LEMANIA FIDUCIAIRE
Finance - Controlling - Fiscalité
Laurent BOYER
Expert Comptable
% Switch Vibration
Route de Thonon, 152 C
1222 VÉSENAZ (GE)
CHE-271.152.759
(+41) 78 310 93 97
laurent.boyer@lemania-fidu.ch

Importance d'une Compliance maîtrisée => les Cyberattaques récentes visant les administrations françaises

Depuis l'été 2025, les services numériques de l'État français font face à une succession inédite d'incidents de cybersécurité. Le Premier ministre a lui-même reconnu fin avril 2026 que la France enregistrait en moyenne trois vols de données par jour touchant des organismes publics. Plusieurs facteurs structurels sont régulièrement cités par les experts et les parlementaires :

- une base numérique ancienne, certains systèmes d'information datant des années 1990 ;
- un budget cybersécurité de l'État estimé à environ 1 % du budget numérique, contre une moyenne de 10 % dans les grandes entreprises privées ;
- une centralisation croissante des données citoyennes (France Connect, ANTS, ÉduConnect, DGFiP, Tchap...), qui fait de chaque plateforme une cible à très forte valeur ;
- un vecteur d'attaque dominant : l'usurpation d'identifiants légitimes (comptes d'agents ou de tiers habilités), plutôt que l'exploitation de failles techniques sophistiquées ;
- un retard de transposition en droit français de la directive européenne NIS2, la loi « Résilience » étant bloquée au Parlement depuis septembre 2025 (la Commission européenne a saisi la CJUE contre la France le 8 juillet 2026 pour ce retard).

Données et volumes concernés

- **Premier volet (impots.gouv.fr) :** environ 678 000 particuliers et professionnels concernés (identité, adresse, revenu fiscal de référence, quotient familial, taux de prélèvement à la source, SIREN et raison sociale pour les entreprises).
- **Second volet (SPDC – données cadastrales) :** extraction revendiquée de plus de 252 000 lignes, correspondant selon l'attaquant à plus de 2 millions de propriétaires (identité, adresses, identifiants fonciers et parcelles cadastrales).
- La DGFiP précise que les espaces personnels « impots.gouv.fr » des usagers n'ont pas été compromis et qu'aucun mot de passe n'a été dérobé.

Points de vigilance soulevés

- **Délai de détection et de notification :** l'intrusion initiale a été détectée et bloquée fin juin, mais l'exfiltration de données n'a été identifiée qu'après la revendication publique du pirate, mi-août — soit un délai très supérieur au délai réglementaire de notification à la CNIL (72 heures après constat).
- **Vecteur récurrent :** usurpation d'identifiants légitimes (agent DGFiP + tiers habilité), et non exploitation d'une vulnérabilité logicielle inédite — un facteur commun à plusieurs incidents publics récents.
- **Sensibilité des données :** contrairement à un mot de passe, les données fiscales et cadastrales extraites ne peuvent pas être « changées » après coup, ce qui prolonge le risque pour les personnes concernées (phishing ciblé, usurpation d'identité, fraude).

Autres incidents marquants touchant le secteur public en 2026

- **ANTS (avril 2026) :** faille de type IDOR sur le portail ants.gouv.fr ; jusqu'à 11,7 millions de comptes concernés (identité, adresse, contact).
- **Éducation nationale — ÉduConnect (avril 2026) :** environ 3,5 millions d'élèves mineurs exposés.
- **Éducation nationale — personnels (juillet 2026) :** nouvelle intrusion via un compte professionnel usurpé, données d'agents en académie depuis 2001 potentiellement extraites (identité, fonction, pour partie coordonnées et numéro de sécurité sociale).

- **INSEE (juin 2026) :** annuaire interne compromis, environ 12 800 agents et anciens agents concernés (identité et coordonnées professionnelles, sans données bancaires ni de santé).
- **CROUS (mars 2026) :** environ 774 000 dossiers étudiants exposés.
- **FICOBA (février 2026) :** environ 1,2 million de comptes bancaires (IBAN, RIB, identité du titulaire) consultés illégitimement, via usurpation d'identifiants d'un agent.

Point commun : ces incidents résultent souvent d'usurpations d'identifiants légitimes plutôt que d'attaques techniques complexes contre les défenses périmétriques => lacunes de gouvernance des accès plutôt que simple déficit d'outillage.

4. Pourquoi une compliance maîtrisée limite l'impact de ces attaques

Une politique de conformité solide n'empêche pas à elle seule une cyberattaque, mais elle réduit significativement la probabilité d'occurrence, la durée d'exposition et l'ampleur des conséquences. Plusieurs bénéfices concrets ressortent de l'analyse des incidents ci-dessus

a) cartographie des risques

En Audit/Révision Légal(e), on doit **identifier, évaluer et hiérarchiser** les risques juridiques, réglementaires et opérationnels auxquels une organisation est exposée. On doit, pendant la durée de la mission, connaître les différents services, les particularités internes / externes à l'entité, auditer les principaux cycles mais aussi orienter chaque année la mission sur des risques classés selon leur fréquence et leur importance :

- risque survenant rarement + conséquences peu importantes (financières, réputationnelles, juridiques + judiciaires, …) => négligeable
- risque survenant fréquemment + conséquences importantes => surveillance raisonnable
- risque survenant rarement + conséquences importantes => surveillance renforcée
- risque survenant fréquemment + conséquences importantes => surveillance prioritaire

afin de prioriser les actions de contrôle et d'audit.

En audit légal, elle sert de socle au plan de mission : en cas de contrôle ou/et de sinistre post mission elle constitue notamment une preuve de diligence (obligation de moyens + orientation des moyens).

Typiquement, les hackers ont utilisé un "cheval de Troie" pour déployer une technique beaucoup moins lourde et complexe : on entre en usurpant des identifiants légitimes (comptes d'agents ou de tiers habilités), on n'utilise pas les failles techniques sophistiquées, on peut entrer régulièrement après avoir constaté que l'accès n'est ni suspendu ni supprimé, faute de double identification (notamment via des applis tierces sur mobile utilisant la reconnaissance faciale) l'utilisateur légitime ignore que l'accès a été utilisé frauduleusement.

Typiquement, l'utilisateur "basique" de www.impots.gouv.fr constate quotidiennement que l'accès est très différent de celui d'un compte bancaire (au niveau sécurisation) et de nombreux tiers spécialisés ont signalé dans la presse, par le passé, que les portes d'entrée étaient insuffisamment sécurisées / technologie trop ancienne et mal adaptée.

Typiquement, en Suisse, l'accès au Portail Fiscal se fait via plusieurs process : le portail AFC impose (et informe) la suppression du décompte de TVA "Easy" (process trop simple), avec basculement vers TVA "Pro"(process renforcé). De manière analogue, on peut passer du process CH-LOGIN vers AGOV. Point commun de ces process => 1 utilisateur référencé avec un numéro de tél, toute demande d'accès (id+pw) nécessite ensuite une 2e authentification par (code sur tél) / (code sur mail) (reconnaissance faciale). Tout accès par une autre personne ayant extrait nos données pourrait être bloquée et signalée de par le fait que la double authentification nous enverrait un message de demande de connexion alors que nous n'avons pas initié cette demande.

Les risques ont donc mal été cernés et leur importance mal évaluée => les outils techniques n'ont pas été upgradés pour mise à niveau.

a) Réduction de la surface d'attaque liée aux identités

La quasi-totalité des incidents recensés repose sur des identifiants usurpés. Une gouvernance des accès conforme aux référentiels ANSSI (authentification multifacteur généralisée, principe du moindre privilège, architecture Zero Trust / ZTNA en remplacement des VPN traditionnels) réduit directement ce vecteur dominant.

Pour respecter ces référentiels il faut :

- savoir qu'ils existent ….. et suivre leur évolution
- les mettre en place dans les process nous concernant

- exiger des intervenants extérieurs qu'ils les connaissent et les appliquent
- tester régulièrement
- auditer (interne) régulièrement
- solliciter un audit externe pour avoir un avis extérieur et impartial => l'auditeur ne délivrera pas de conseil (interdit de par son mandat) mais soulignera ce qui fonctionne et ce qui est déficient

b) Détection plus rapide des incidents

Dans le cas DGFiP, l'intrusion a été bloquée en juin mais l'exfiltration de données n'a été identifiée que fin des semaines plus tard. Des dispositifs de détection active (EDR, SIEM, SOC) recommandés par l'ANSSI et attendus dans le cadre de NIS2 permettent de raccourcir ce délai, limitant la fenêtre d'exploitation par l'attaquant.

- mettre en place et mettre à jour
- auditer (interne)
- auditer (externe)

c) Respect des délais réglementaires (RGPD)

La conformité RGPD impose une notification à la CNIL sous 72 heures après constat d'une violation, et une information des personnes concernées « dans les meilleurs délais » lorsque le risque est élevé. Une organisation dotée de procédures de gestion de crise et de notification déjà éprouvées limite le risque juridique, réputationnel et le préjudice supplémentaire subi par les personnes concernées (retard dans l'alerte au phishing, par exemple).

Le RGPD est souvent une contrainte mal maîtrisée => en faire un argument commercial et technique, en devenant proactif

d) Anticipation réglementaire (NIS2)

La directive NIS2 impose aux entités essentielles, dont les administrations publiques, des obligations renforcées de gestion des risques cyber. Une mise en conformité anticipée, plutôt que subie après un incident, évite les correctifs dans l'urgence et les surcoûts associés — la France elle-même fait l'objet d'un contentieux européen pour retard de transposition.

e) Maîtrise des coûts et de l'impact réputationnel

Les épisodes DGFiP, ANTS et Éducation nationale ont chacun généré : saisine CNIL, communication de crise, cellule interministérielle, exposition médiatique et parlementaire (questions écrites, commission d'enquête), et risque de contentieux indemnitaire des personnes concernées. Une compliance maîtrisée en amont (audits réguliers, cartographie des risques, plans de réponse à incident testés) réduit ces coûts indirects, souvent supérieurs au coût de la remédiation technique elle-même.

f) Effet de confiance

Dans un contexte où plusieurs administrations sont touchées successivement, une organisation capable de démontrer une gouvernance de la conformité robuste (traçabilité des accès, chiffrement, gestion des tiers habilités, formation des agents) préserve la confiance des usagers et partenaires — un actif difficile à reconstruire une fois entamé.

Les activités de Compliance (conformité) permettent de communiquer positivement et de rassurer les tiers => proactif (tout le contraire d'une position passive, "en attente du problème")

5. Recommandations synthétiques

1. Généraliser l'authentification multifacteur résistante au phishing sur tous les accès distants et privilégiés.
2. Remplacer progressivement les architectures VPN par une approche Zero Trust (ZTNA).
3. Renforcer les capacités de détection (EDR/SIEM/SOC) pour réduire le délai entre intrusion et détection de l'exfiltration.
4. Formaliser et tester régulièrement les procédures de notification RGPD (article 33/34) pour tenir le délai de 72 heures.
5. Accélérer la mise en conformité NIS2 en amont de la transposition législative définitive.
6. Auditer en priorité la gestion des comptes à privilèges et des accès de tiers habilités, vecteur commun à la majorité des incidents recensés.