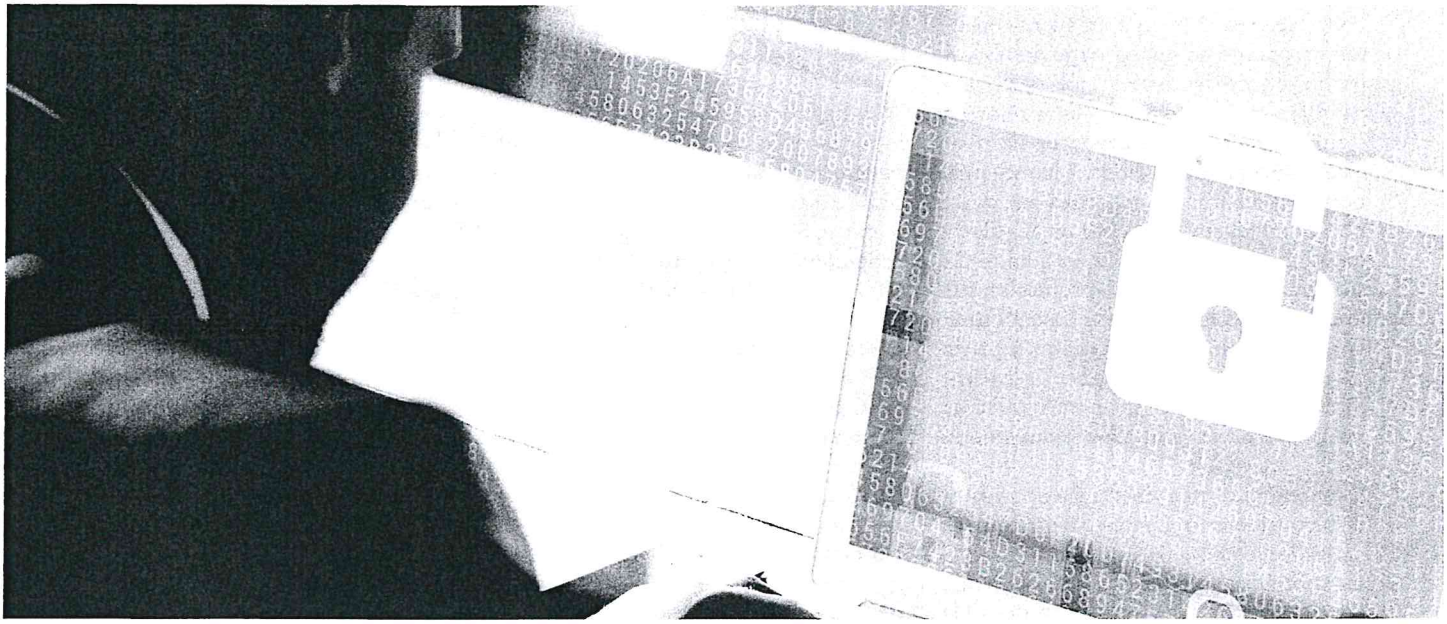


FOCUS

DIX COMMANDEMENTS POUR SE PRÉMUNIR DE LA CYBERCRIMINALITÉ

Face à la recrudescence des cyberattaques, le Conseil supérieur a publié, en marge de la 2e journée du numérique, dix fiches pratiques pour faire face à la cybercriminalité.

Une nouvelle typologie d'infractions, désignée par le mot-valise « cybercriminalité », fait la une des journaux ces dernières années : Twitter, Spotify, EBay, TF1, KPMG, TV5 Monde... Le développement exponentiel de ces fraudes a été rendu possible par l'incontournable digitalisation de notre économie, qui offre une toute nouvelle panoplie d'outils à la disposition des escrocs.

La révolution numérique (Cloud, mobilité, réseaux sociaux, big data...) bouleverse notre quotidien et notre façon de travailler. Mais en emportant avec lui ses outils de travail et les données de l'entreprise, le salarié redéfinit les contours d'un système d'information qui devient d'autant plus difficile à délimiter et donc à sécuriser.

En outre, les grandes entreprises ne sont plus les cibles privilégiées des cyberattaques. La fragilité des PME et TPE, bien moins équipées et protégées que les grandes structures, attire de plus en plus les cybercriminels. En effet, on peut légitimement s'interroger sur leur capacité à se protéger des attaques alors que des grandes entreprises, disposant d'un contrôle interne renforcé, sont piratées. La question n'est donc plus de savoir s'il y a un risque d'attaque, mais plutôt quelle en sera l'ampleur et la fréquence.

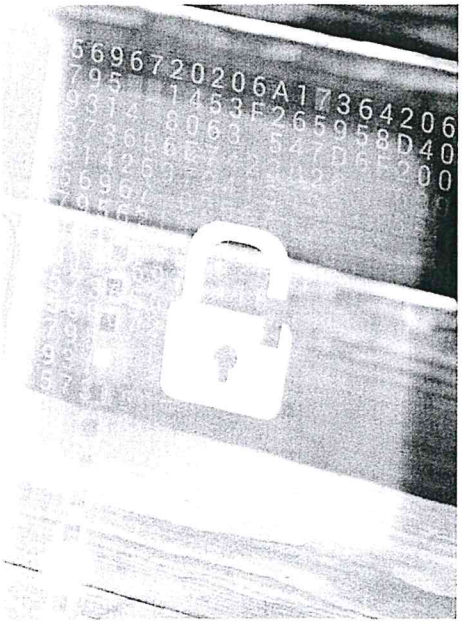
Dans cette optique, les cabinets doivent anticiper les risques et sensibiliser les collaborateurs, noyau dur de ce nouvel écosystème afin de prévenir, détecter et éviter ces menaces.

Le Conseil supérieur de l'ordre des experts-comptables a ainsi publié les « 10 commandements pour se prémunir de la cybercriminalité » dans le cadre de la 2e Journée du numérique qui s'est tenue le 7 décembre 2017 à Paris.

L'objectif est de faire prendre conscience aux professionnels des efforts à produire en termes de protection de l'information. Elles proposent des bonnes pratiques essentielles et élémentaires, faisant appel le plus souvent à du simple bon sens ; mais également des outils pratiques et pragmatiques permettant de mieux se protéger.

Les 10 commandements

1. La confidentialité tu garantiras
2. Un contrat de cyber-assurance tu souscriras
3. Une perte ou un vol tu anticiperas
4. De boucliers tu te muniras
5. Aux cyberattaques tu réagiras
6. Le RGPD tu respecteras
7. Des clés USB (et tous supports physiques externes) tu te méfieras
8. De bonnes pratiques managériales tu adopteras
9. Les usages tu règlementeras
10. Les collaborateurs tu sensibiliseras



« Quand c'est gratuit, c'est toi le produit ! »

Ce slogan, déclaré par le représentant de la Direction générale de la sécurité intérieure (DGSI) lors de la journée du numérique 2017, invite les experts-comptables à avoir un comportement avisé et responsable. Il s'agit d'un enjeu prioritaire pour le Conseil supérieur face à la recrudescence des cyberattaques des cabinets.

L'humain au cœur du système de prévention

Les dix commandements proposés placent le degré de sensibilisation de l'humain, au cœur du système de prévention.
En effet, la sensibilisation des salariés de l'entreprise est le premier rempart le plus efficace contre les cyberattaques. Car si l'enjeu même de la sécurité de tous n'est pas vu comme la somme des vigilances de chacun, nous risquons de passer à côté des pré-requis de base. Il est ainsi primordial, de placer l'homme au cœur du système de prévention.

Rappelons que la négligence humaine demeure la principale source de risques. La sensibilisation doit donc être le maillon clé de la cybersécurité !

Les dix commandements résumés ci-après pourront donc servir de « table de loi » en matière de cybersécurité permettant de :
› promouvoir la vigilance et mettre en place des mesures de sécurité de base
› ralentir et décourager le cybercriminel.

L'essentiel des dix commandements

1 La confidentialité tu garantiras

« Toute révélation d'un secret est la faute de celui qui l'a confié » Jean de la Bruyère

› Sécurisez les échanges de données sensibles ;
› Disposez de mots de passe robustes : caractères diversifiés, renouvellement régulier, pas de stockage ;
› Ne divulguez pas d'informations sensibles et soyez vigilant ;
› Maîtrisez votre e-réputation.

2 Un contrat de cyber assurance tu souscriras

« On ne peut affirmer avec plus d'assurance que rien n'est assuré » Anatole France

› Définissez la typologie des risques assurables : données personnelles, système d'information de l'assuré, données des tiers ;
› Analysez les offres disponibles : couverture des dommages immatériels, préjudices, frais de communication de crise ; prise en charge de la gestion de crise et de la restauration des données ; responsabilité civile ;
› Répertoriez les propositions de valeur pour l'assuré : évaluation, quantification, réduction et transfert des risques, expertise post-incident.

3 Une perte ou un vol tu anticiperas

« Celui dont la pensée ne va pas loin verra ses ennuis de près » Confucius

› Ayez une stratégie rigoureuse de sauvegarde ;
› Soyez conscient des avantages et inconvénients des supports ;
› Prenez des précautions dans l'utilisation des supports.

4 De boucliers tu te muniras

« Lorsque deux forces sont jointes, leur efficacité est double » Isaac Newton

› Munissez-vous d'antivirus et d'antispam : régulièrement à jour et actif, inspectez le contenu des clés USB et fichiers téléchargés ;
› Vérifiez que les systèmes sont régulièrement à jour : évitez les systèmes obsolètes et les versions logicielles anciennes, révoquez les droits des collaborateurs en cas de départ, etc ;
› Disposez de pares-feux actifs.

• • •

...

5 Aux cyberattaques tu réagiras

« Il n'y a pas de vent favorable pour celui qui ne sait où il va »
Sénèque

› Adoptez une méthodologie de traitement du risque au jour de l'attaque : débranchez l'ordinateur du réseau, n'utilisez plus l'équipement corrompu, portez plainte, ne payez pas la rançon, procédez à une analyse complète par l'antivirus, lancez la récupération des données, prévoyez des plans de secours, etc.
› Contactez les structures d'assistance aux victimes de cyberattaques : ACYMA, CERT, Cybermalveillance, Stopransomware.

6 Le RGPD tu respecteras

« Pour savoir où l'on va, il faut savoir d'où l'on vient »
Proverbe africain

Vous êtes tous concernés par le RGPD, mais faites-vous partie des 9 % d'entreprises qui se déclarent prêtes ?

› Désignez un responsable des questions personnelles ;
› Cartographiez vos traitements de données personnelles existants dans le cabinet ;
› Priorisez et hiérarchisez les actions à mener ;
› Gérez les risques ;
› Organisez les processus internes ;
› Documentez pour prouver la conformité au RGPD en cas de contrôle.

7 Des clés USB (et tous supports physiques externes) tu te méfieras

« Un ordinateur en sécurité est un ordinateur éteint. Et encore... »
Bill Gates

› Adoptez des mesures préventives : n'utilisez jamais une clé USB "abandonnée", avant toute utilisation, scannez et nettoyez la clé USB, bloquez la fonction "Autorun", affectez une clé par usage, chiffrez le contenu de vos clés USB ;
› Préparez vos déplacements à l'étranger : n'emportez que les données indispensables pour la mission, marquez vos clés et gardez-les sur vous, jetez-les après usage.

CAP SUR LE NUMÉRIQUE
ORDRE DES EXPERTS-COMPTABLES

PRÉSENTATION DE CAP SUR LE NUMÉRIQUE

Lancée à l'occasion de la 2e Journée du numérique, la plateforme Capsurlenumerique.fr est destinée à accompagner les experts-comptables dans leur transition numérique.

Newsletter Cap sur le numérique : le bon plan pour rester informé

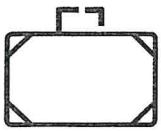
Vous souhaitez garder un train d'avance ? Inscrivez-vous à cette newsletter pour bénéficier de la veille que l'équipe Cap sur le numérique assure sur tous les sujets digitaux, mais aussi pour rester informer des actualités du Comité transition numérique du Conseil supérieur, et des événements organisés par l'Ordre autour du numérique.

Bimensuelle, cette newsletter vous parviendra les 1ers et 3e vendredis de chaque mois ; un moyen idéal d'enrichir vos lectures du week-end.

Inscrivez-vous sur :
www.capsurlenumerique.fr/newsletter/

8 De bonnes pratiques managériales tu adopteras

« Celui qui déplace une montagne commence par déplacer de petites pierres » Confucius



- Instaurez une classification des données de l'entreprise ;
- Adoptez de bonnes habitudes de travail ;
- Renforcez vos procédures internes : restrictions d'accès, gestion des départs des collaborateurs, procédure en cas de modification des RIB fournisseurs ;
- Supervisez, auditez et corrigez : tests d'intrusion, plan de reprise et de continuité d'activité.

9 Les usages tu règlementeras

« Si vous pensez que la technologie peut résoudre tous vos problèmes de sécurité, alors vous ne comprenez ni les problèmes, ni les technologies...» Bruce Schneir

- Encadrez les pratiques par l'utilisation d'une charte informatique ;
- Fixez les règles et consignes que les utilisateurs doivent respecter ;
- Rendez-la opposable aux salariés soit en l'annexant au contrat de travail des salariés, soit en formalisant l'acceptation individuelle par chacun des salariés ou en lui donnant une valeur de règlement intérieur.

10 Les collaborateurs tu sensibiliseras

« Le maillon faible se situe entre la chaise et le clavier » Anonyme

- Sensibilisez les collaborateurs ;
- Nommez un responsable de la sécurité du Système d'Information pour piloter la démarche et coordonner les différentes actions à mener ;
- Impliquez et responsabilisez les usages dans les mécanismes de cyberprévention : informez, sensibilisez, formez, motivez.
- Soyez interactif et passez d'une pédagogie "passive" à une pédagogie "active".

EN SAVOIR PLUS

Retrouvez ces dix fiches pratiques en téléchargement sur Bibliordre.fr, la plateforme de téléchargement du Conseil supérieur.

POUR ALLER PLUS LOIN

- Testez vos réflexes en matière de Cybersécurité et formez-vous à la sécurité numérique grâce à l'ANSSI sur :

  www.capsurlenumerique.fr/testez-vos-reflexes-matiere-de-cybersecurite-formez-a-securite-numerique/
- Rendez-vous sur la plateforme Cybermalveillance d'assistance aux victimes :

  www.capsurlenumerique.fr/lancement-national-dispositif-assistance-aux-victimesactes-cybermalveillance/
- Visionnez avec vos collaborateurs les vidéos de la hack-academy : hack-academy.fr
- Préparez-vous au règlement européen sur la protection des données : www.cnil.fr

Constance Camilleri
Directeur de l'Innovation
du Conseil supérieur