Les bonnes et les moins bonnes nouvelles concernant les exigences de DORA en matière de reporting

Les entités financières européennes et leurs fournisseurs tiers devront bientôt se conformer aux nouvelles lois de l'UE en matière de cybersécurité et de partage des informations et des renseignements. Si certaines entreprises peuvent déjà être soumises à des règles similaires, d'autres devront peut-être partir de zéro.

Depuis longtemps les entreprises de services financiers (FS) de l'Union européenne appellent à une normalisation des lois sur la cybersécurité.[1] Cependant, il faut faire attention à ce que vous souhaitez !

La bonne nouvelle est que le règlement sur la résilience opérationnelle numérique (*Digital Operational Resilience Act*, ou DORA, comme on l'appelle plus communément) réalise exactement ce que les entreprises du secteur des services financiers souhaitent. Il harmonise un tas de réglementations et de normes d'information provenant des 27 pays de l'UE, devenues difficiles à concilier. En exigeant des entreprises qu'elles intègrent la cybersécurité dans l'ensemble de leurs activités, cette mesure devrait réduire les coûts globaux de mise en conformité et alléger les formalités administratives.[2]

La moins bonne nouvelle est que l'heure tourne. Avec moins de 24 mois avant la mise en œuvre complète de DORA, certaines entreprises du secteur des services financiers pourraient rencontrer des difficultés pour en respecter l'échéance.[3]

Collecte et partage de l'information

Se préparer à la mise en conformité avec le règlement DORA peut être un défi. Les exigences sont nombreuses dans l'organisation, et les sanctions pour non-conformité peuvent être sévères.[4] Les éviter requiert une responsabilisation de la direction en matière de continuité des activités, de gestion des incidents, de communication de crise et d'exercices permettant de tirer des leçons.

Dans deux articles précédents sur le règlement DORA, nous avons examiné trois de ses cinq piliers. Deux d'entre eux concernent la gestion des risques numériques ; le dernier définit les exigences en matière de tests opérationnels. Pour ce dernier article de notre série, nous présentons les deux piliers de partage de l'information (signalement des incidents et partage de l'information et des renseignements). Ils ont deux objectifs distincts : offrir la possibilité de partager des informations relatives aux cyberattaques afin principalement d'améliorer la détection, et la capacité des acteurs du secteur à signaler efficacement les incidents.

Les deux piliers fourniront également aux régulateurs bruxellois une visibilité accrue et en temps réel des incidents de cybersécurité dans l'ensemble de l'UE.[5]

Alors qu'elles se préparent à l'entrée en vigueur du règlement DORA, les entreprises du secteur des services financiers doivent comprendre que les exigences sont tout sauf un exercice ponctuel de *box-ticking*, surtout si l'on considère les dispositions détaillées du règlement en matière de communication. En vertu du règlement DORA, les entreprises du secteur des services financiers doivent maintenir un plan de communication en cas de crise qui garantit que « des informations actualisées sont transmises à l'ensemble du personnel interne et des intervenants externes concernés ».[6] En termes pratiques, ce mandat exige des tests et une formation continus pour s'assurer que les organisations ont les bonnes personnes et les bons processus en place, et que des solutions de rechange sont disponibles si les canaux de communication normaux étaient compromis.

Il est clair qu'il y a beaucoup à prendre en compte. Nous répondons ici aux questions relatives aux deux piliers qui peuvent préoccuper les responsables de la conformité, les conseils d'administration et les cadres dirigeants.

Q: En quoi l'exigence de déclaration d'incident prévue par DORA modifie-t-elle le fonctionnement actuel des entreprises du secteur financier ?

C'est très relatif, mais les nouvelles exigences en matière de cybersécurité se traduisent souvent par des exigences accrues en matière technique comme de reporting, ce qui peut être onéreux. En vertu du règlement DORA, certains incidents nécessiteront la divulgation presque immédiate de détails spécifiques et exhaustifs, en cas de violation de données.[7] Concrètement, les entreprises du secteur financier doivent être prêtes à gérer une cyberattaque survenue et à divulguer des détails spécifiques aux régulateurs.

La nature même des cyberattaques vient compliquer les choses : les cyberincidents ne sont parfois identifiés que des semaines voire des mois après... Pris ensemble, ces nouvelles exigences déclaratives exercent une pression énorme sur les entités financières. Pour être fin prêtes, elles doivent mettre en place l'infrastructure appropriée - y compris les systèmes d'alerte précoce et leur approche opérationnelle, ainsi que les plans de gestion de crise et de communication de crise.

Q: Qu'en est-il du partage de l'information et des renseignements - cela change-t-il les choses pour les entreprises ?

Cela dépend. Comme les exigences en matière de reporting, les piliers de partage d'informations et de renseignements du règlement DORA seront nouveaux pour certaines entreprises, tandis que d'autres peuvent déjà être conformes dans certains domaines. Par exemple, certaines organisations travaillent depuis des années avec des centres de partage et d'analyse des informations en Europe pour signaler les cyberincidents. Toutefois, les efforts précédents n'ont jamais atteint cette ampleur, et les organisations n'ont pas eu à faire face à des sanctions aussi sévères en cas de non-conformité.

Gardons également à l'esprit que les exigences en matière de partage d'informations et de renseignements sont d'une nature plus technique que pour les autres piliers de DORA. Les entreprises doivent donc veiller à ne pas divulguer par inadvertance des informations sensibles lorsqu'elles se conforment aux nouvelles règles.

Q: La protection des informations sensibles - voilà une question majeure. Comment les entreprises du secteur des services financiers se gardent-elles de divulguer des secrets commerciaux lorsqu'elles sont amenées à partager des informations sur des menaces et des incidents de cybersécurité ?

Il s'agit de préoccupations sérieuses à prendre en compte avant la mise en œuvre. Le partage d'informations sensibles ne doit se faire qu'avec des personnes et des organisations de confiance, et par le biais d'une plateforme sécurisée.

Q: La divulgation d'un incident rend parfois les entreprises frileuses par souci réputationnel. Que doivent garder à l'esprit les entreprises du secteur des services financiers si le pire venait à se produire ?

Premièrement, une crise de cybersécurité est toujours due à un facteur externe. Aussi, l'opinion publique sera sensible à la manière dont la direction réagit à la crise. Avec DORA, les entreprises doivent s'assurer que les fondements de leur résilience opérationnelle sont en place, ce qui inclut leurs plans de gestion de crise et de communication de crise. Mais la façon dont la direction gère, par exemple, une violation de données,

est primordiale pour la gestion de la réputation. Cela signifie généralement qu'il faut divulguer la violation aux parties prenantes concernées en temps utile - et ce, par une communication claire, transparente et ouverte. Les entreprises doivent également disposer d'un régime interne de test et de formation qui tienne compte de tous les impacts possibles sur leurs activités et qui leur donne l'occasion de passer en revue ces plans, notamment en définissant les rôles et les responsabilités de chaque membre de l'équipe.

Les cinq piliers de DORA*

— Test de résilience opérationnelle numérique

— Gestion des risques numériques

— Rapports d'incidents

— Partage d'informations et de renseignements

— Gestion des risques numériques pour les tiers

* FTI Consulting organise les exigences de DORA en cinq piliers clés ; d'autres sources peuvent les organiser différemment.

Pour en savoir plus

1 "EU Cybersecurity Initiatives and the Finance Sector." European Union Agency for Cybersecurity. March 2021. https://www.enisa.europa.eu/publications/EU_Cybersecurity_Initiatives_in_the_Finance_Sector/at_download/fullReport

2 "Regulation of the European Parliament and of the Council on digital operational resilience for the financial sector and amending Regulations (EC) No 1060/2009, (EU) No 648/2012, (EU) No 600/2014 and (EU) No 909/2014." European Commission. Sept. 24, 2020. https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52020PC0595

3 Ibid.

4 "REPORT on the proposal for a regulation of the European Parliament and of the Council on digital operational resilience for the financial sector and amending Regulations (EC) No 1060/2009, (EU) No 648/2012, (EU) No 600/2014 and (EU) No 909/2014." European Commission. July 12, 2021. https://www.europarl.europa.eu/doceo/document/A-9-2021-0341_EN.html

5 FTI Consulting analysis.

6 "REPORT on the proposal for a regulation of the European Parliament."

7 FTI Consulting analysis.

THOMAS HUTIN
Head of Cybersecurity
France