Deloitte.

Une bonne longueur d'avance : comment renforcer la cybersécurité dans le secteur des sciences de la vie et des soins de santé

Si le renforcement de l'analytique et du signalement des cyberrisques constitue une étape cruciale pour les organisations du secteur des sciences de la vie et des soins de santé, ce n'est à certains égards qu'une première étape.

En octobre 2020, trois organismes américains ont uni leurs forces pour lancer un avertissement sévère aux hôpitaux et aux fournisseurs de soins de santé : les attaques de rançongiciels sont de plus en plus fréquentes, et les institutions doivent immédiatement prendre des mesures pour se protéger.

Selon le rapport, produit conjointement par l'Agence américaine de cybersécurité et de sécurité des infrastructures (CISA), le Federal Bureau of Investigation (FBI) et le département de la Santé et des Services sociaux (HHS) des États-Unis, les attaques de rançongiciels, les interruptions de service et les vols de données ont tous considérablement augmenté dans le secteur depuis 2019, et la pandémie de COVID-19 n'a fait qu'aggraver le problème.[1]

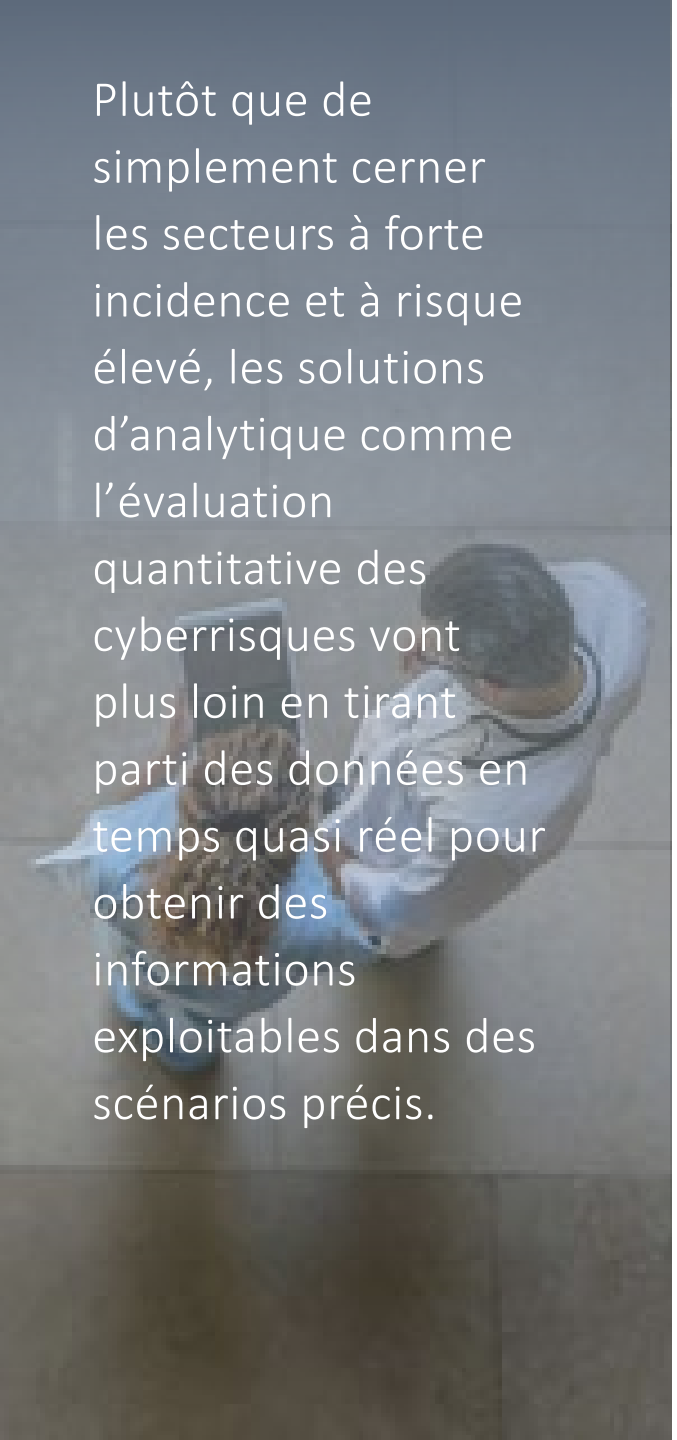
En termes clairs, les cybercriminels considèrent les organisations du secteur des sciences de la vie et des soins de santé non seulement comme une source de revenus importants, mais également comme une mine de données sensibles. Afin de contrer ces menaces, le moment est venu pour le secteur de relever son niveau de jeu en ce qui a trait à la cybersécurité.

Oublier l'ancienne méthode

Le défi découle en partie du fait que plusieurs institutions du secteur des sciences de la vie et des soins de santé évaluent actuellement les risques en se fondant sur une estimation qualitative et sur une opinion non validée. Quel est le problème? Une telle approche est à la fois vague et mal adaptée aux cybermenaces avancées d'aujourd'hui.

Afin de monter dans l'échelle de maturité, les chefs de la sécurité de l'information doivent réellement établir les priorités des secteurs les plus exposés à des risques et les gérer, sécuriser les données des employés et des patients, et bien déterminer les systèmes d'entreprise et les normes qui sont indispensables pour faire avancer les choses, ce qui nécessite l'accès à une robuste approche d'analytique et de signalement des cyberrisques. Pour prendre des décisions plus éclairées et établir des objectifs à l'échelle de l'entreprise, ils doivent disposer de rapports et de tableaux de bord visuels sur les cyberrisques qui sont aussi crédibles, défendables et exploitables que les états financiers.

[1]Agence américaine de cybersécurité et de sécurité des infrastructures, *Ransomware Activity Targeting the Healthcare and Public Health Sector*, 2020.



Une nouvelle approche de signalement des cyberrisques

Pour avoir une vue d'ensemble des secteurs à risque les plus critiques et de leurs angles morts, les organisations d'aujourd'hui se tournent par conséquent vers des solutions d'analytique plus avancées.

Plutôt que de simplement cerner les secteurs à forte incidence et à risque élevé, ces approches vont plus loin en tirant parti de données en temps quasi réel pour obtenir des informations exploitables dans des scénarios précis. Ainsi, tandis qu'une approche traditionnelle de gestion des cyberrisques pourrait permettre de repérer un risque élevé d'atteinte à la réputation, une approche orientée sur les données pourrait quant à elle indiquer non seulement l'application susceptible de contribuer à ce risque, mais également les mesures qui peuvent être prises pour l'atténuer. À un niveau plus détaillé, elle pourrait sans doute même montrer que le risque peut être réduit de X % en utilisant un certain type de serveur sécurisé.

En fait, un tel niveau d'information pourrait :

- fournir à la direction et au conseil d'administration une vision claire des cyberrisques ainsi que des renseignements sur les régions, les secteurs d'activité et les services vulnérables;
- permettre d'appliquer un cadre de cybersécurité généralement reconnu (p. ex., cadre de cybersécurité du NIST, FAIR, etc.);
- soutenir la prise de décisions en calculant des cotes de cyberrisque à partir de données en temps quasi réel, et consolider ces données tirées de systèmes et d'entités variés;
- donner lieu à des analyses plus précises des causes profondes.

Cette capacité peut permettre aux institutions du domaine des sciences de la vie et des soins de santé de regrouper, de normaliser et d'enrichir leurs données. Elle associe un risque à des secteurs précis de l'organisation – par exemple, une gamme de produits ou un hôpital donné – et elle peut aider ces institutions à améliorer leur position relativement aux risques en prenant de meilleures décisions d'investissement qui sont harmonisées avec leur stratégie de cybersécurité. En toute logique, elle peut permettre ce qui suit :

- **Cotation des risques relatifs normalisée.** En quantifiant les risques selon une échelle normalisée et en examinant des facteurs comme les processus, la criticité des actifs, la vulnérabilité et la gravité des menaces, les chefs de la sécurité de l'information peuvent comparer les risques de façon plus précise dans l'ensemble de l'organisation, puis établir les priorités des initiatives de réduction des cyberrisques.
- **Modélisation de scénarios et analytique prédictive.** L'analytique et le signalement des cyberrisques permettent aux chefs de la sécurité de l'information d'effectuer des analyses par simulation afin de repérer des occasions de diminuer leur cote de cyberrisque.
- **Valeur à risque (VAR) et rendement du capital investi (RCI) en dollars.** Les solutions fondées sur les données permettent de quantifier les risques en termes financiers dans le but de pouvoir comparer les coûts, les avantages et le RCI de chaque décision d'affaires. La valeur à risque est un élément particulièrement utile permettant à chaque personne au sein de l'organisation – de la direction à la fonction finance, en passant par la gestion des opérations – d'avoir la même conception des risques.
- **Pouvoir de décision conjoint.** Les dirigeants abordent tous l'évaluation des risques différemment selon le niveau où ils se situent dans l'organisation, le degré de supervision qu'ils exercent et leurs priorités. Grâce aux solutions d'analytique et de signalement des cyberrisques, chacun peut extraire différentes perspectives des données afin de trouver des réponses à ses questions les plus pertinentes sur les cyberrisques et de prendre des décisions en conséquence.
- **Informations exploitables.** Les solutions actuelles ne se limitent pas à cerner les risques les plus pertinents. Elles fournissent également des informations exploitables qui contribuent à favoriser leur atténuation proactive.

Le signalement n'est qu'un début

Si le renforcement de l'analytique et du signalement des cyberrisques constitue une étape cruciale pour les organisations du secteur des sciences de la vie et des soins de santé, ce n'est à certains égards qu'une première étape. Une fois les bases établies pour gérer activement les cyberrisques au moyen des données et pour favoriser la prise de mesures contribuant à l'atteinte des IRC, il devient possible d'utiliser ces données pour faire progresser l'organisation davantage.

Par exemple, une fois que vous possédez suffisamment d'information sur l'incidence financière de vos décisions d'affaires, vous pouvez déterminer à quoi affecter vos prochains investissements pour obtenir un meilleur rendement. Vous pouvez aussi mieux définir votre tolérance aux risques idéale et évaluer avec plus de précision le niveau de risque d'investissement que vous êtes disposé à accepter. De plus, selon votre niveau de maturité, vous pouvez bénéficier d'une visibilité sans précédent des risques cachés, et prendre des mesures axées sur la gestion avisée des risques, qui pourraient consister à renforcer les contrôles, à affecter des ressources supplémentaires ou à atténuer les risques par le biais d'une police de cyberassurance.

En passant de l'analytique et du signalement avancés à l'évaluation quantitative des cyberrisques, les organisations devraient pouvoir faire plus que fortifier leurs moyens de défense contre les individus mal intentionnés. Cette solution devrait également positionner un secteur mis à rude épreuve afin qu'il puisse renforcer la sécurité des données, mieux protéger la vie privée des gens, et prendre des décisions d'investissement harmonisées avec les priorités stratégiques.

Personne-ressource

Amir Belkhelladi | Associé, Leader de la Cybersécurité, Canada
+1 514 393 7035
abelkhelladi@deloitte.ca