L’information confidentielle

Caroline Baker

Josephine Rendall-Neal

12th May 2022

LinkedIn
Twitter
Email
Print

Il y a quelques mois, l’industrie de l'édition à Londres a été bouleversée par une histoire hors du commun : un employé subalterne chez une maison d’édition avait été arrêté par le FBI et accusé d’avoir volé des centaines de manuscrits non publiés en usurpant l’identité de personnes littéraires connues (y compris des auteurs célèbres tels que Margaret Atwood et Sally Rooney). Son employeur a suspendu son contrat de travail immédiatement. Les détails de cette affaire (en anglais) sont disponibles ici.

Bien que ceci soit une affaire aux faits exagérés – la plupart des employeurs ne verront jamais le FBI frapper à leur porte – c’est un rappel utile pour les employeurs qu’il est extrêmement important de protéger leurs informations confidentielles. Il y a certaines démarches que toutes sociétés peuvent entreprendre pour se protéger :

- La société peut limiter l’accès à l’information qu’elle souhaite protéger selon la sensibilité de cette dernière et la catégorie de l’employé (leur département/équipe, leur ancienneté, etc.). Lorsqu’il s’agit des informations les plus sensibles (par exemple, concernant une fusion

ou acquisition, ou un projet de recherche extrêmement important), la société peut renforcer la protection autour de cette information en la divulguant seulement aux employés qui ont strictement besoin de connaitre l'information pour effectuer leur travail, et en éliminant tout autre accès à l'information. Cela permet de limiter les risques qu'elle soit divulguée, et au cas où il y aurait une fuite, de permettre à la société d'identifier la source plus facilement.

- Les employeurs doivent s'assurer que leurs salariés puissent repérer les signes d'une tentative de « phishing ». Dans l'exemple dont nous parlions ci-dessus, le criminel usurpait l'identité de personnes connues en utilisant des faux noms de domaines et des adresses électroniques qui étaient assez semblables à ceux utilisés par les personnes réelles pour tromper ses interlocuteurs. Les employeurs feraient bien d'alerter leurs salariés aux dangers du phishing et de leur donner les outils nécessaires pour pouvoir reconnaitre les différentes menaces, et réagir de façon appropriée afin de protéger la société. Ceci peut être effectué par la mise en place d'une politique informatique, ou par des séances de formation. Les meilleurs systèmes informatiques au monde ne vous sauverons pas si un salarié est dupé et envoie un document clé à un escroc.
- Les employeurs feraient bien de garder un œil sur leurs contrats de travails et de s'assurer que ceux-ci restent à jour. Les protections contractuelles dont profite la société doivent être solides et précises pour protéger les informations confidentielles de l'organisation. Pour protéger les informations les plus sensibles, il est parfois prudent de mettre en place des accords de confidentialité avec les salariés qui y auront accès par-dessus leurs contrats de travails.

Pour conclure, la chose la plus importante pour les amoureux de la littérature est la suivante : même si vous voulez vraiment lire le prochain roman de Margaret Atwood, une peine criminelle n'en vaut pas la peine (probablement)

