ACADEMY & FINANCE

Gérer les cyberattaques dans le secteur financier suisse

Que faire quand le pire est arrivé ?

> Les différents types de cyberattaques : ransomware, spyware, hameçonnage, hacking...
> Nouvelles obligations d'annonce : quelles sont les attentes concrètes ?
> Quelle réponse immédiate à la cyberattaque ?
> Démarches juridiques et bonnes pratiques (responsabilités, gestion de crise, gestion financière et réputationnelle, cyberassurance)

Thierry Demiéville,

Senior Legal Counsel

Titulaire d'un Master en droit avec mention de l'Université de Fribourg, d'un LL.M en droit commercial et des sociétés (Queen Mary University of London), d'un CAS en digital finance law et d'un CAS en compliance in financial services de l'Université de Genève, Thierry Demiéville est un juriste spécialisé dans les questions de droit bancaire, abordant les problématiques dans une perspective transversale, sous l'angle juridique, compliance et de la finance numérique, avec 20 ans d'expérience dans le domaine financier. Il a notamment été responsable juridique auprès de Flow Bank SA, Senior Legal Officer auprès de la Lloyds TSB Bank, succursale de Genève, Sous-Directeur au sein du Service juridique de la Compagnie Bancaire Helvétique, responsable juridique & compliance auprès d'IG Bank SA, Directeur-Adjoint au sein du Service juridique de la Banque Cramer & Cie SA, juriste au Registre central auprès de BNP Paribas Private Bank (Suisse) et Sous-Directeur au sein du Fichier central (représentant juridique du service) de Mirabaud & Cie.

Introduction
1) Définition de la cyberattaque
• Définition légale de la loi fédérale sur la sécurité de l'information (LSI)
2) Enjeux critiques pour les institutions financières
3) Bref historique
• Les débuts (années 1980)
• Années 1990
• Montée en puissance (années 2000-2010)
• Ere de la cybercriminalité organisée (2010-2020)
• Période récente (2020-2025)
4) Types de cyberattaques le plus fréquent

NOUVELLES OBLIGATIONS LÉGALES ET RÉGLEMENTAIRES

Obligation envers l'Office fédéral de la Cybersécurité (OFCS) de signaler les cyberattaques
- Entités assujetties à l'obligation de signaler
- Conditions déclenchant l'obligation d'annonce
- Délais d'annonce : 24h, 14 jours
- Mode de transmission de l'annonce
• Formulaire d'annonce de l'OFCS
- Contenu de l'annonce
- Transmission des informations provenant des annonces entre autorités
- Soutien de l'OFCS aux exploitants d'infrastructures
- Violation de l'obligation d'annonce

Obligation envers la FINMA de signaler les cyberattaques
- Entités assujetties à l'obligation de signaler
• Obligation de signaler la cyberattaque dont l'entité assujettie a été victime
• Obligation de signaler la cyberattaque dont le prestataire de service de l'entité assujettie a été victime
- Conditions déclenchant l'obligation d'annonce
- Délais d'annonce : 24h, 72h
- Mode de transmission de l'annonce
- Contenu de l'annonce
• Détermination du degré de gravité de la cyberattaque pour l'annonce dans les 24h et les 72h
• Degré de gravité : grave, élevé, moyen
• Contenu de l'annonce : dans les 24h, dans les 72h
- Rapport conclusif sur les causes
- Preuves et analyses du bon fonctionnement de l'organisation de crise
- Violation de l'obligation d'annonce

Obligation envers le Préposé fédéral à la protection des données et de la transparence (PFPDT) de signaler les cyberattaques
- Entités assujetties à l'obligation de signaler
• Obligation de signaler la cyberattaque dont l'entité assujettie a été victime
• Obligation de signaler la cyberattaque dont le prestataire de service de l'entité assujettie a été victime
- Conditions déclenchant l'obligation d'annonce
- Délais d'annonce, mode de transmission de l'annonce
- Contenu de l'annonce
- Rapport conclusif sur les causes
- Violation de l'obligation d'annonce

Obligation envers les autorités locales de signaler les cyberattaques
- Cas de la filiale étrangère

TYPOLOGIE DES PRINCIPALES CYBER-ATTAQUES : qualification juridique, mode opératoire, exemples

Attaques par des logiciels malveillants (« malwares »)
- Rançongiciel (« ransomware »)
• Paiement de la rançon
> Situation vis-à-vis du droit suisse
> Pratique des autorités
> Assurabilité du « ransomware »
- Cheval de Troie (trojan)
- Logiciel espion (« spyware »)
- Enregistreur de frappes (« keylogger »)
- Réseau d'ordinateurs infectés (« Botnet »)
- Ver informatique (« worm »)

Attaques par déni de service
- Déni de service distribué (« DDoS »)
- Déni de service applicatif

Attaques d'ingénierie sociale
- Hameçonnage (« phishing », « spear phishing », "whaling", "vishing", "smishing", Fraude au président)
- Usurpation d'identité de site ("website spoofing ")

Atteintes à l'intégrité, à la confidentialité et à la disponibilité des données
- Exfiltration de données
- Altération ou destruction de données
- Sabotage

Intrusions et compromissions de systèmes (« hacking ») :
- De l'entrée à la consolidation de l'accès
• Exploitation de vulnérabilités (« exploit »)
• Escalade de privilèges
• Persistance dans le système (« backdoor »)
- Techniques d'intrusion spécifiques
• Attaques « supply chain »
• Force brute

Attaques ciblant des infrastructures critiques
- Qualification juridique
- Mode opératoire
- Attaques contre des infrastructures financières de marché

GENÈVE, JEUDI 9 OCTOBRE 2025, 8.30-15.30, HÔTEL PRÉSIDENT / ONLINE

GESTION DE LA CYBERATTAQUE

Phase 1 – Réponse immédiate à la cyberattaque

1) Détection et alerte interne
- Identification de l'incident par l'IT, la sécurité ou un autre employé
- Notification immédiate
• Ordre de priorité ?
• Gravité de l'incident
• Départements/Organes concernés
- Activation de la cellule de crise cyber (comité ad hoc)
• Objectifs de la cellule de crise
• Composition pluridisciplinaire

2) Isolation et confinement : systèmes compromis, accès suspects, éviter la suppression des preuves

3) Analyse et qualification : nature et ampleur de l'attaque, données et systèmes touchés

4) Notifications réglementaires urgentes : OFCS, FINMA, PFPDT, autorités locales

5) Notifications facultatives
- Annonce au Service de Coordination de la lutte contre la Criminalité sur Internet (SCOCI)
- Annonce à la police cantonale (section spécialisée en cybercriminalité)

6) Information individuelle aux clients directement impactés : obligation légale, obligation réglementaire, obligation contractuelle

7) Communication de crise interne aux employés : objectifs, contenu, FAQ interne

8) Communication de crise externe : clients, partenaires contractuels, médias, publication sur le site web de la Banque

9) Engagement des partenaires externes : but de leur intervention, rapport de l'expert
- Experts techniques
- Experts en investigation forensique
- Cabinets spécialisés en communication de crise

Phase 2 – Gestion des conséquences juridiques, opérationnelles, réputationnelles et financières

1) Remédiation technique
- Eradication du malware ou fermeture de la faille exploitée
• Eradication du malware
• Fermeture de la faille exploitée
- Restauration des systèmes à partir des sauvegardes saines
• Exemples de mesures à prendre
- Renforcement immédiat des mesures de sécurité
• Exemples de mesures de sécurité à activer

2) Gestion juridique et réglementaire
- Evaluation de la responsabilité civile, pénale et administrative de l'institution financière
• Responsabilité civile
> Responsabilité contractuelle : envers les clients, envers les collaborateurs, envers les partenaires contractuels
> Responsabilité légale : envers les clients, envers les collaborateurs, envers les partenaires contractuels
• Responsabilité administrative : organisation inappropriée et violation de la garantie de l'activité irréprochable
• Responsabilité pénale : responsabilité de l'entreprise pour organisation déficiente, responsabilité personnelle des individus
- Dépôt d'une plainte pénale : buts du dépôt de la plainte pénale, preuves à fournir
- Communication continue avec la FINMA, l'OFCS et le PFPDT

3) Gestion financière et assurances
- Chiffrage des pertes directes : coûts techniques immédiats, indisponibilité des systèmes, surcoûts opérationnels, paiement de rançon, pertes/fuites de données sensibles, pertes patrimoniales résultant d'actes frauduleux informatiques
- Chiffrage des pertes indirectes : perte de revenus (gain manqué), atteinte réputationnelle, hausse des primes d'assurance, contentieux, amendes réglementaires, coûts de mise en conformité renforcée
- Activation des clauses d'assurances cyber : couverture des cyberassurances, dommages propres, dommages de tiers, conditions d'activation de l'assurance cyber, événement déclencheur, moment du déclenchement de la couverture, notification de l'incident, exclusions, charge de la preuve, clauses spécifiques propres aux cyberrisques, clauses relatives aux dommages liés à des chantages (« ransomware »), clauses relatives à la protection des données personnelles, clauses relatives à des amendes ou peines pécuniaires, clauses relatives aux monnaies virtuelles, liens avec la RC dirigeants (D&O) et la RC professionnelle

Phase 3 – Post-incident et bonnes pratiques

1) Retour d'expérience
- Analyse détaillée de la chaîne d'événements
- Identification des points faibles techniques et organisationnels
- Rédaction d'un rapport post-incident

2) Renforcement de la sécurité
- Correction des vulnérabilités exploitées
- Mise à jour des politiques de sécurité
- Renforcement des sauvegardes et de la segmentation réseau
- Tests d'intrusion

3) Formation et sensibilisation
- Formation ciblée selon le rôle des employés
- Campagnes internes contre le phishing et l'ingénierie sociale
- Tests réguliers de la cellule de crise

4) Amélioration des procédures et mise à jour des contrats
- Mise à jour du plan de réponse à un incident
- Clarification des rôles et responsabilités
- Mise à jour des contrats avec les prestataires de services et des clauses de sécurité

15.30 Fin du séminaire

GENÈVE, JEUDI 9 OCTOBRE 2025, 8.30-15.30, HÔTEL PRÉSIDENT / ONLINE

INFORMATION & INSCRIPTION
Tel: +41 22 849 01 11
Fax: +41 22 849 01 10
info@academyfinance.ch
Academy & Finance SA
Rue Neuve-du-Molard 3,
1204 Genève
www.academyfinance.ch

PRIX
920 CHF (+ TVA 8.1%)
Inscriptions supplémentaires de la même société : -50%
Le déjeuner (12.35-14.00) est inclus.

AF 1453

☐ Je m'inscris au séminaire "Gérer les cyberattaques dans le secteur financier suisse".
☐ Je participerai dans la salle ☐ Je participerai online sur Zoom

Nom et prénom .....

Fonction .....

Société.....

Adresse .....

Code postal et ville .....

Tel .....Email..... .....

Date ..... Signature ... .