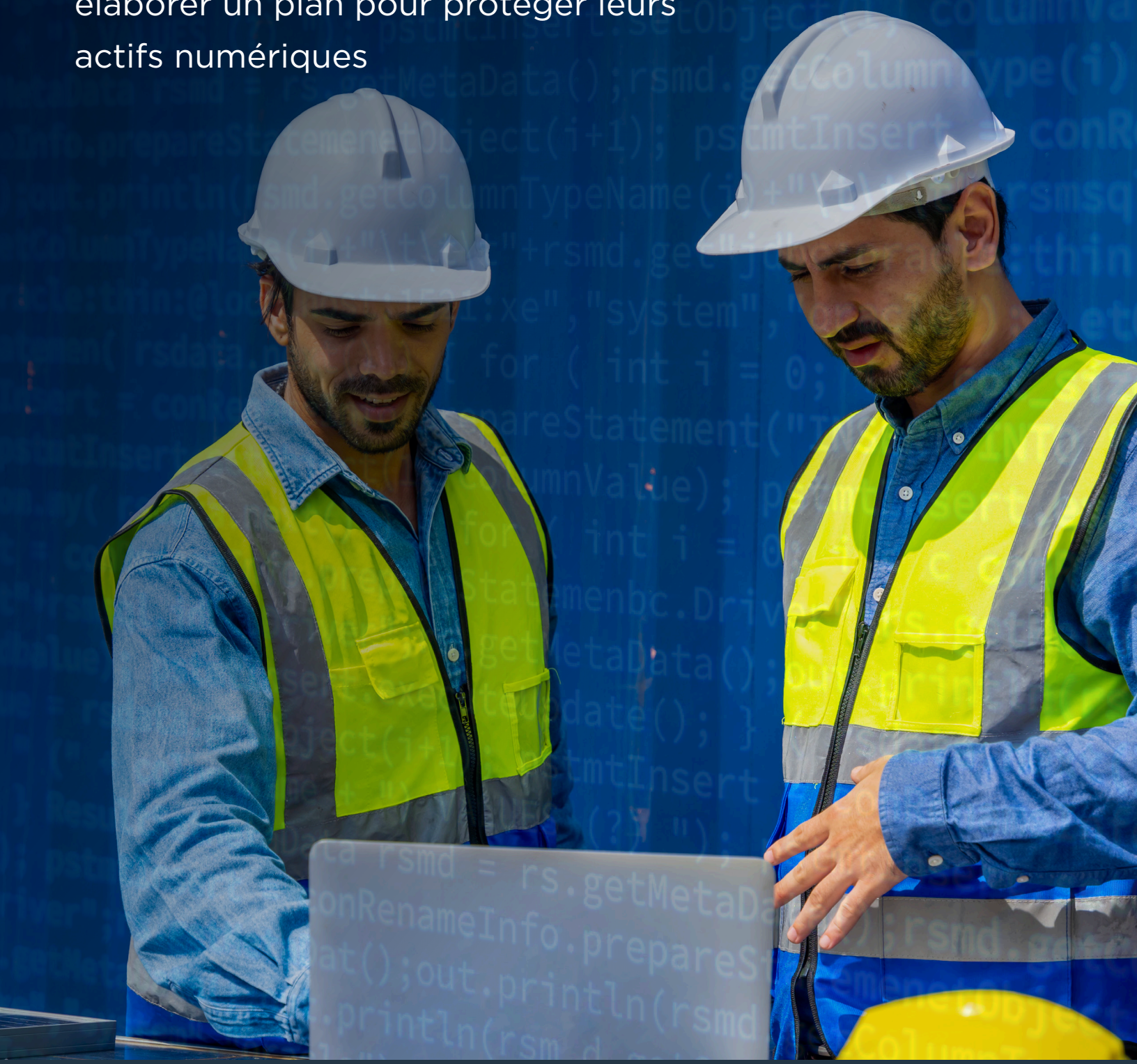
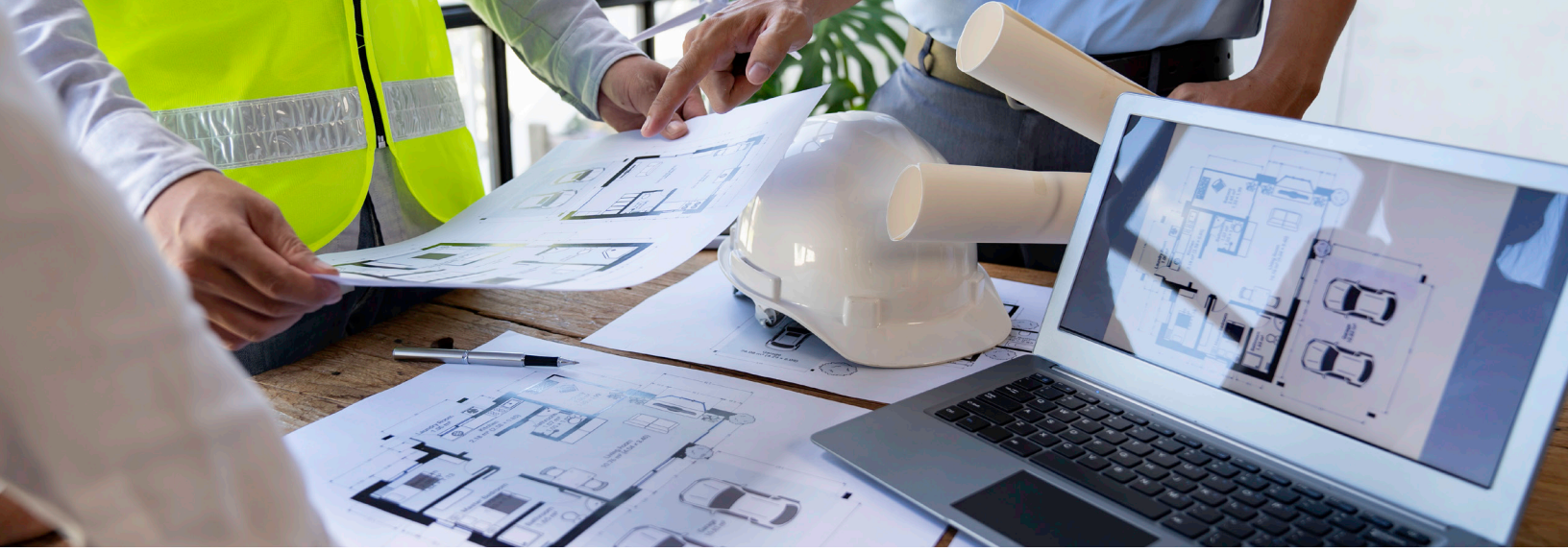
CONSTRUCTION

Élaborer une Stratégie de Cybersécurité

Comment les entreprises de construction peuvent élaborer un plan pour protéger leurs actifs numériques





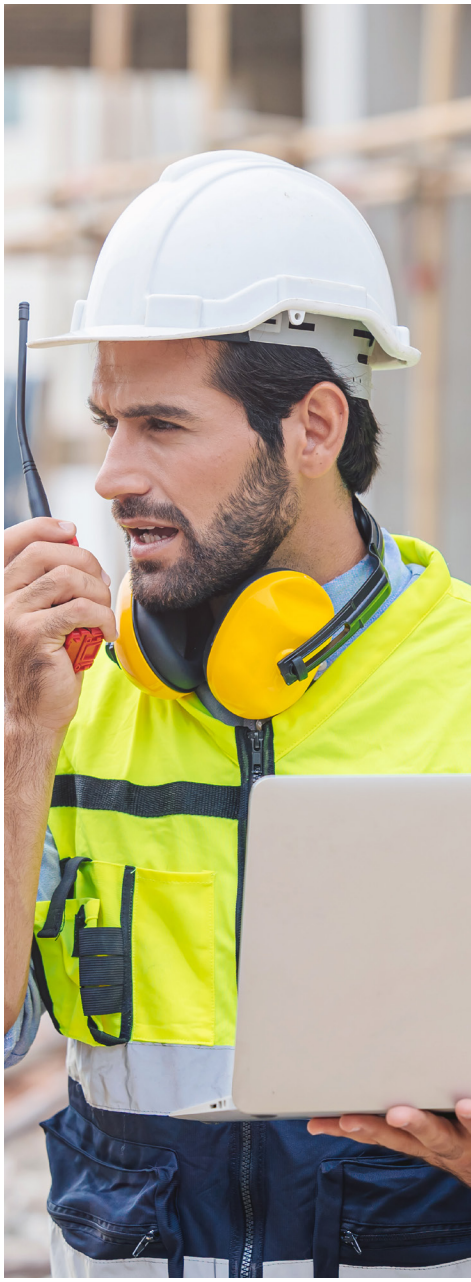
La technologie continue d'évoluer dans la construction, les entreprises adoptant chaque jour de nouveaux programmes, systèmes, dispositifs de sécurité et dispositifs IoT. Ce qui a commencé comme un passage des méthodes traditionnelles utilisant des tables à dessin aux logiciels modernes de conception assistée par ordinateur (CAO) et de modélisation des données du bâtiment (BIM) est devenu une dépendance transformationnelle à l'égard de la technologie, des données et d'autres actifs numériques, de la conception du projet à son achèvement. Les entreprises de construction abritant une multitude de données utiles, telles que la propriété intellectuelle, les plans de projets gouvernementaux, les conceptions exclusives et les comptes financiers, elles constituent une cible lucrative pour les cybercriminels.

En raison de ces risques, il est impératif que les entreprises de construction élaborent des stratégies visant à atténuer leur exposition à la cybercriminalité et créent un plan complet de réponse aux incidents cybernétiques. Pour garantir leur résilience, les entreprises de construction, quelle que soit leur taille, doivent d'abord comprendre ***pourquoi*** elles sont des cibles attrayantes, ***quelles sont*** les principales menaces en matière de cybersécurité et ***comment*** mettre en œuvre des stratégies proactives et des mesures de protection pour atténuer les risques.

Le Pourquoi.

Mal préparés et attaqués

La cybersécurité est cruciale pour toute organisation, et le secteur de la construction ne fait pas exception, car il est confronté à des menaces telles que les attaques par rançongiciels, les infections par logiciels malveillants et l'hameçonnage. Cependant, de nombreuses entreprises de construction ne disposent pas de l'infrastructure et du soutien nécessaires pour se protéger contre les cyberattaques, et sont vulnérables aux failles de sécurité pour les raisons suivantes :



- **Une préparation insuffisante.** La majorité des entreprises de construction - près des trois quarts[1] — n'ont pas priorisé la cybersécurité et ne sont pas préparées à une cyberattaque ou à une violation de système. En 2023, le secteur de la construction et de l'immobilier a été cité comme le premier secteur victime de violations aux États-Unis, avec plus de 1,5 milliard de fichiers compromis par des acteurs malveillants.[2]

- **Une utilisation accrue de la technologie.** Les dispositifs technologiques tels que la robotique, les systèmes sur site, les commandes de machines, l'intelligence artificielle et les drones ont amélioré l'efficacité du travail sur les sites des projets, mais les dispositifs sont exceptionnellement vulnérables aux violations et nécessitent une évaluation de la cybersécurité.

- **Risques liés aux tiers.** L'industrie est devenue un réseau complexe qui collabore avec de multiples entreprises, fournisseurs de matériaux, prestataires, entrepreneurs, etc. Chaque nouvelle connexion de tiers liée à ces différentes technologies crée des défis d'intégration et davantage de cyber-expositions. En fait, les entreprises de construction se classent au troisième rang des industries nord-américaines pour ce qui est des attaques par rançongiciels; il est donc important de connaître et d'évaluer les dispositions de vos tiers en matière de sécurité.

[1]Construction Today, «Safeguarding the Construction Industry in the Digital Age,» 3 octobre 2023.

[2]IT Governance, «Data Breaches and Cyber Attacks in the USA in December 2023,» 10 janvier 2024.

- **Stockage de renseignements.** Les entreprises de construction stockent d'énormes quantités de données personnelles et commerciales sensibles, y compris des informations exclusives, de la propriété intellectuelle, des plans gouvernementaux, des conceptions de projets, des données financières de l'entreprise ou du client et des comptes bancaires de l'entreprise, ce qui en fait une cible lucrative pour les cybercriminels.

Le Quoi.

Types d'attaques et de menaces

Bien que les entreprises de construction soient vulnérables à de nombreux types de cybermenaces, les rançongiciels, les vols de données et les transferts de fonds frauduleux sont les trois principales préoccupations.

Les attaques par rançongiciels impliquent que des cybercriminels infectent le système d'une entreprise avec un logiciel malveillant qui crypte les fichiers jusqu'à ce qu'un paiement soit effectué pour leur libération. Les dommages causés par les rançongiciels ne se limitent pas aux seuls paiements : Il peut s'agir d'un accès non autorisé aux renseignements de l'entreprise, d'une responsabilité potentielle

vis-à-vis des fournisseurs et des clients et d'une atteinte à la réputation. Les cyberattaques peuvent perturber les calendriers d'approvisionnement et les échéances des projets, ce qui peut entraîner des retards, des dépassements de coûts et des problèmes de qualité. Les entreprises peuvent également encourir des sanctions financières ou des poursuites judiciaires en cas de non-respect des délais.

Le vol de données — par rançongiciels, piratage psychologique ou cyberattaques — reste un problème important. Les entreprises de construction gèrent de la propriété intellectuelle confidentielle (documents de conception, brevets, stratégies de soumission, etc.), ce qui les rend une cible de choix pour les cybercriminels qui reconnaissent la valeur de ces données.

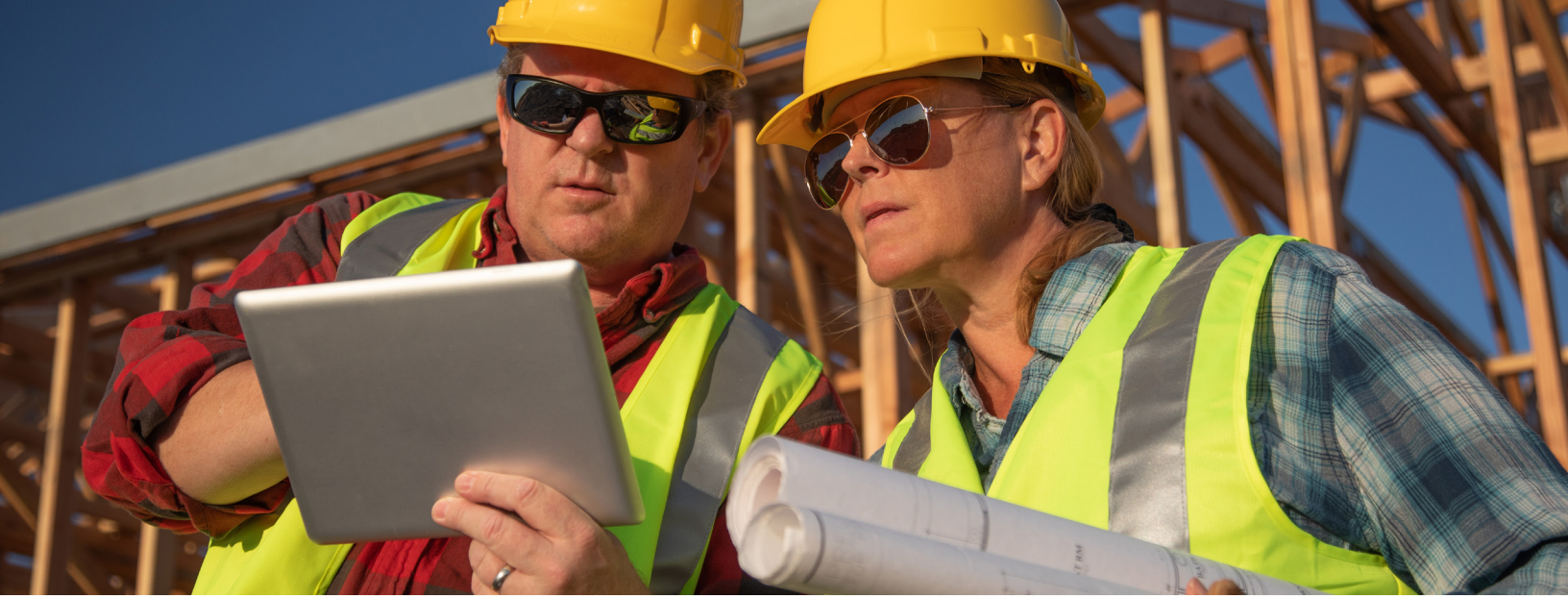
Les transferts de fonds frauduleux, également connus sous le nom de **compromission des paiements électroniques,** constituent un autre risque cybernétique auquel les entreprises de construction sont confrontées en raison du montant substantiel des fonds transférés sur divers comptes d'entreprises, de clients ou de fournisseurs par l'intermédiaire des services bancaires en ligne. Les virements frauduleux sont souvent le résultat du piratage psychologique, qui implique une manipulation psychologique par les cybercriminels qui utilisent des courriels et des appels téléphoniques spécifiquement conçus pour déclencher des réactions émotionnelles, comme un sentiment d'urgence ou de peur, afin de gagner la confiance d'une victime qui ne se doute de rien. Les cybercriminels attirent la victime ou la trompent pour qu'elle donne accès à des systèmes restreints, en exposant des données privées ou en téléchargeant des logiciels malveillants.

Les entreprises de conception et de construction sont également confrontées à des attaques de piratage psychologique, d'hameçonnage et d'harponnage, ainsi qu'à des violations internes et externes de la part d'acteurs malveillants qui tentent d'infiltrer leurs systèmes informatiques pour accéder à des informations privées et perturber les activités de l'entreprise.

En comprenant les caractéristiques des différentes cybermenaces, les entreprises seront en mesure d'identifier leurs vulnérabilités, de mettre en œuvre des mesures de sécurité appropriées et d'élaborer un plan d'action en cas de violation.

LE SAVIEZ VOUS?

Les failles liées à l'hameçonnage ont coûté en moyenne 4,72 millions $ aux entreprises en 2023.



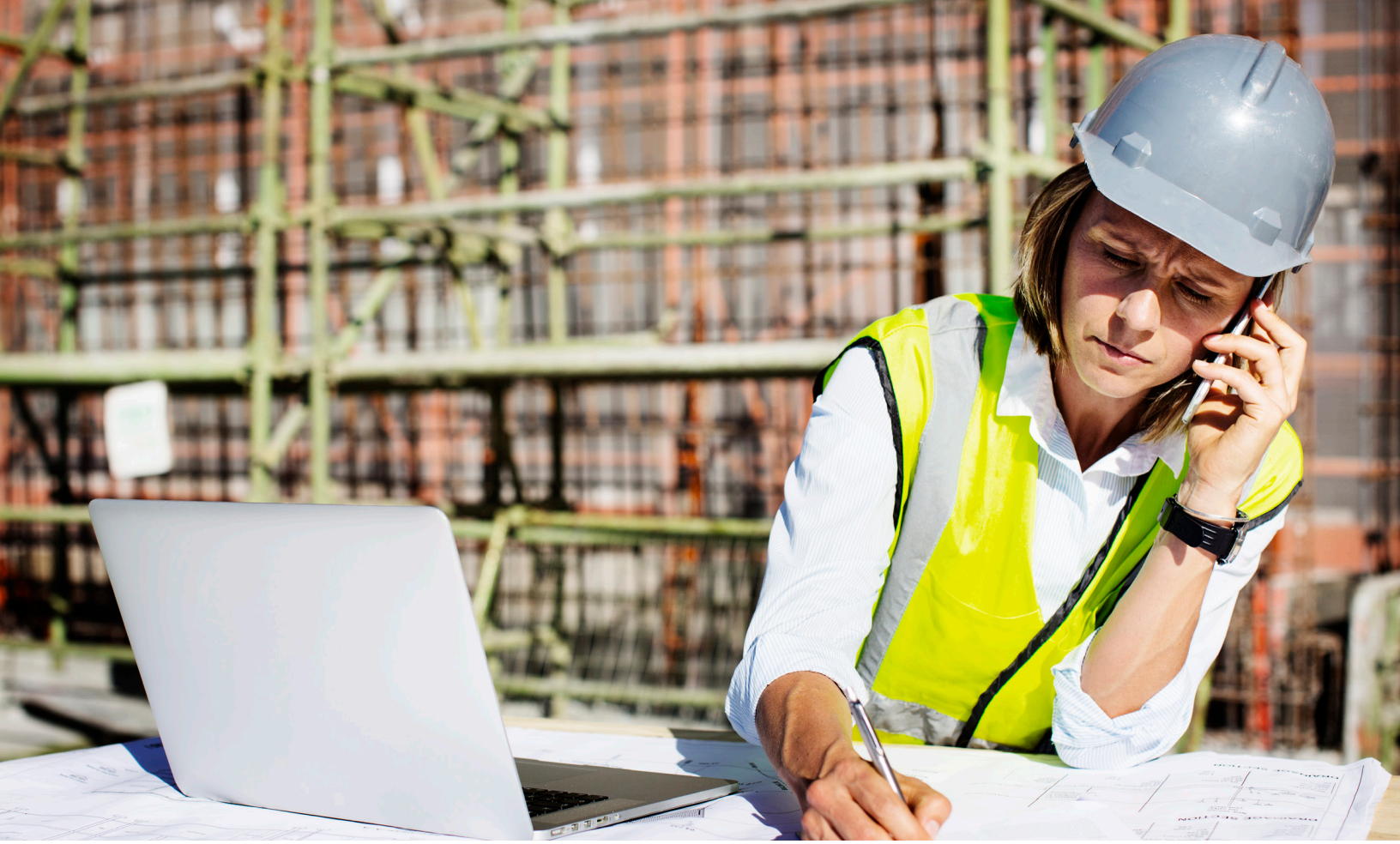
Le Comment.

Planifier et prévenir

Bien que les cybermenaces soient de plus en plus répandues, les entreprises de construction peuvent prendre des mesures préventives pour minimiser les risques. Un programme efficace commence par l'instauration d'une culture de la sécurité en choisissant et en soutenant une personne au sein de l'organisation pour prendre en charge et gérer les risques liés à la cybersécurité. Pour se protéger, les entreprises de construction devraient :

- **Crypter les données, mettre à jour les logiciels et les pare-feu.** L'un des moyens les plus faciles pour les cybercriminels d'accéder aux données de l'entreprise est de passer par des logiciels et des applications obsolètes. Qu'il s'agisse de logiciels de fournisseurs tiers reconnus ou d'applications personnalisées créées par l'équipe informatique de l'entreprise, il convient de toujours corriger les vulnérabilités et de les mettre à jour régulièrement. L'activation ou la configuration du cryptage des données protège également les données sensibles en transit ou au repos.

- **Former le personnel à la cybersécurité.** Les cybercriminels peuvent accéder aux données de l'entreprise et transférer des fonds par l'intermédiaire des employés en recourant au piratage psychologique et à des escroqueries au faux ordre de virement. Apprenez à vos employés comment traiter les informations confidentielles, mettez en place des processus en plusieurs étapes pour confirmer les changements de routage bancaire des fournisseurs ou des clients, identifiez les cybermenaces et signalez les liens suspects et toute autre activité douteuse.



○ **Utiliser l'authentification multifacteur (AMF).** Cette méthode fournit une couche de sécurité supplémentaire lors de l'accès à des informations sensibles, telles que les comptes bancaires, les factures de construction et les documents juridiques. En plus de s'assurer que l'AMF est mise en œuvre pour l'accès au courrier électronique et au réseau de l'entreprise, elle devrait également être utilisée pour protéger les comptes privilégiés ou les comptes d'administrateur système et être exigée pour l'accès aux sauvegardes du système.

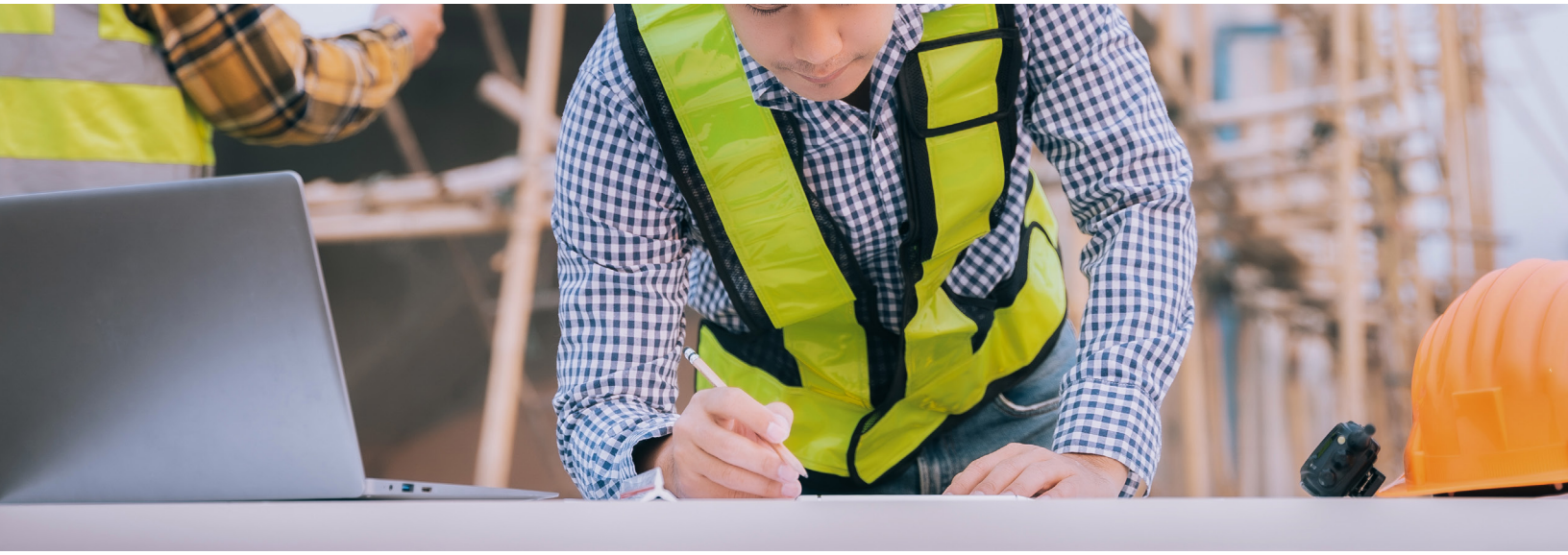
○ **Élaborer un plan d'intervention en cas d'incident et le mettre à l'épreuve.** Sachez quoi faire, qui appeler et comment vous mobiliser en cas de cyberattaque. Consultez des experts en la matière, notamment des spécialistes des technologies de l'information, des équipes d'intervention en cas d'incident, des courtiers d'assurance et des spécialistes en matière d'intervention en cas d'atteinte à la vie privée. Sachez également ce qu'il ne faut pas faire en cas de violation pour éviter de compromettre davantage la sécurité et la réputation de l'entreprise. Donnez vie à ces plans en organisant des exercices de préparation comprenant des jeux de rôle.

- **Prioriser les risques externes.** Identifiez et atténuez les cyber-risques lors de la collaboration avec des organisations externes. Examinez et renforcez les relations contractuelles afin de vous assurer que des mesures de protection adéquates en matière de cybersécurité sont en place pour tous les participants au projet, y compris les sous-traitants, les vendeurs et les fournisseurs.

- **Souscrire une assurance adéquate.** Faites appel à des professionnels de l'assurance et à des spécialistes des services de gestion des risques de confiance pour obtenir une protection suffisante en matière de cybersécurité et mettre en œuvre des stratégies d'atténuation des risques.

Les entreprises de construction doivent établir des bases solides en matière de cybersécurité afin de protéger leurs actifs numériques et les informations confidentielles de leurs clients et de leurs partenaires commerciaux.

Contactez les **spécialistes de l'assurance construction de HUB International** pour en savoir plus sur la protection de votre entreprise contre une cyberattaque.

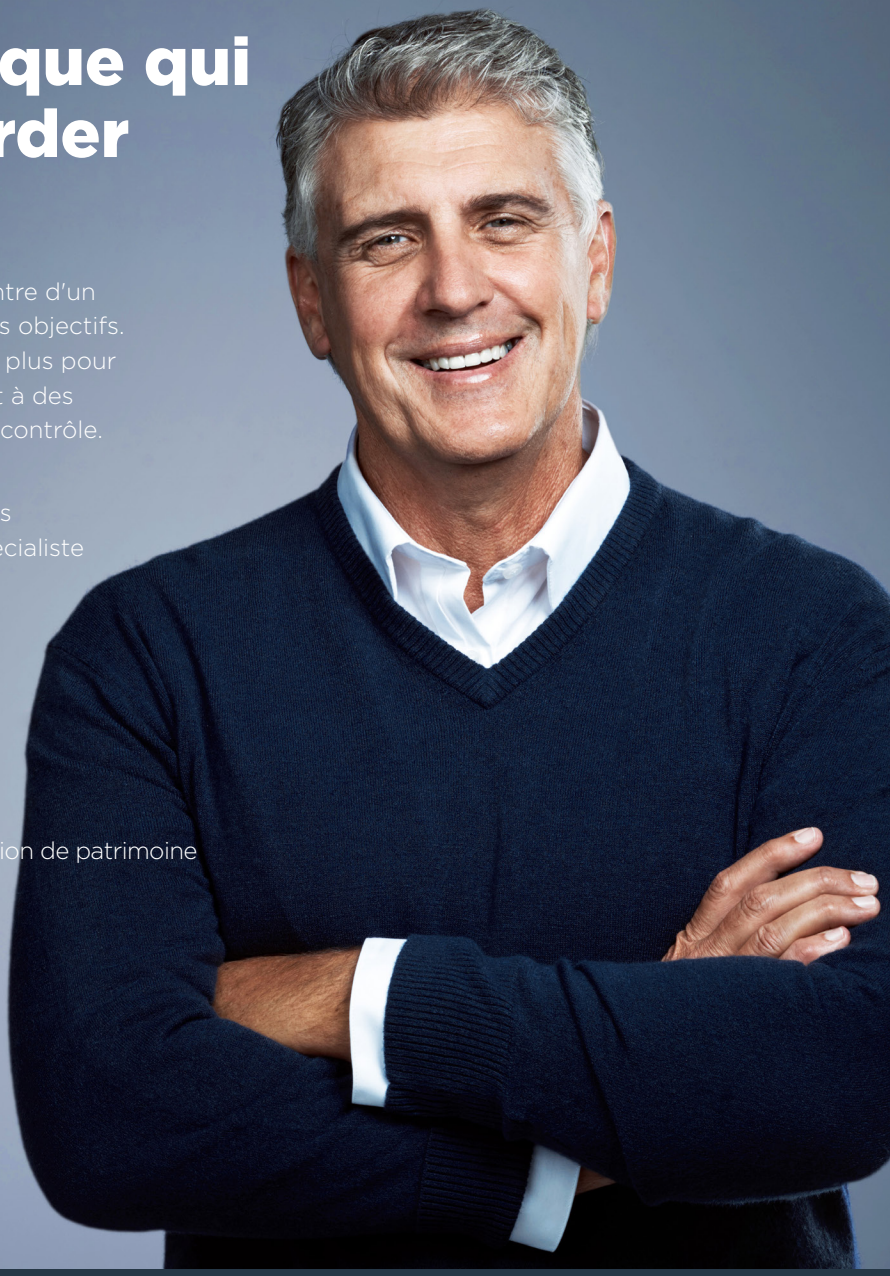


Un soutien stratégique qui vous permet de garder le contrôle.

Lorsque vous faites équipe avec nous, vous êtes au centre d'un vaste réseau d'experts qui vous aideront à atteindre vos objectifs. Avec HUB, vous avez la certitude que ce qui compte le plus pour vous sera protégé — grâce à un soutien sans relâche et à des solutions sur mesure qui vous permettent de garder le contrôle.

Pour plus d'informations sur la façon de gérer vos coûts d'assurance et de réduire vos risques, contactez un spécialiste de l'assurance construction de HUB.

hubinternational.com/construction



Prêt pour demain.

Risque et assurance | Avantages sociaux | Retraite et gestion de patrimoine

hubinternational.com

HUB