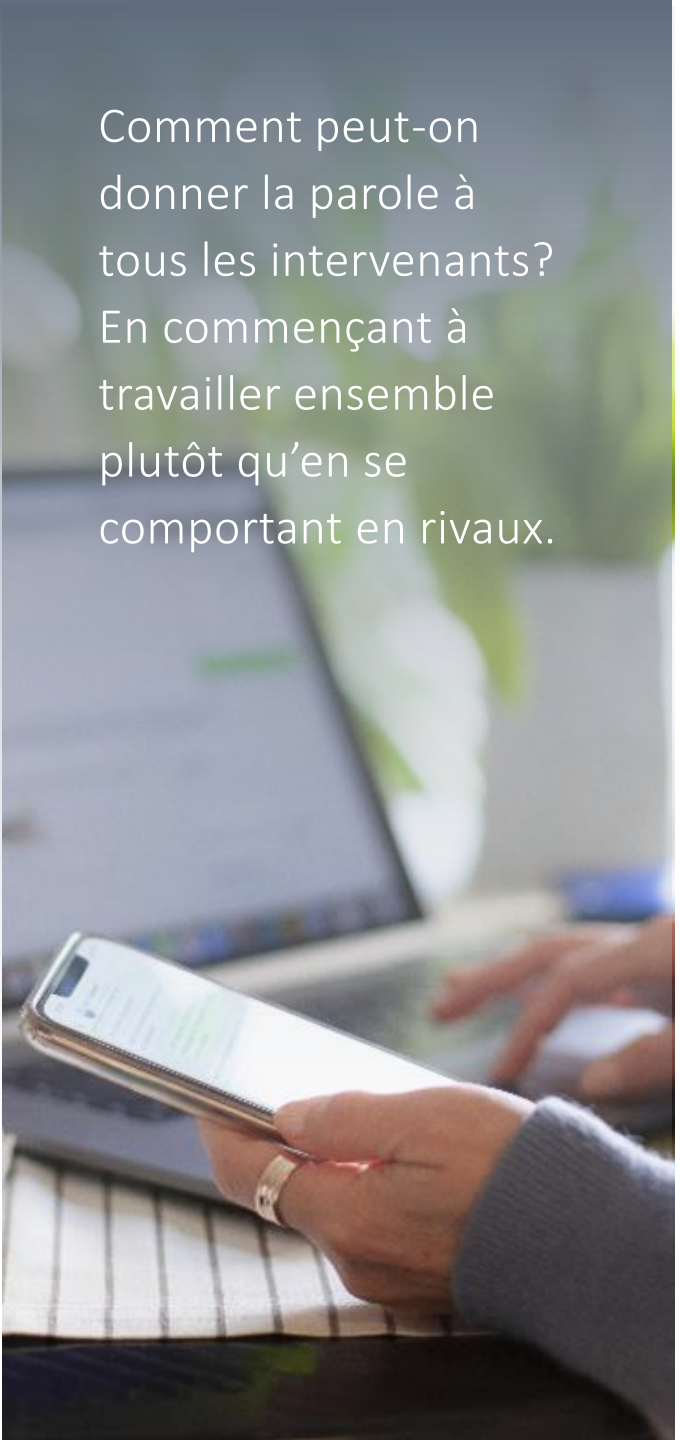
La transformation est progressive, elle est perturbatrice et elle provoque des conflits entre les équipes du numérique qui sont les porte-étendards de ces nouvelles initiatives et les équipes de la technologie opérationnelle (TO), sur lesquelles repose leur mise en œuvre.

Les conflits culturels entre les services, les TI et la TO ne sont peut-être pas nouveaux, mais leurs contrecoups menacent maintenant de s'étendre bien au-delà des défis liés à la productivité. De plus, ils exposent les entreprises à des niveaux de cyberrisque plus élevés.

Partager le risque

Il y a des ratés aux deux extrémités du spectre. D'une part, les équipes de la transformation numérique ont tendance à travailler dans un environnement raréfié et à glorifier les grandes idées – même quand elles rompent avec des pratiques opérationnelles classiques.

Avides de bénéficier de l'avantage d'être des précurseurs, ces équipes omettent parfois d'intégrer dès le départ la sécurité dans leurs processus, créant des failles dans la sécurité qui exposent non intentionnellement leurs organisations à un risque accru de violation. Pire encore, de nombreuses organisations du secteur des TI peinent à suivre le rythme auquel les risques causés par les projets numériques surgissent, ce qui crée des lacunes potentiellement graves dans le contrôle de la sécurité.



La cybersécurité à tous les niveaux

D'autre part, les équipes de la TO sous-estiment peut-être leur vulnérabilité aux cyberattaques. Habituées à travailler isolément dans des usines et des installations de fabrication, elles ont généralement du mal à saisir à quel point l'accroissement de la connectivité change les règles du jeu.

L'infonuagique, le télétravail et les chaînes d'approvisionnement étendues ont abattu les fortifications qui, auparavant, protégeaient les systèmes de TO – offrant aux cybercriminels une surface de frappe élargie. Au cours des dernières années, partout dans le monde, les systèmes de contrôle de la supervision et les systèmes d'acquisition de données, les contrôleurs logiques programmables, les systèmes de sécurité et les systèmes de contrôle industriel ont été dans la mire des pirates informatiques.

Dans le cadre d'un sondage mené en 2019 par Deloitte et la Manufacturers Alliance for Productivity and Innovation, 40 pour cent des répondants ont indiqué qu'un cyberincident était survenu dans la conduite de leurs activités au cours des 12 mois précédents. Les attaques subies par leurs installations ont occasionné aux entreprises des coûts estimatifs supérieurs à 150 millions de dollars. Dans un cas, une attaque perpétrée contre des systèmes de sécurité a même mis la vie de travailleurs en danger. Le secteur ER&PI est particulièrement exposé à des attaques ciblées de ce type contre des usines, des véhicules autonomes et des centres d'exploitation à distance.

Ces ratés ne passent pas inaperçus. Chaque incident d'envergure qui défraie l'actualité fait croître le risque d'atteinte à la réputation dans un secteur qui, souvent, fait les frais d'une publicité négative. Les conseils d'administration y réagissent en exerçant des pressions grandissantes tant sur le personnel des services que sur les équipes de la TO pour renforcer la cybersécurité.

Que faire?

Il ne s'agit pas simplement d'intégrer les TI et la TO ni d'harmoniser les fonctions traditionnellement cloisonnées. Pour assurer leur cyberrésilience, les organisations doivent aller plus loin, c'est-à-dire élaborer un cadre de gouvernance de la sécurité et l'infuser à tous les niveaux de l'entreprise – de la salle du conseil à l'usine.

Bien qu'elle soit la pièce maîtresse des initiatives de transformation numérique, la cybersécurité relève encore en général du seul domaine des TI. Cela doit changer. Les organisations doivent devenir aptes à créer des processus de cybersécurité bien définis aux niveaux de l'entreprise, des unités d'affaires et de l'équipement. De plus, elles doivent clarifier la reddition de comptes à chaque niveau hiérarchique pour que des pratiques exemplaires puissent être intégrées dans le travail quotidien du personnel.

Comment peut-on donner la parole à tous les intervenants? En commençant à travailler ensemble plutôt qu'en se comportant en rivaux. Cela peut se traduire par l'exécution de jeux de guerre ou de cybersimulations pour encourager des équipes hétérogènes à réagir collectivement à un scénario de violation. Ou encore par la production d'un jumeau numérique des installations de fabrication, qui servira de terrain de jeu à des parties prenantes interfonctionnelles pour faire des simulations de crise permettant d'évaluer la cyberrésilience de l'organisation et de modéliser des scénarios de rechange.

Les exercices de ce genre ne visent pas seulement à colmater des brèches culturelles. Leur objectif consiste à renforcer la cybersécurité des entreprises pour qu'en cas d'attaque (et il y en aura, c'est inéluctable), elles aient acquis la maturité fonctionnelle nécessaire pour intervenir efficacement.

Personne-ressource

Amir Belkhelladi | Leader canadien, Cybersécurité
abelkhelladi@deloitte.ca

À propos de Deloitte
Deloitte offre des services dans les domaines de l'audit et de la certification, de la consultation, des conseils financiers, des conseils en gestion des risques, de la fiscalité et d'autres services connexes à de nombreuses sociétés ouvertes et fermées dans différents secteurs. Deloitte sert quatre entreprises sur cinq du palmarès Fortune Global 500MD par l'intermédiaire de son réseau mondial de cabinets membres dans plus de 150 pays et territoires, qui offre les compétences de renommée mondiale, le savoir et les services dont les clients ont besoin pour surmonter les défis d'entreprise les plus complexes. Deloitte S.E.N.C.R.L./s.r.l., société à responsabilité limitée constituée en vertu des lois de l'Ontario, est le cabinet membre canadien de Deloitte Touche Tohmatsu Limited. Deloitte désigne une ou plusieurs entités parmi Deloitte Touche Tohmatsu Limited, société fermée à responsabilité limitée par garanties du Royaume-Uni, ainsi que son réseau de cabinets membres dont chacun constitue une entité juridique distincte et indépendante. Pour une description détaillée de a structure juridique de Deloitte Touche Tohmatsu Limited et de ses sociétés membres, voir www.deloitte.com/ca/apropos.

Notre raison d'être mondiale est d'avoir une influence marquante. Chez Deloitte Canada, cela se traduit par la création d'un avenir meilleur en accélérant et en élargissant l'accès au savoir. Nous croyons que nous pouvons concrétiser cette raison d'être en incarnant nos valeurs communes qui sont d'ouvrir la voie, de servir avec intégrité, de prendre soin les uns des autres, de favoriser l'inclusion et de collaborer pour avoir une influence mesurable.

Pour en apprendre davantage sur les quelque 330 000 professionnels de Deloitte, dont plus de 11 000 font partie du cabinet canadien, veuillez nous suivre sur LinkedIn, Twitter, Instagram, ou Facebook.

© Deloitte S.E.N.C.R.L./s.r.l. et ses sociétés affiliées.