



Prise de position sur la réglementation concernant la gestion des cyberrisques

L'essentiel en bref:

- Les cyberattaques sont en constante évolution. La pression est élevée: les entreprises doivent identifier les faiblesses, établir des priorités et les corriger rapidement
- Seule une connaissance fondée des menaces les plus actuelles permettra de protéger efficacement les infrastructures de communication et d'information
- La gestion des cybermenaces nécessite une action commune, où l'économie assume la responsabilité et compte sur des conditions-cadre claires de l'État

Les cyberattaques se multiplient dans le monde entier et représentent une menace croissante pour l'économie, l'État et la société. Des infrastructures critiques sont dans le collimateur, mais également des entreprises de toute taille. La lutte contre les cyberrisques incombe à l'ensemble de la société.

Une prise de position indique la voie à suivre pour créer un cadre fiable

Malgré l'hétérogénéité des menaces, la politique fédérale mise sur une réglementation étatique et des mesures de rétorsion plutôt que sur la collaboration. Le récent durcissement de la loi sur la sécurité de l'information (LSI), dont les nouvelles dispositions sont entrées en vigueur le 1^{er} avril 2025,

illustre cette tendance. Il introduit des obligations de signaler strictes, accompagnées de sanctions sévères. L'entreprise victime d'une cyberattaque est ainsi pénalisée plusieurs fois.

Pourtant, la situation pourrait être différente: l'économie est en effet prête à assumer des responsabilités. Cependant, elle attend de l'État qu'il établisse un cadre fiable et flexible, fondé sur la confiance et la responsabilité commune.

Dans ce contexte, *economiesuisse* a publié une prise de position sur la réglementation concernant la gestion des cyberrisques, élaborée en étroite collaboration avec ses membres.

[Accéder à la prise de position](#)

La cybersécurité a besoin d'une approche réglementaire souple et efficace

Les cyberrisques ne peuvent pas être appréhendés au moyen de règles rigides. Il faut au contraire un cadre réglementaire dynamique, fondé sur des principes, qui n'entrave pas l'innovation et permette en même temps de réagir rapidement aux nouvelles menaces. L'économie suisse soutient donc les principes suivants:

- **Une coopération d'égal à égal entre l'État et l'économie:** Ceux-ci doivent assumer ensemble la responsabilité pour la cybersécurité. Cela passe par un dialogue continu fondé sur la confiance.
- **Une autorégulation spécifique au secteur:** Des solutions sectorielles éprouvées accroissent l'efficacité et la flexibilité dans la gestion des risques.
- **Des données fiables et des échanges d'informations:** Un état des lieux commun et des échanges d'informations anonymisées sur les menaces sont décisifs.
- **La prévention plutôt que des sanctions:** Des incitations et du soutien encouragent les acteurs à mettre en place des mesures de prévention et de sécurité – il faut éviter des sanctions excessives.

Un avantage concurrentiel grâce à une infrastructure numérique résiliente

Une protection efficace contre les cyberrisques renforce la souveraineté numérique de la Suisse et constitue un facteur décisif pour la place économique. Seules des conditions-cadre favorables à l'innovation peuvent maintenir la compétitivité de l'économie suisse à long terme.

La prise de position a notamment pour but de contribuer à un large débat sur la réglementation de l'IA et de donner ainsi des impulsions importantes pour le développement futur de ce domaine technologique en plein essor.