DocuSign®

Livre blanc

Sécurité et juridique: une collaboration indispensable

Comment des équipes performantes travaillent ensemble pour assurer la sécurité des applications, la détection des menaces et le respect des règles

Présentation: objectifs communs, rôles complémentaires

Les services juridiques et de sécurité partagent l'objectif commun de protéger une entreprise contre tout préjudice. Mais même si les deux ont comme mission de veiller à la sécurité et à la conformité, les équipes respectives jouent des rôles distincts dans la réalisation de ces objectifs. Grâce à une collaboration étroite et à une communication régulière, chaque équipe peut aider l'autre à optimiser la sécurité et la conformité dans l'ensemble de l'entreprise.

Dans certaines entreprises, le service juridique élabore des politiques de sécurité et/ou de traitement des données à l'intention des employés, afin de garantir un traitement approprié des informations. Dans d'autres entreprises, ces politiques peuvent être mises au point par le service de sécurité en concertation avec le service juridique. Ces politiques aident à définir les informations sensibles, ce qui constitue une activité autorisée et le mécanisme par lequel répondre aux exigences de conformité contractuelle, réglementaire et interne. Le service juridique et la sécurité collaborent souvent avec les ressources humaines pour tenir les employés informés de ces politiques.

Selon les exigences de ces politiques, le service de sécurité déploie des outils et des processus visant à renforcer la visibilité et la vigilance dans l'écosystème de sécurité des données de l'entreprise; cela inclut généralement la surveillance des données sur le trafic et les activités, ainsi que l'analyse des comportements suspects. En cas d'incident touchant la sécurité ou d'autres données, le service de sécurité fera souvent appel au service juridique pour l'aider à évaluer la menace et à déterminer les mesures à prendre en vue d'atténuer toute atteinte à la réputation et aux finances, ainsi que tout autre préjudice potentiel à l'entreprise.

Le point de départ d'une collaboration fructueuse entre les services de sécurité et juridique consiste en une définition claire des rôles et des responsabilités ainsi qu'une planification proactive, avant la survenance d'une violation ou d'un incident touchant les données. La planification en amont est cruciale, car les employés donnent rarement le meilleur d'eux-mêmes dans des situations de violation, et une démarche improvisée peut compliquer davantage la réponse d'une entreprise, notamment en ce qui concerne la signification de notifications de violation qui peut être requise en vertu des réglementations pertinentes.

Les plans complets doivent inclure la surveillance quotidienne des activités sur les applications utilisateurs et tierces, ainsi que des procédures détaillées de réponse aux incidents en vue de s'attaquer aux activités suspectes ou aux violations. Dans le cadre de l'élaboration de ces plans, les services juridiques et de sécurité doivent traiter sur un pied d'égalité tant les menaces externes qu'internes. Bien que les menaces externes soient généralement plus médiatisées, certaines menaces pour une entreprise peuvent émaner de la négligence ou d'une malversation de la part d'un employé ou d'un manque de formation de celui-ci.

Lors de l'évaluation des applications tierces, les services juridiques et de sécurité se doivent d'interagir afin de s'assurer que ces outils sont sûrs et conformes aux politiques pertinentes. Par la force des choses, cette interaction commence par l'étape d'évaluation et d'intégration et se poursuit par les étapes de mise en œuvre et de maintenance.

Une relation étroite et symbiotique entre les services juridique et de sécurité permet de protéger l'entreprise et ses données, ainsi que de les mettre en situation de conformité. Collectivement, ces services protègent l'entreprise en élaborant, en communiquant et en appliquant des politiques et des procédures efficaces en matière de sécurité et de traitement des données.

Le présent livre blanc se penche sur les liens réciproques entre les équipes juridiques et de sécurité des entreprises et met en lumière les meilleures pratiques aux fins d'une collaboration fructueuse. Les contributions intégrées au présent document ont été recueillies lors d'entretiens avec les responsables juridiques et de sécurité de DocuSign, ainsi que des experts du cabinet d'avocats DLA Piper.

Le défi de la prévention des activités non autorisées

Les équipes de sécurité sont chargées de détecter et de maîtriser toute une série de menaces, qu'elles proviennent de l'extérieur ou de l'intérieur de l'entreprise. Alors que les menaces externes sont généralement identifiées au niveau du réseau, des attaques de plus en plus sophistiquées comme l'hameçonnage peuvent être mieux traitées dans une application.

Les menaces internes et les activités non autorisées peuvent également être particulièrement difficiles à détecter, car elles peuvent être intentionnelles, malveillantes ou involontaires, faisant suite à une négligence ou à une erreur humaine anodine. Avant d'attirer l'attention sur l'urgence de s'attaquer à ces menaces, l'équipe de sécurité doit d'abord définir ce qui constitue une activité suspecte ou non autorisée.

Risques inhérents aux menaces internes

Les violations attribuées à une activité non autorisée, comme la négligence de la part d'un employé ou d'un sous-traitant, peuvent être tout aussi préjudiciables, sinon plus, que les violations malveillantes. Quelle que soit l'intention derrière la violation ou l'origine de celle-ci, le risque auquel s'expose une entreprise est tout aussi grave.

L'édition 2020 de l'étude « Cost of a Data Breach » menée par l'institut Ponemon a révélé que:

- 7% des violations malveillantes trouvent leur source dans des actes commis par des employés en place
- 19% des violations malveillantes sont attribuées à des identifiants volés ou compromis
- 23% de l'ensemble des violations sont attribuées à une erreur humaine comme la négligence de la part d'un employé ou d'un sous-traitant

Ces chiffres démontrent que les menaces proviennent souvent de l'intérieur d'une entreprise, et non seulement de « mauvais joueurs » externes. En outre, l'étude de Ponemon semble révéler que même les menaces externes peuvent être attribuées à une activité non autorisée d'un employé ou être exacerbées par celle-ci.

7%
des violations malveillantes trouvent leur source dans des actes commis par des employés en place

19%
es violations malveillantes sont attribuées à des identifiants volés ou compromis

23%
de l'ensemble des violations sont attribuées à une erreur humaine comme la négligence de la part d'un employé ou d'un sous-traitant

Source: L'édition 2020 de l'étude «Cost of a Data Breach» menée par l'institut Ponemon

«Il est important de surveiller les activités des utilisateurs et d'analyser leur comportement afin de détecter les anomalies et les intrusions potentielles pour protéger l'entreprise. Une violation de la politique par un employé peut être une erreur de sa part commise en toute innocence ou un signe d'activités malveillantes. Il incombe aux équipes de sécurité de repérer cette activité et de la faire remonter au service juridique si nécessaire».

Andrew Serwin
Associé, président de la branche américaine et co-président mondial, segment Protection, confidentialité et sécurité des données et cybersécurité
DLA Piper

Mise en place des politiques de sécurité et de traitement des données

Alors qu'il revient aux équipes de sécurité de prévenir et de détecter des menaces, ainsi que de répondre à celles-ci, il incombe aux équipes juridiques de mettre l'entreprise en adéquation avec ses politiques internes, les réglementations externes et les obligations contractuelles qu'elle peut avoir envers des tiers relativement aux contrôles de la sécurité et du traitement des données. Pour cette raison, et dans certains cas, l'équipe juridique peut être considérée comme l'architecte de la politique de sécurité.

Comment le service juridique oriente-t-il la politique de sécurité?

Lors de la mise en place d'une politique de sécurité efficace, le service juridique peut évaluer les forces et les faiblesses de l'entreprise, en s'appuyant sur les données provenant directement du service de sécurité, afin de déterminer le risque. Les politiques de sécurité et de traitement des données combinent les obligations de conformité à l'égard des lois sur la confidentialité des données, des exigences réglementaires, des engagements contractuels et des procédures opérationnelles pertinentes. D'abord et avant tout, des politiques peuvent être élaborées pour exonérer l'entreprise de toute responsabilité. Cependant, des politiques efficaces devraient également inclure des directives globales sur la sécurité des données et des mesures normatives comme les capacités d'intervention en matière d'audit, de rapport et d'incidents.

Ces politiques donnent le ton des priorités en matière de sécurité au sein d'une entreprise et permettent d'identifier les mécanismes par lesquels les informations sensibles ou confidentielles doivent être gérées. Ce cadre peut également aider l'équipe de sécurité à déployer des ressources de manière stratégique afin de protéger l'entreprise en fonction de la source la plus probable des menaces.

Par exemple, si une politique de sécurité identifie un risque associé aux données stockées dans une application tierce, l'équipe de sécurité peut consacrer des ressources supplémentaires au suivi des activités sur cette application afin de détecter toute activité non autorisée.

«Des politiques de sécurité et de traitement des données sont mises en œuvre pour prévenir l'exposition aux risques et aider à assurer la conformité. Nous travaillons en étroite collaboration avec le service juridique pour comprendre le risque commercial associé au non-respect des politiques, et le risque de non-conformité lié aux réglementations. L'équipe de sécurité est appelée à surveiller et à protéger les données selon une norme. Par ailleurs, en cas de survenance d'une activité non autorisée, le concours de l'équipe juridique doit également être sollicité pour aider à évaluer l'ampleur du problème et la responsabilité potentielle de l'entreprise».

Niall McGrath
Directeur principal des opérations de sécurité
DocuSign

Application des politiques de sécurité des données

Pour une entreprise, les équipes de sécurité sont les spécialistes en la matière et sont donc généralement censées prendre les mesures nécessaires visant à protéger les données de l'entreprise. D'un point de vue technique, les équipes de sécurité surveillent les données sur le trafic et les activités. Elles collaborent également avec le service informatique pour définir les niveaux d'autorisation qui minimisent le risque de compromission des informations sensibles. Le service de sécurité doit également anticiper les menaces et s'efforcer de remédier aux vulnérabilités susceptibles d'être exploitées par des acteurs malveillants.

Plans et guides pratiques de réponse aux incidents

Les plans et guides pratiques de réponse aux incidents (RI) sont des atouts essentiels pour les équipes de sécurité chargées d'organiser des opérations contre d'éventuelles menaces. Un guide pratique sur les RI se compose de réponses conditionnelles qui imposent des mesures dans un ordre étape par étape. Les réponses comprennent une combinaison de mesures automatiques fondées sur la technologie et des facteurs décisionnels humains, et incluent généralement des directives sur la façon de contenir des menaces et d'envoyer des notifications dans le cadre du processus des opérations de sécurité. Les guides pratiques sont généralement rédigés par le responsable de la sécurité des systèmes d'informations (RSSI), en consultation avec le service juridique, et doivent identifier l'ensemble étendu des parties prenantes clés de l'entreprise susceptibles d'être touchées par un incident. La consignation de ces informations peut contribuer à garantir l'alignement dans toute l'entreprise avec les réponses internes qui peuvent s'avérer nécessaires, au-delà des équipes juridiques et de sécurité, soit les premiers intervenants.

«Les guides pratiques sont normatifs quant à la communication et aux points de décision Oui/Non. Plus l'équipe de sécurité peut fournir des informations détaillées au service juridique, meilleures seront les décisions que celui-ci peut prendre quant à la marche à suivre».

Niall McGrath
Directeur principal des opérations de sécurité
DocuSign

Un guide pratique établit les critères d'évaluation des incidents de sécurité et fournit un guide étape par étape définissant les mesures à prendre à chaque étape. Ces critères aident les équipes à évaluer les incidents de sécurité afin de déterminer si une activité suspecte a été autorisée ou non.

En règle générale, les guides pratiques précisent également le moment auquel le service juridique doit intervenir dans le processus, et ce service collabore avec les équipes pour évaluer les étapes spécifiques « à suivre/ne pas suivre » et les exigences particulières en matière de rapports. Les guides pratiques peuvent préciser également les moyens par lesquels les équipes de sécurité doivent informer les services juridiques du statut d'un incident de sécurité et le moment auquel ils doivent le faire. Les guides pratiques mondiaux peuvent aussi aider les entreprises à normaliser les opérations de sécurité sur plusieurs sites, et le respect des consignes du guide pratique peut aboutir à des opérations de sécurité plus cohérentes et plus efficaces.

«Les services juridique et de sécurité se concertent pour définir les alertes. Le plan de réponse aux incidents de sécurité et les directives y afférentes sont rédigés par le RSSI et son équipe en tenant compte des critères prédéfinis. Le plan présente en détail les critères permettant la remontée d'informations au sein du service de sécurité et précise le moment auquel le service juridique, le responsable de la confidentialité (ou le délégué à la protection des données), le service de communication d'entreprise et le directeur de l'exploitation, entre autres, doivent intervenir».

Ronald Plesco
Associé, Confidentialité, sécurité et cybersécurité
DLA Piper

La sécurité comme détective

L'une des principales responsabilités du service de sécurité est d'analyser les données d'activités afin de détecter tout comportement suspect, et d'enquêter sur ce comportement pour déterminer s'il était interdit. Si le service de sécurité détecte une activité interdite susceptible de constituer une violation, il poursuivra son enquête sur cette activité et pourra prendre des mesures préliminaires comme la fermeture d'un compte, pour remédier à la menace.

Une fois la menace contenue, le service de sécurité doit recueillir toutes les informations pertinentes sur la violation et se reporter au guide pratique pour déterminer qui informer et quand. Les cas plus graves répondent généralement aux critères par défaut, pour être portés à l'attention du service juridique.

«Le service juridique collabore avec le service de sécurité lorsqu'un incident de traitement des données se produit. Le service de sécurité recueille généralement les données et enquête sur l'incident lui-même, les circonstances l'entourant et le moment auquel il s'est produit pour en déterminer la cause profonde. Le service juridique prête main-forte en ce qui concerne les politiques internes, les obligations de conformité réglementaire et autres obligations contractuelles auxquelles l'entreprise peut être soumise. Plus le service de sécurité peut fournir des informations au service juridique au début de l'enquête sur l'incident touchant les données, plus nous aurons une visibilité sur les défaillances du service de sécurité et de la protection des données. Cela nous place dans la meilleure position pour aider à assurer une conformité continue, à déterminer les moyens pour atténuer la responsabilité et à gérer correctement les risques associés à l'incident».

Cindy Rosser
Directrice des produits, de la propriété intellectuelle et des affaires réglementaires
DocuSign

Une fois notifié, le service juridique examine l'incident dans le contexte des politiques de sécurité et d'autres politiques pertinentes de l'entreprise, des lois et réglementations applicables en matière de protection des données et des obligations contractuelles. Les services de sécurité et juridique travaillent ensuite de concert pour s'en tenir au plan de réponse aux incidents, s'attaquer à la cause de l'incident et éviter d'autres préjudices à l'entreprise.

«Les services juridiques et de sécurité participent conjointement à l'élaboration des stratégies de sécurité. Si une situation difficile se présente, le service de sécurité active son processus de remontée d'informations. Le guide de réponse aux incidents de sécurité (guide RI) renferme des critères prédéfinis très clairs. Si ceci se produit, alors cela s'ensuivra».

Ronald Plesco
Associé, Confidentialité, sécurité et cybersécurité
DLA Piper

Comment le service juridique promeut-il la conformité?

Du point de vue du service juridique, il est essentiel de veiller à ce que l'entreprise se mette en conformité avec ses politiques internes, les réglementations gouvernementales et ses obligations contractuelles. Par conséquent, les politiques de conformité bien pensées doivent être axées sur la façon dont les entreprises gèrent les activités non autorisées dès lors qu'elles se rapportent à ces obligations. Il s'agit d'un point essentiel, car une activité non autorisée peut constituer un problème pour les services juridique, de sécurité, des RH ou d'autres services d'une entreprise, selon le service responsable de la politique.

Respect des réglementations en matière de protection des données

La conformité avec le RGPD, la HIPAA, la CCPA et d'autres réglementations sert de fondement à la sécurité des données et à d'autres politiques axées sur la conformité. Par exemple, la CCPA impose des directives strictes en matière de confidentialité des données et prévoit même des dommages-intérêts réglementaires par incident en cas de violation. Le service juridique doit travailler en étroite collaboration avec le service de sécurité pour veiller à la conformité avec les lois en vigueur sur la confidentialité des données afin d'éviter la compromission de la sécurité et de la protection des données régies par ces lois. En cas de violation, une réponse efficace et concertée peut aider à limiter la portée de la violation et la responsabilité correspondante.

Le service de sécurité doit également exercer des contrôles adéquats pour répondre aux normes minimales en matière de protection des données. Le service juridique peut, régulièrement, recommander l'affinage de ces mécanismes de contrôle en vue de garantir une conformité continue, y compris les exigences de notification, afin d'atténuer la responsabilité potentielle d'une entreprise.

Application des politiques réglementaires et de conformité

Les employés devraient être informés des politiques de sécurité et de traitement des données d'une entreprise, et s'y conformer. Si la violation de ces normes peut engager la responsabilité du service juridique, d'autres équipes comme les RH, l'informatique et la sécurité peuvent également être pointées du doigt. Si une violation potentielle ou réelle est identifiée, le service juridique doit déterminer la responsabilité potentielle et les mesures à prendre. Dans certains cas, il peut être nécessaire de signaler ces violations aux responsables de l'entreprise, aux organismes de réglementation ou même aux forces de l'ordre.

«Afin de garantir la mise en conformité permanente de notre entreprise, nous nous appuyons sur des formations obligatoires pour l'ensemble de nos employés ainsi que sur des guides d'exploitation qui renferment et présentent en détail les procédures et processus favorisant la conformité. Nous examinons et peaufinons régulièrement les directives concernant les politiques et les contrôles afin de respecter les obligations de conformité dans un contexte de réglementation en constante évolution».

Cindy Rosser
Directrice des produits, de la propriété intellectuelle et des affaires réglementaires
DocuSign

Les incidents liés à la sécurité et au traitement des données sont généralement détectés par les équipes de sécurité, qui supervisent les activités liées aux données dans l'ensemble de l'entreprise. Lorsqu'une activité non autorisée comme une violation apparente des politiques est détectée ou identifiée, les équipes de sécurité enquêtent généralement sur l'incident et fournissent une analyse des causes profondes au service juridique. L'enquête peut se porter simplement sur l'activité ayant provoqué l'incident touchant les données en question ou, dans certains cas, sur des informations détaillées concernant la source de l'activité non autorisée à l'origine de l'incident.

Grâce à ces informations, les services juridiques peuvent analyser les implications juridiques liées à l'incident, notamment les problèmes de conformité, le niveau de risque de l'incident et la responsabilité potentielle de l'entreprise.

La conformité et la sécurité des données convergent dans les applications tierces

Les grandes entreprises s'appuient généralement sur des applications tierces pour réaliser des fonctions commerciales vitales. Ces applications peuvent être au service d'une seule équipe ou être profondément intégrées dans plusieurs unités opérationnelles d'une entreprise. Si le service juridique n'est pas le seul responsable du processus de sécurisation des applications tierces, il travaille souvent en étroite collaboration avec le service de sécurité pour examiner et déployer de nouvelles solutions relativement à la sécurité et à la confidentialité. Plus précisément, le service juridique aide à déterminer si l'utilisation d'une application par son entreprise est conforme aux normes internes, mais également aux exigences réglementaires. En outre, l'équipe de sécurité peut examiner et évaluer si des contrôles suffisants sont disponibles par le biais des fonctionnalités de l'application, afin de répondre aux exigences minimales en matière de sécurité des informations.

Évaluation des applications tierces

Les services juridiques et de sécurité examinent tous deux les applications tierces afin de déterminer si elles peuvent répondre aux exigences de sécurité et de conformité d'une entreprise. Chaque équipe détermine si l'application est conforme ou non, et prend également en compte les avantages que procure cette application. Ces équipes peuvent prendre en compte les certifications de conformité, les tests de pénétration, les examens de code, les audits de fonctionnalités, les cessions d'obligations contractuelles et d'autres mesures pour évaluer l'outil ou le service.

«Lors de l'intégration de nouvelles applications de fournisseurs tiers, le service juridique peut aider à évaluer le risque de conformité lié à l'utilisation de ces applications. Les entreprises adoptant une approche plus raisonnable à l'égard de la conformité auront souvent mis en place un processus d'évaluation des fournisseurs tiers basé sur des exigences clés liées à la conformité. Le service juridique, peut-être en collaboration avec le bureau du RSSI, peut élaborer un profil de risque pour chaque fournisseur afin d'aider l'entreprise dans son ensemble à déterminer s'il convient de poursuivre l'utilisation de l'application de ce fournisseur».

Ronald Plesco
Associé, Confidentialité, sécurité et cybersécurité
DLA Piper

Une fonctionnalité essentielle que recherchent les entreprises dans les applications tierces est la visibilité sur les activités des utilisateurs et des comptes. Les équipes de sécurité et juridique peuvent tous bénéficier d'une visibilité sur les activités, car elle permet à leur entreprise de compléter les fonctionnalités existantes d'audit et de surveillance de la conformité ainsi que de la sécurité. En particulier, si une application tierce offre une visibilité sur les activités des utilisateurs et des comptes d'une entreprise, les équipes de sécurité peuvent collaborer avec les équipes de conformité et/ou juridique pour identifier les activités à risque ou non conformes des utilisateurs de cette application.

Lors de l'élaboration des stratégies de réponse de sécurité impliquant des applications tierces utilisées dans la production, le service juridique peut formuler des conseils sur les initiatives de formation et de sensibilisation recommandées en vue de réduire les activités non autorisées et de former les utilisateurs aux meilleures pratiques afin d'éviter les éventuels faux positifs détectés par l'équipe de sécurité. Par exemple, si une entreprise s'inquiète du transfert et de la suppression d'accords par des employés en violation de sa politique de conservation des documents, le service de sécurité pourra configurer des alertes afin d'effectuer le suivi des activités sur les comptes liées aux téléchargements, aux transferts ou aux suppressions de documents.

«Il revient au service de sécurité d'offrir une visibilité aux équipes juridiques, comme une caméra, pour qu'elles puissent garder un œil sur ce qui se passe à l'intérieur d'un entrepôt. Bien que le service de sécurité puisse surveiller le paysage de sécurité de l'information d'une entreprise en assurant le suivi des activités des comptes et l'authentification des utilisateurs, il doit idéalement être alerté en cas de survenance d'une activité suspecte comme la suppression d'énormes volumes de données ou l'envoi d'importantes quantités de documents à des emplacements où l'entreprise ne dispose ni de bureaux, ni de clients ni de fournisseurs. Lorsqu'un incident de sécurité se produit, les équipes de sécurité peuvent alors s'associer aux équipes juridiques pour déterminer une réponse appropriée afin de respecter les exigences de conformité».

Niall McGrath
Directeur principal des opérations de sécurité
DocuSign

Déploiement d'applications tierces

Si les applications tierces répondent aux normes de sécurité et de conformité d'une entreprise, le service juridique peut s'associer au service de sécurité pour recommander des seuils d'activité et d'alerte que l'équipe des opérations de sécurité devrait suivre et analyser. En outre, si une entreprise s'inquiète de la compromission d'informations dans une application particulière, le service de sécurité peut avoir besoin de la capacité de suivre des opérations comme les téléchargements, les connexions ou toute autre activité susceptible d'aboutir à la compromission de données dans cette application.

Si une grande partie des informations sensibles ou exclusives sont traitées par plusieurs applications tierces, les entreprises peuvent déployer un logiciel de gestion des informations et événements de sécurité (SIEM) pour suivre les activités sur plusieurs applications en même temps. Ces outils confèrent aux équipes de sécurité une visibilité accrue sur les activités quotidiennes d'une entreprise afin qu'elles puissent enquêter sur les comportements suspects ou anormaux capables d'exposer l'entreprise à des risques.

Par exemple, si une entreprise souhaite utiliser un nouveau logiciel intégrant à la fois des informations exclusives et sensibles, l'application sera soumise à un processus d'examen complet de l'intégration du fournisseur. Une fois l'application déployée, le service de sécurité peut mettre en œuvre un plan d'exploitation et surveiller les activités sur l'application aux fins de détection de tout comportement inhabituel grâce à son système SIEM. Si une activité inhabituelle est détectée, le service de sécurité peut se reporter au guide pratique correspondant pour décider de la marche à suivre.

En outre, le service de sécurité peut collaborer avec les services juridique et informatique pour déterminer et mettre en place des protocoles d'accès, d'administration et de cryptage appropriés, conformes aux politiques de l'entreprise et aux réglementations applicables.

«Lorsqu'une entreprise cherche à intégrer une nouvelle application, la diligence raisonnable du fournisseur est cruciale pour aider l'entreprise à maintenir la conformité même pendant l'utilisation de cette application. Peut-être que les contrôles de conformité liés à la sécurité de l'information exigent que l'outil enregistre les activités, qu'il soit doté d'alertes automatisées ou qu'il s'intègre étroitement à nos systèmes actuels via une API. Dans quelle mesure l'outil présente-t-il un risque pour l'entreprise? Si le fournisseur omet de mettre en œuvre les mécanismes de contrôle requis, l'outil ne répondra pas aux exigences de sécurité. Ce processus d'examen de diligence raisonnable est une étape importante pour aider une entreprise à respecter ses obligations en matière de sécurité et de conformité».

Cindy Rosser
Directrice des produits, de la propriété intellectuelle et des affaires réglementaires
DocuSign

Les avantages d'une collaboration efficace entre les services de sécurité et juridiques

Le service de sécurité relève le défi quotidien de la protection d'une entreprise en détectant et en examinant les menaces potentielles et en répondant à celles-ci. Ses équipes protègent une entreprise en évaluant les menaces internes et externes, et en s'attaquant à ces menaces le plus rapidement possible. Le service juridique contribue à la protection de l'entreprise en conseillant les responsables des politiques, de sorte que les équipes compétentes connaissent les politiques de sécurité et règlementaires. Les équipes juridiques jouent également un rôle essentiel au sein d'une entreprise lorsqu'il s'agit de l'application des politiques de sécurité des données et de conformité à l'échelle de l'entreprise.

Les documents comme les guides pratiques et les politiques de sécurité des données sont d'une importance cruciale pour que les services de sécurité et juridique sachent clairement ce qui constitue une activité non autorisée et ce qui peut être considéré comme une violation. Lorsqu'une entreprise veut avoir recours à des applications tierces qui seront utilisées pour traiter ou stocker des informations sensibles ou exclusives, les équipes juridiques et de sécurité peuvent travailler de concert pour s'assurer que l'application répond à la fois aux normes de conformité et de sécurité.

Les entreprises comptent sur la relation étroite entre les équipes juridiques et de sécurité pour garantir la mise en place de mesures de conformité et de sécurité efficaces. En conjuguant leurs efforts, les services de sécurité et juridique peuvent détecter rapidement les menaces avérées, les traiter sans délai et prendre les mesures qui s'imposent. Grâce à une communication régulière et des responsabilités clairement définies, les services juridiques et de sécurité peuvent instaurer une relation de travail symbiotique pour protéger et sécuriser efficacement l'écosystème d'une entreprise.

«Le secteur s'oriente vers les services juridiques et les équipes du responsable de la sécurité des systèmes d'informations qui adoptent une approche véritablement concertée à l'égard de la sécurité des applications, de la réponse aux incidents et de la conformité aux politiques».

Andrew Serwin
Associé, président de la branche américaine et co-président mondial, segment Protection, confidentialité et sécurité des données et cybersécurité
DLA Piper

Découvrez comment renforcer vos opérations de sécurité ici:
docusign.fr/produits/monitor

DocuSign France
9-15 rue Maurice Mallet
92130 Issy-les-Moulineaux

docusign.fr

Pour plus d'informations
Appelez le
+33 (0) 975 181 331