Monthly
Newsletter
March 2023

**IT Security and Cybercrime**

# Cybersécurité – Dix commandements juridiques pour la prévention

Roland Mathys

**Key Take-aways**

**1.**
Dans le cadre de la cyber prévention, il convient de tenir compte non seulement des aspects techniques et organisationnels, mais aussi des aspects juridiques. Cela est encore trop peu fait aujourd'hui.

**2.**
Les principales instructions juridiques peuvent être résumées en dix points et mises en œuvre à un coût raisonnable.

**3.**
Si les mesures juridiques préventives sont négligées, une entreprise risque de subir de multiples inconvénients allant de la violation de contrat à des sanctions.

## Introduction

La cybercriminalité est omniprésente. Il ne se passe guère de jour sans qu'une grande entreprise ou une administration ne soit victime d'une cyberattaque. Les cyberattaques sont aujourd'hui perçues comme l'un des **plus grands risques du point de vue de l'entreprise**. Avec l'augmentation constante de la menace des cyberattaques, la prise de conscience des mesures préventives s'est fortement accrue. Les mesures techniques et organisationnelles sont au premier plan. En revanche, les **mesures juridiques** dans le domaine de la cyber prévention **sont encore rares** – à tort, car là aussi, il reste beaucoup à faire pour être prêt en cas de cyberattaque. Les principales recommandations préventives d'un point de vue juridique sont résumées ci-dessous sous la forme de dix commandements.

**La dimension contractuelle des cyber incidents n'est guère prise en compte.**

## 1 Sécurité de l'information

La sécurité de l'information est avant tout considérée comme un sujet technique, mais elle a également une dimension juridique. Selon le règlement général de l'UE sur la protection des données (**RGPD**), des mesures techniques et organisationnelles appropriées doivent être prises pour **garantir la sécurité des données**, faute de quoi de lourdes amendes de plusieurs millions d'euros peuvent être infligées. De même, en vertu de la future loi suisse sur la protection des données (**LPD**), le non-respect des exigences minimales en matière de sécurité des données sera punissable et sanctionné par une amende pouvant aller jusqu'à 250 000 CHF.

La sécurité de l'information insuffisante peut en outre entraîner une violation de **secrets protégés par le droit pénal** (p. ex. le secret médical) et être punie en cas d'intention (éventuelle) ou même de négligence pour le secret bancaire. Les obligations légales visant à garantir la sécurité de l'information figurent également dans des réglementations sectorielles (p. ex. dans le secteur financier) ainsi que, pour les organes des sociétés, dans le *Swiss Code of Best Practice for Corporate Governance*.

## 2 Équipe d'intervention en cas d'urgence cybernétique

Une entreprise devrait disposer d'une équipe d'urgence capable d'intervenir en cas de cyber incident et de prendre les mesures nécessaires. Une telle équipe de réponse aux urgences cybernétiques (*Cyber Emergency Response Team* ; **CERT**) doit être **formée et instruite à l'avance**; si le cyber incident s'est déjà produit, il n'y a pas de temps à perdre.

Le CERT doit être composée **des bons rôles et personnes** afin de bien fonctionner en cas de crise. Outre les domaines spécialisés, des représentants de la sécurité de l'information, du domaine de la communication et du domaine juridique/*compliance* devraient être représentés au sein du CERT. La direction d'une entreprise doit également être impliquée dans le CERT.

Le **rôle des juristes** du CERT est de prendre toutes les mesures juridiques nécessaires en temps utile et dans le bon ordre en cas d'un cyber incident. Il s'agit notamment de contacter la (cyber) assurance (voir ci-dessous), de signaler les violations de la protection des données aux autorités et aux personnes concernées, d'ouvrir une enquête interne, de déposer une plainte pénale ou de préparer la défense contre les prétentions de tiers.

## 3 Spécialistes externes

Les prestataires de services externes tels que les experts en sécurité et en matière forensique, les "négociateurs" en cas de demande de rançon et les avocats devraient être mis à contribution suffisamment tôt. Il convient de conclure des **accords de mandat** avec ces prestataires et de vérifier l'absence de conflits d'intérêts. Si une entreprise ne commence avec ces préparations qu'après la survenue d'un cyber incident, elle perd un temps précieux et se trouve dans une position défavorable pour négocier.

Les **points de contact et les voies de communication** doivent être définis pour tous les prestataires de services (y compris la disponibilité du service de piquet, selon les besoins). En outre, les prestataires de services doivent être familiarisés avec les spécificités de l'entreprise et les processus déterminants (voir ci-dessous) afin d'être rapidement opérationnels en cas d'urgence.

## 4 Processus et directives

Dans le cadre de la préparation à un cyber incident, les processus pertinents doivent être documentés et des directives doivent être établies. Cela vaut notamment pour la **procédure de notification d'une violation** de la protection des données, qui doit être effectuée dans un bref délai après la connaissance d'un incident et de sa portée. Les directives relatives à la sécurité sont également importantes, par exemple les instructions aux collaborateurs sur la gestion des cyber risques. En outre, il convient de préparer des projets pour la communication interne et externe, qui peuvent être rapidement adaptés, si nécessaire, aux circonstances spécifiques du cyber incident survenu.

Une fois établie, la documentation **doit être vérifiée et actualisée en permanence**, par exemple lorsque de nouveaux scénarios de risque apparaissent, que des modifications sont apportées à l'infrastructure informatique ou que de nouvelles dispositions légales doivent être respectées. Les documents mentionnés servent d'une part à pouvoir agir rapidement, de manière planifiée et ciblée en cas d'incident cybernétique et à minimiser ainsi les conséquences de l'incident. D'autre part, la documentation a pour but de prouver la conformité avec les exigences minimales en matière de sécurité des données et la mise en œuvre des mesures correspondantes.

## 5 Compliance

Les entreprises qui **ne sont pas dans le collimateur** des autorités négligent parfois la conformité en matière de protection des données. Mais cela peut changer rapidement en cas de cyber incident, lorsqu'une entreprise se retrouve soudainement sous le feu des projecteurs des autorités. S'il sort alors que l'entreprise concernée n'a pas mis en œuvre les directives de protection des données conformément à la loi, d'autres problèmes risquent de survenir.

Citons **par exemple** le cas d'une entreprise qui, en raison d'une violation de la sécurité des données, a notifié l'autorité de protection des données d'un État membre de l'UE. Lors du traitement de cette notification, il s'est avéré que les informations relatives à la protection des données sur le site web devaient également être adaptées, qu'un représentant de l'UE devait être désigné et qu'un registre des activités de traitement devait être établi.

## 6 Autorités

Outre l'intégration d'experts externes dans le CERT, il convient d'établir et d'entretenir des contacts avec les autorités compétentes en cas de cyber incident. Il s'agit notamment des **autorités de protection des données, des autorités pénales et d'autres autorités de surveillance** (par exemple dans le domaine financier).

L'entreprise doit d'abord déterminer quelles sont les autorités **compétentes sur le plan local et matériel**. Si une entreprise peut s'adresser à différents services, il faut se demander quelle autorité dispose de la plus grande compétence et expérience dans le traitement des cyber incidents ; pour les autorités pénales en Suisse, cela s'applique généralement aux autorités des cantons qui ont créé leurs propres départements de cybercriminalité. Au sein de l'autorité compétente, il convient également de connaître les **interlocuteurs** importants et les possibilités de contact afin de garantir un accès aussi direct que possible.

Il est également recommandé de rechercher **l'échange** avec les représentants des autorités dans le cadre de la cyber prévention. Cela permet aux autorités d'en savoir plus sur l'entreprise et d'évaluer la criticité d'une cyberattaque. Parfois, les entreprises (p. ex. les opérateurs d'infrastructures critiques) discutent au préalable avec les autorités des procédures à suivre en cas de cyber incident. D'après notre expérience, les autorités se montrent généralement ouvertes et coopératives vis-à-vis d'un tel échange.

## 7 Contrats

La cybersécurité fait de plus en plus souvent l'objet d'accords contractuels. Les contrats conclus avec les principaux partenaires doivent être examinés en vue des **dispositions relatives à la cybersécurité** afin d'éviter toute violation de contrat.

Cet examen doit permettre de déterminer si un contrat impose des **exigences minimales** en matière de cybersécurité et si l'entreprise s'y conforme. En outre, il convient de savoir à l'avance si un cyber incident constitue une **violation du contrat** (éventuellement en fonction de sa gravité) et quelles sont les conséquences juridiques qui y sont liées. Il est également important de savoir si (et dans quel délai) le partenaire contractuel doit être **informé** d'un cyber incident.

Toutes ces conclusions devraient être consignées dans un **inventaire** régulièrement mis à jour et accessible hors ligne (par exemple sur papier). Les incidents dans lesquels l'accès à de tels documents a échoué précisément parce que les documents avaient été cryptés au cours d'une attaque par ransomware ne manquent pas d'ironie, mais se produisent malheureusement dans la pratique.

**Une cyber assurance peut couvrir un risque résiduel, mais ce n'est pas la panacée.**

## 8 Chaîne logistique et prestataires de services

Souvent, une **faille de sécurité** n'existe pas dans l'entreprise attaquée elle-même, mais dans sa chaîne logistique ou chez un prestataire de services informatiques (p. ex. fournisseur de cloud ou de logiciels). En ce qui concerne les tiers critiques pour l'entreprise, une *due diligence* contractuelle doit donc être effectuée en plus de la *due diligence* technique.

Dans le cadre de la ***due diligence* contractuelle**, le contrat avec le tiers doit être analysé en particulier sur les thèmes suivants : Normes et mesures de sécurité, certifications, droits d'audit, tests de vulnérabilité, mesure de la diligence, assurances et garanties contractuelles, obligation d'information (p. ex. consultation du rapport forensique), obligation d'assistance en cas de cyber incident et rémunération, voies de recours (p. ex. responsabilité, résiliation extraordinaire), couverture d'assurance et autres garanties.

Si le contrat ne contient **pas de dispositions suffisantes** sur ces points, il est recommandé de le (re)négocier. Si cela n'entraîne pas d'amélioration, la résiliation du contrat (ou la renonciation à la conclusion du contrat) devrait être considérée.

## 9 Formation et sensibilisation

Le facteur humain constitue l'une des portes d'entrée les plus fréquentes pour les cyberattaques, que ce soit par le biais d'attaques de *phishing*, de pièces jointes infectées par des virus ou d'un *social engineering* sophistiqué. Il est donc important d'aiguiser la conscience des cyberattaques, de montrer les modes d'attaque typiques et de former le comportement adéquat. Ces formations doivent être régulières et, compte tenu du progrès technique, leur contenu doit être actualisé.

Les formations font partie des **mesures organisation-**

**nelles** visant à garantir la sécurité de l'information. Leur négligence doit donc être considérée comme une violation de la sécurité des données, avec les conséquences que cela implique.

## 10 Assurance

Malgré toutes les mesures préventives, un **risque résiduel** subsiste ; une (cyber)assurance peut éventuellement le couvrir. Mais il ne faut en aucun cas se fier uniquement à l'assurance et négliger les mesures préventives décrites précédemment.

Tout d'abord, il faut se demander si et dans quelles conditions les cyber incidents sont couverts par l'assurance. En règle générale, les compagnies d'assurance exigent la preuve d'un **niveau de protection technique minimal**. Il convient ensuite de vérifier quels **types de dommages** sont couverts (p. ex. paiement de rançons, dommages indirects suite à une interruption de l'activité, coûts liés au dépôt d'une plainte pénale).

Une entreprise devrait également se renseigner à l'avance sur les **obligations à respecter en cas de sinistre**. Outre l'avis de sinistre, il s'agit typiquement d'obligations de documentation, de mesures visant à réduire le dommage ou de la collaboration avec des prestataires de services externes prédéfinis.

Enfin, il est recommandé de **comparer** et d'évaluer différents fournisseurs de cyber assurances en fonction des principales caractéristiques de leurs prestations. Il existe par exemple des différences considérables dans le délai pour obtenir la garantie de prise en charge des coûts, qui, selon notre expérience, peut aller de moins d'une heure à plusieurs jours.

## Conclusion

Outre les mesures techniques, les mesures juridiques revêtent également une importance fondamentale dans le cadre de la cyber prévention. La plupart de ces mesures ne relèvent pas de la *rocket science* et peuvent être mises en œuvre à peu de frais. Il est donc d'autant plus important d'accorder à ces aspects l'attention qu'ils méritent.


**Louis Burrus**
Associé Genève
louis.burrus@swlegal.ch

**Clara Poglia**
Associée Genève
clara.poglia@swlegal.ch

**Roland Mathys**
Associé Zurich
roland.mathys@swlegal.ch

**Peter Burckhardt**
Associé Zurich
peter.burckhardt@swlegal.ch






**Schellenberg Wittmer SA**
Avocats

**Zurich**
Löwenstrasse 19
Case postale 2201
8021 Zurich / Suisse
T +41 44 215 5252
www.swlegal.ch

**Genève**
15bis, rue des Alpes
Case postale 2088
1211 Genève 1 / Suisse
T +41 22 707 8000
www.swlegal.ch

**Singapour**
Schellenberg Wittmer Pte Ltd
6 Battery Road, #37-02
Singapour 049909
T +65 6580 2240
www.swlegal.sg