/ par Pascal Clerc, Practice Leader Financial lines chez Kessler & Co SA
Alexandre Voisin, Risk Consultant chez Kessler Consulting SA

Les défis et les clés de la gestion des risques

BÂTIR LA CYBERSÉCURITÉ

La cybersécurité est un enjeu majeur de notre époque. Le secteur de la construction n'échappe pas à ce risque croissant. Les experts de Kessler font le point pour vous.

Comme tout secteur économique, le monde de la construction n'échappe pas, depuis quelques années, aux cyberincidents dont le nombre est en constante augmentation. Pour mémoire, le groupe français Saint-Gobain avait été durement touché lors d'une cyberattaque par ransomware, dont les préjudices avaient été évalués à 250 millions d'euros sous forme de baisse des ventes et à 80 millions d'euros sur le résultat d'exploitation de 2017. Plus récemment et plus proche de nous, des entreprises romandes ont été impactées par des cyberattaques, réduisant leur capacité à fonctionner normalement.

LA PROTECTION DES DONNÉES SENSIBLES

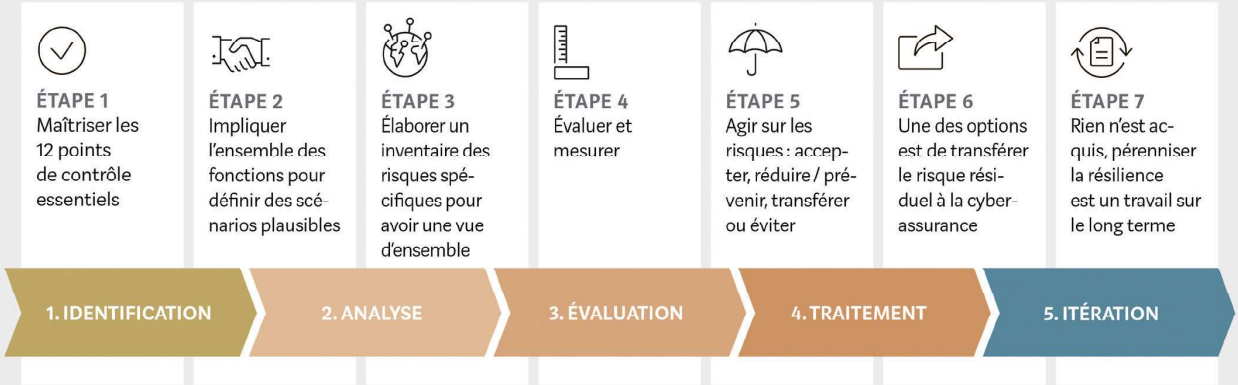
La cybersécurité est donc aussi – et contre toute idée reçue – un enjeu majeur dans la construction, impliquant la protection des données sensibles et spécifiques comme celles transmises au travers du BIM ou encore les informations financières. Les systèmes collaboratifs et de contrôle des chantiers, ainsi que l'automatisation croissante de la gestion des infrastructures exposent le secteur à des risques de cyberattaques pouvant causer des dommages matériels, pécuniers, voire même corporels. Ces attaques sont capables de perturber les opérations de construction et d'entraîner des conséquences légales voire contractuelles. Enfin, les vulnérabilités liées à la chaîne d'approvisionnement ne doivent pas être sous-estimées car les partenaires et fournisseurs constituent aussi des cibles potentielles.

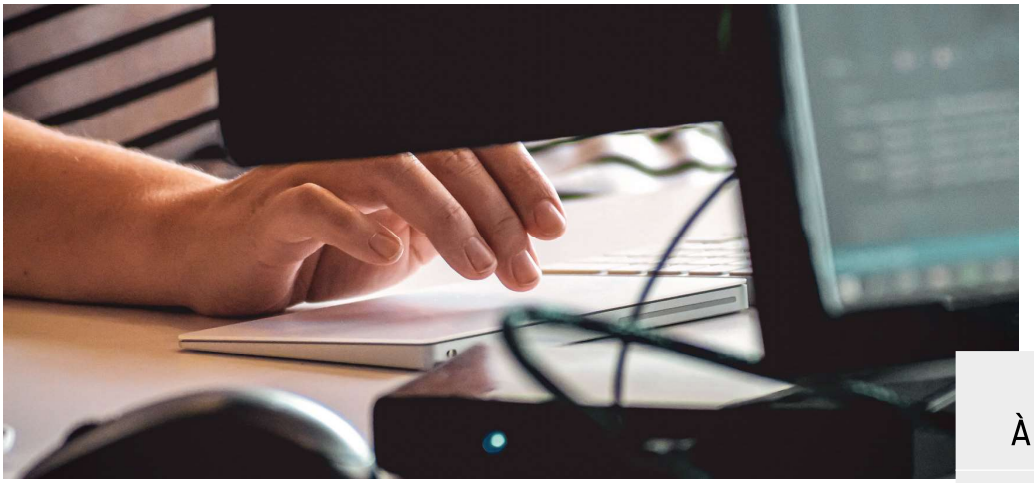
CHOISIR EN CONNAISSANCE DE CAUSE

Il est essentiel d'identifier et de bien connaître ces risques pour prendre les mesures de prévention et de protection qui s'imposent. Tout est dans l'anticipation ! Plus on attend, plus les répercussions réputationnelles et financières peuvent être importantes. Les montants en jeu peuvent vite être colossaux, compte tenu notamment des multiples spécialistes à solliciter pour gérer la crise, mais aussi pour parer aux dommages propres et causés à des tiers. Le Conseil d'administration doit donc pouvoir décider en toute connaissance de cause de l'allocation des ressources humaines et financières. De fait, cette thématique doit lui être présentée dans son ensemble et les décisions doivent être clairement documentées. La démarche passe notamment par des audits des systèmes (identifier les failles, etc.), par une évaluation des risques majeurs selon le modèle d'affaires (que se passerait-il si cela devait arriver ?) et par la prise en compte du risque résiduel (souhaite-t-on transférer ce risque à un tiers, comme une assurance ?).

PROCESSUS DE GESTION DES RISQUES

Les 7 étapes incontournables pour adresser les risques de manière optimale en intégrant le rapport coûts / bénéfices.





MATURITÉ DES ENTREPRISES

Dans ce contexte particulier, le marché de la cyberassurance s'est mobilisé et a réagi en posant de nouveaux standards en termes de cybersécurité, l'objectif étant de réduire la sévérité et la fréquence des incidents au sein des entreprises.

Afin de garantir aux sociétés un haut niveau de résilience et de permettre un transfert du risque résiduel sur le marché de l'assurance, le réseau Marsh a élaboré une liste exhaustive de douze contrôles clés, basée sur des données recueillies dans le cadre de plus de 25 ans d'expérience.

12 CONTRÔLES CLÉS

Voici la liste (schéma ci-dessous) des points critiques destinés à renforcer la cybersécurité au sein de votre entreprise.

Nous observons régulièrement un décalage entre les bonnes pratiques et les mesures mises en place par les entreprises en raison de contraintes parfois budgétaires ou tout simplement liées à un manque de ressources internes. Le choix des priorités, qui incombe in fine au Conseil d'administration, est critique pour maximiser l'efficacité des mesures de cybersécurité à mettre en place. Certains outils de modélisation peuvent aider à renforcer la protection d'une entreprise, plus largement à identifier les pertes potentielles qu'une société pourrait subir, ainsi que les économies possibles qu'elle pourrait réaliser en adoptant de meilleures pratiques en matière de cybersécurité.

UNE APPROCHE HOLISTIQUE

Il ressort de notre expérience que la réponse adéquate à cette problématique requiert l'adoption d'une approche holistique et proactive quant à la gestion des cyberrisques au sein de l'entreprise. L'enjeu est de préserver la disponibilité, l'intégrité et la confidentialité des données (en application de la nLPD).

En conclusion, pour garantir la continuité des opérations, la sécurité des données et la protection de la réputation de l'entreprise, il est important de rappeler la nécessité de s'entourer de partenaires fiables et expérimentés. En effet, les défis auxquels le secteur de la construction est confronté se complexifient au rythme d'une digitalisation accrue. ⊗

À propos de Kessler

Kessler est l'entreprise suisse leader en matière de gestion des risques, de conseil en assurances et de prévoyance professionnelle. Elle regroupe 330 collaborateurs en Suisse et assure le suivi de plus de 1500 moyennes et grandes entreprises suisses issues des services, du commerce et de l'industrie, notamment le secteur de la construction (y compris infrastructure et énergie), ainsi que du secteur public. Spécialisée dans le Risk Management, elle comprend un Team Construction composé d'une dizaine d'experts pour la Suisse romande, sous la direction de Mélanie Coluccia, Responsable Infrastructure & Énergie.

Besoin d'un conseil complet en gestion des risques dans le domaine de la construction ?

kessler.ch

12 CONTRÔLES CLÉS POUR RENFORCER VOTRE SÉCURITÉ

- Authentification multi-facteurs pour tous les accès externes **(MFA)**
- Un concept de **sauvegarde** solide
- **Formation régulière** et actualisée sur la protection des données et la sécurité des informations
- Plans de réponse aux cyber-incidents existants et testés
- Traitement et protection des comptes d'utilisateur, des droits d'utilisateur et d'accès **(PAM)**
- Surveillance et détection efficaces des cyberévènements **(EDR)**
- **Segmentation** appropriée du réseau, cryptage approprié pour la transmission et le stockage des données (notamment personnelles)
- Mesures et outils efficaces contre les logiciels malveillants et les ransomwares
- Organisation et gouvernance appropriées en matière de cybersécurité
- Gestion efficace des correctifs **(patch management)**

Source: «Top Cybersecurity Controls» Marsh, 2022