Enquête cyber-sécurité de l'UCM

Le 7 février 2017

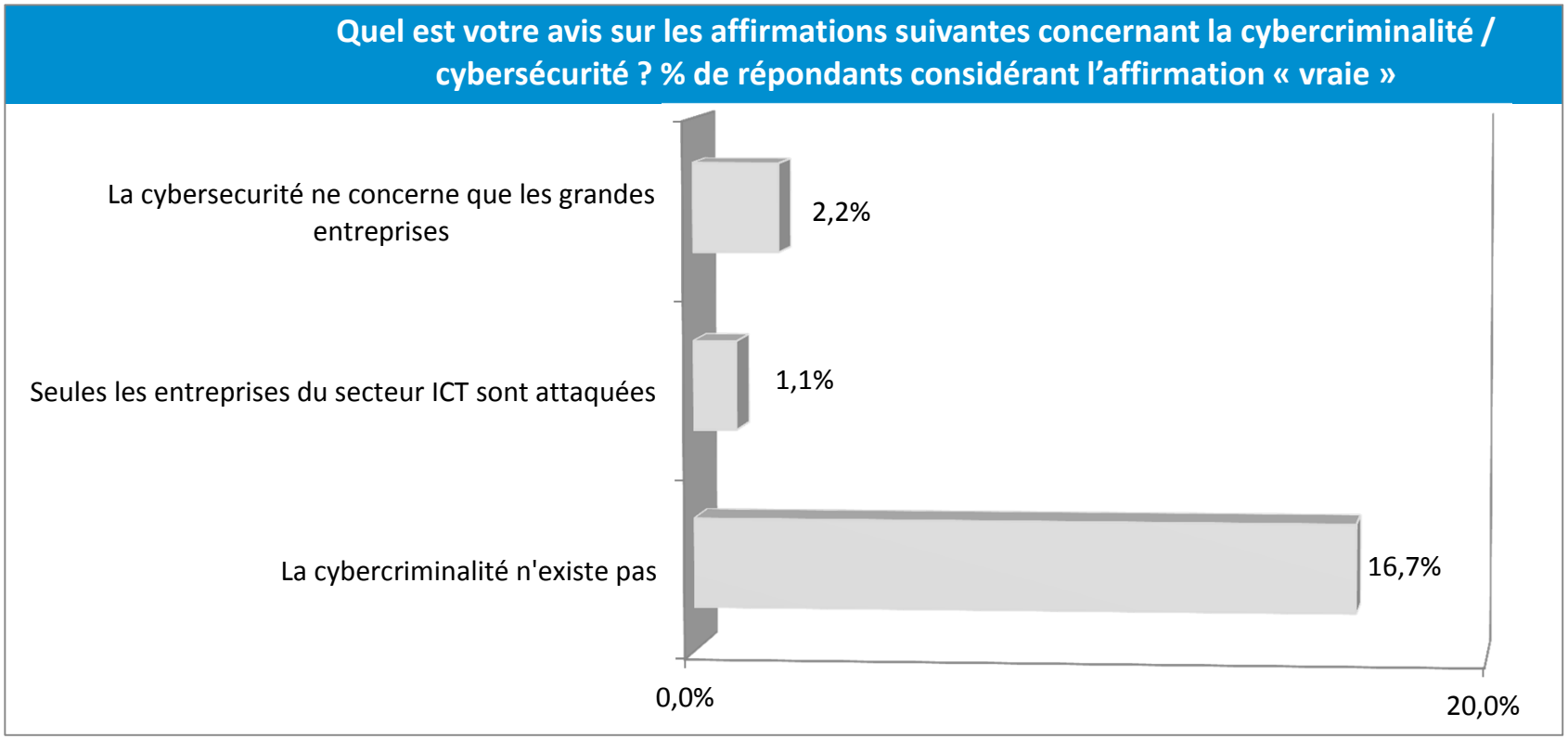
Description

- Objectif : évaluer les problèmes rencontrés par les PME francophones en matière de cyber-sécurité et leurs attentes.

- Méthodologie : enquête menée par questionnaire électronique en août 2016.

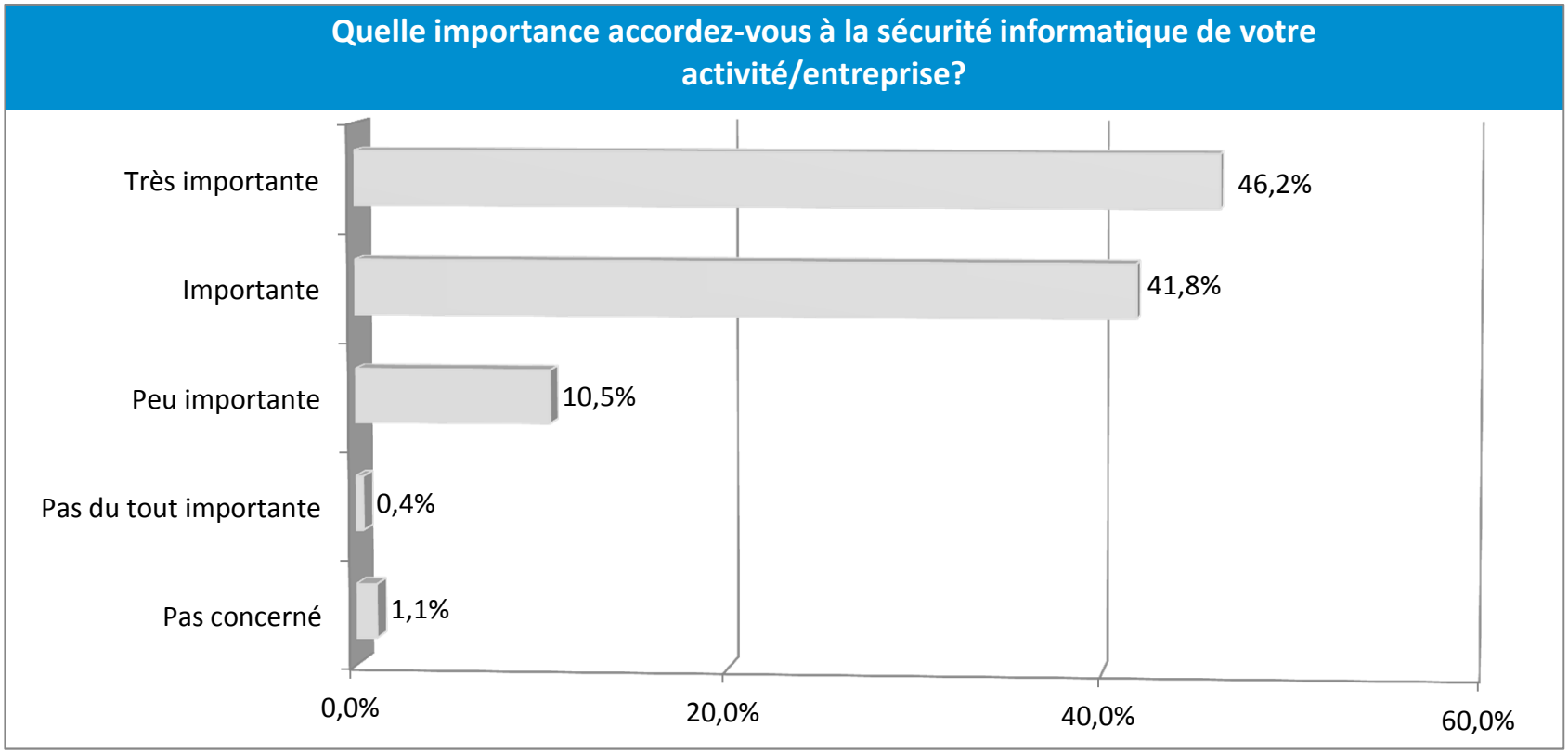
- Echantillon : panel d'environ 300 indépendants et PME francophones interrogés.

Importance de la cyber-sécurité



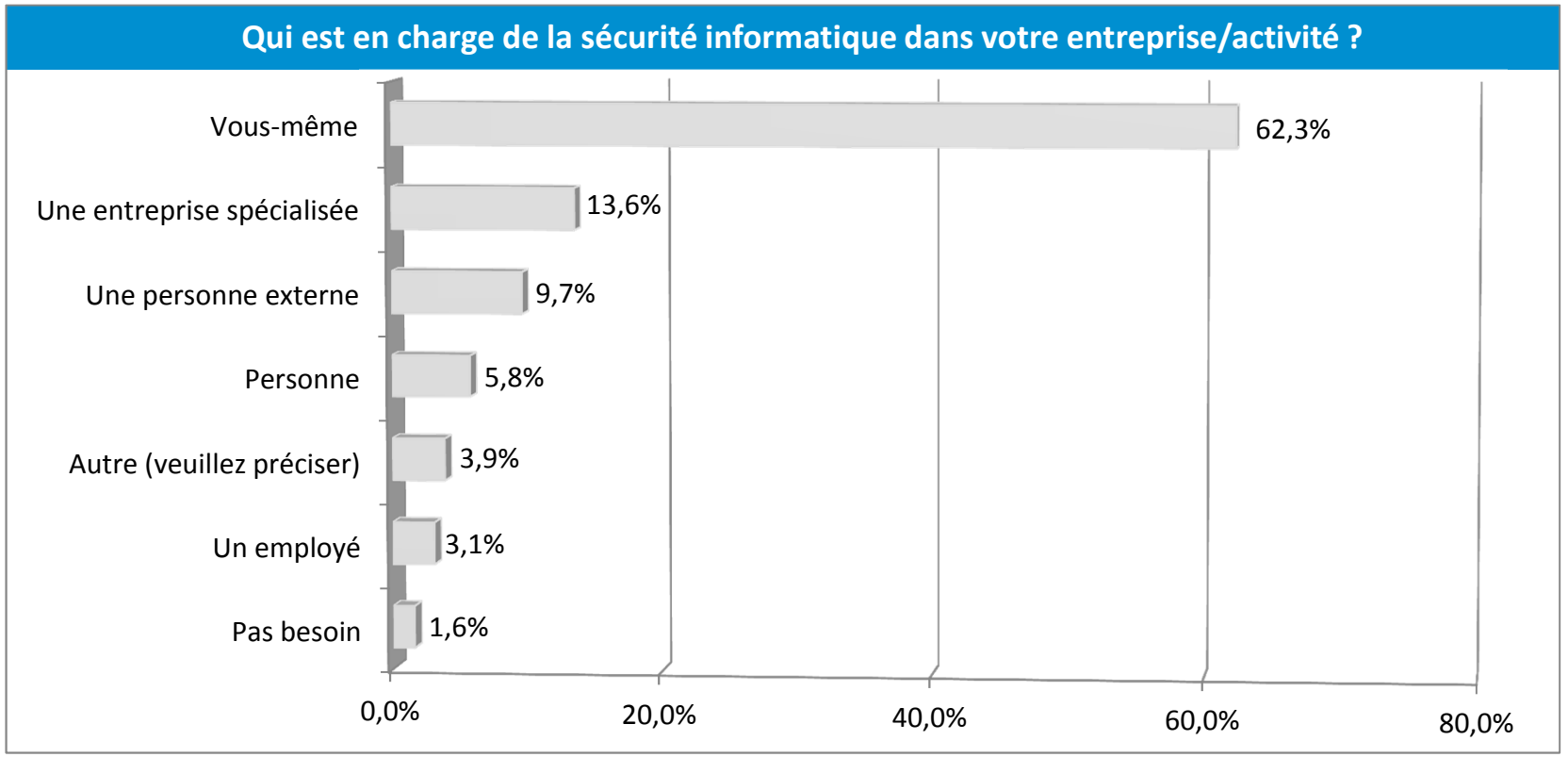
Les PME sont conscientes que la cyber-sécurité les concerne aussi : seules 2% d'entre elles considèrent que la cyber-sécurité ne concerne que les grandes entreprises.

Importance de la sécurité informatique



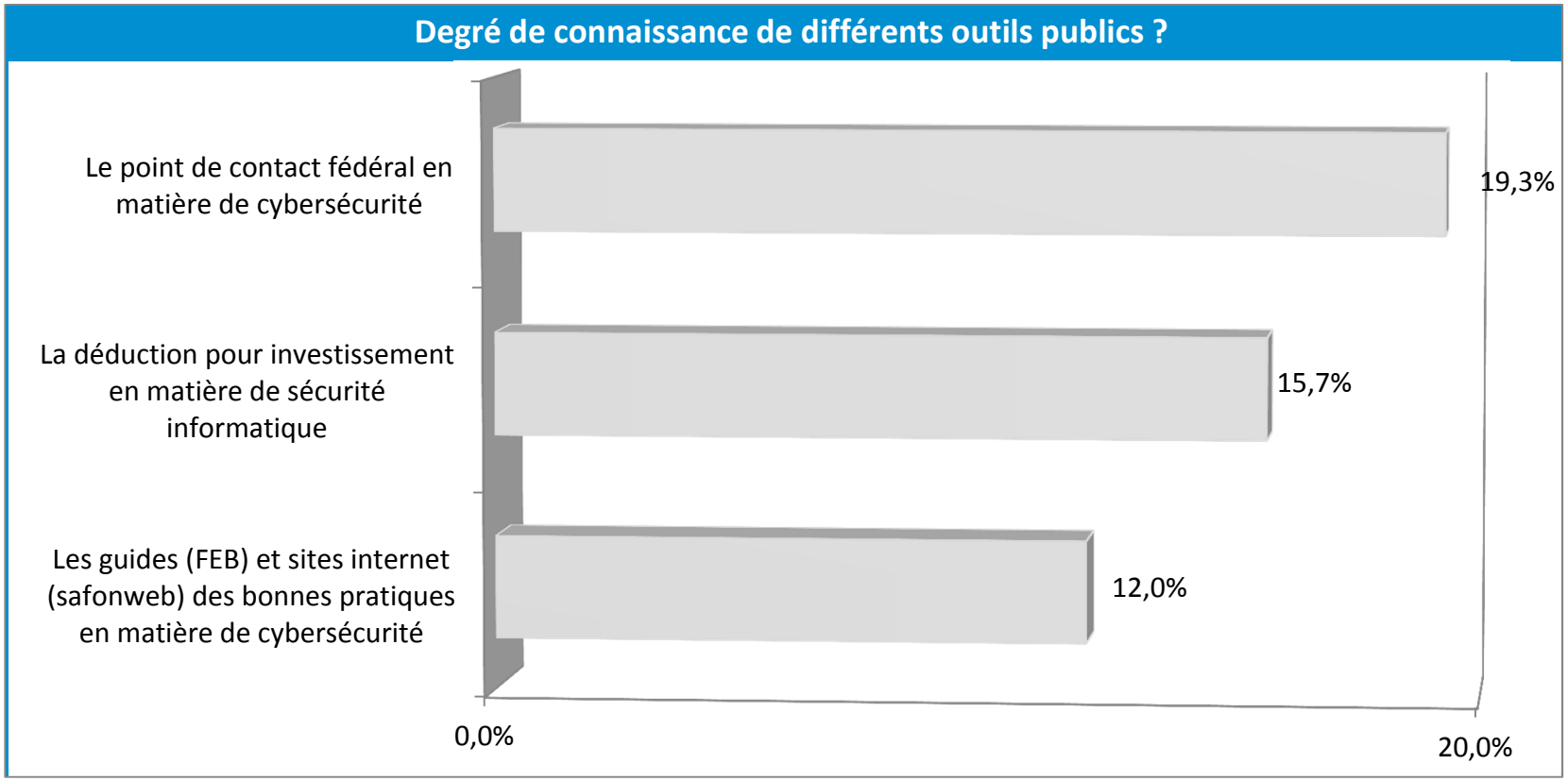
Au total 88% des PME accordent de l'importance ou une grande importance à la sécurité informatique de leur entreprise.

Gestion de la sécurité informatique



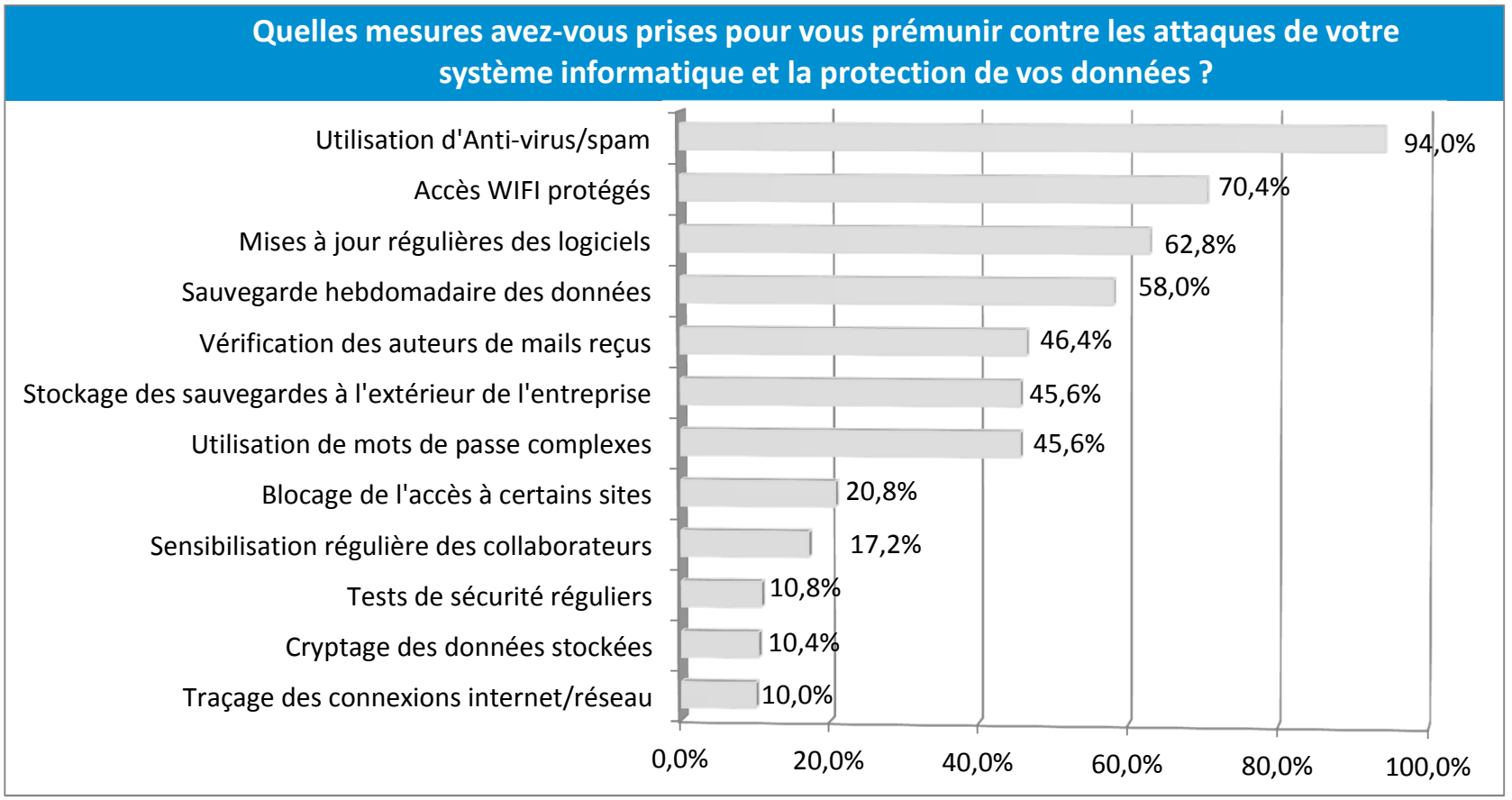
Cette question est traitée dans près de deux tiers des cas par le patron lui même. Les externes viennent ensuite.

Connaissance des outils publics



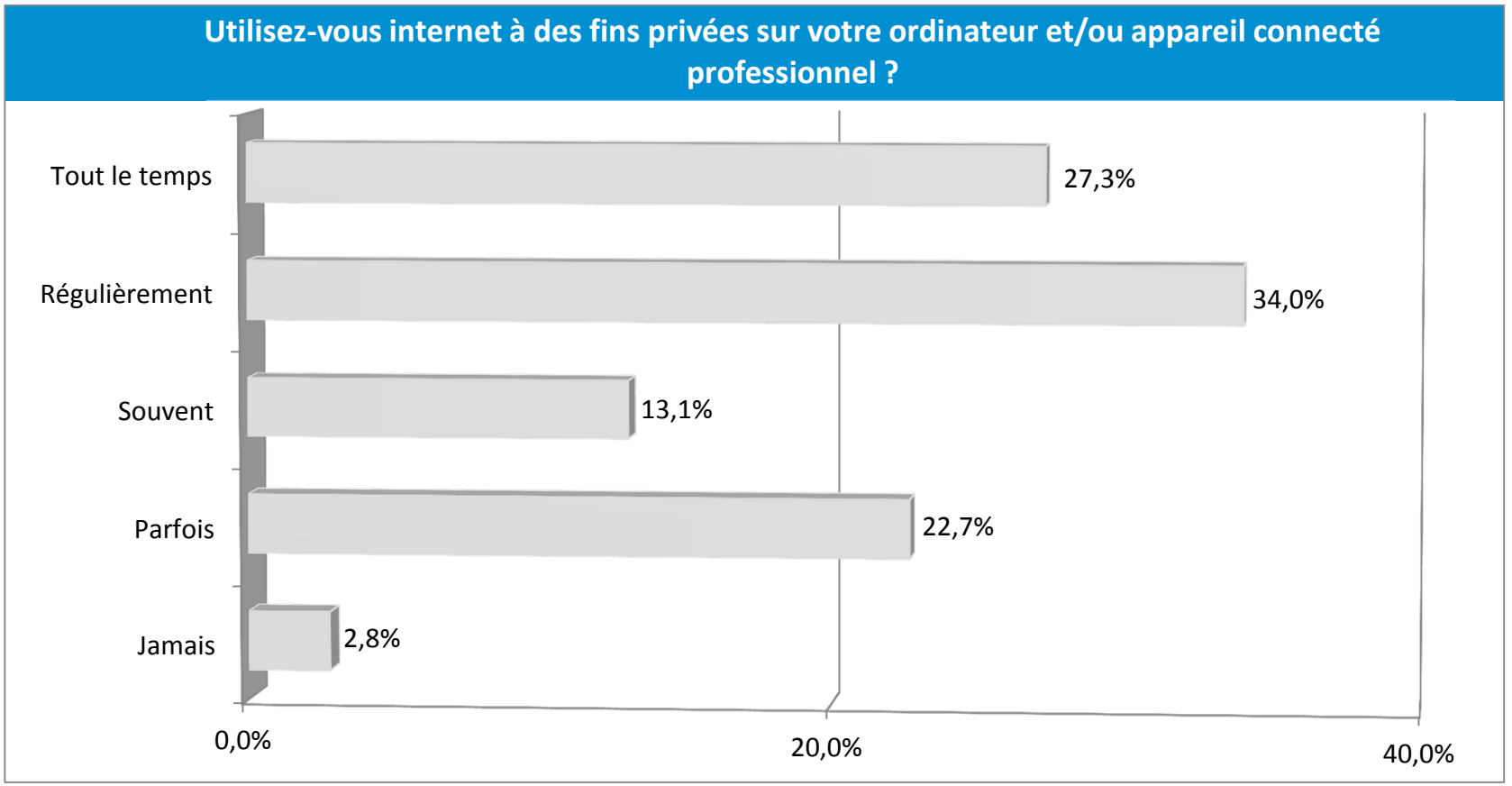
Les indépendants et les PME sont peu au courant des mesures publiques qui existent pour les soutenir ou les conseiller en matière de cyber-sécurité.

Mesures de précaution



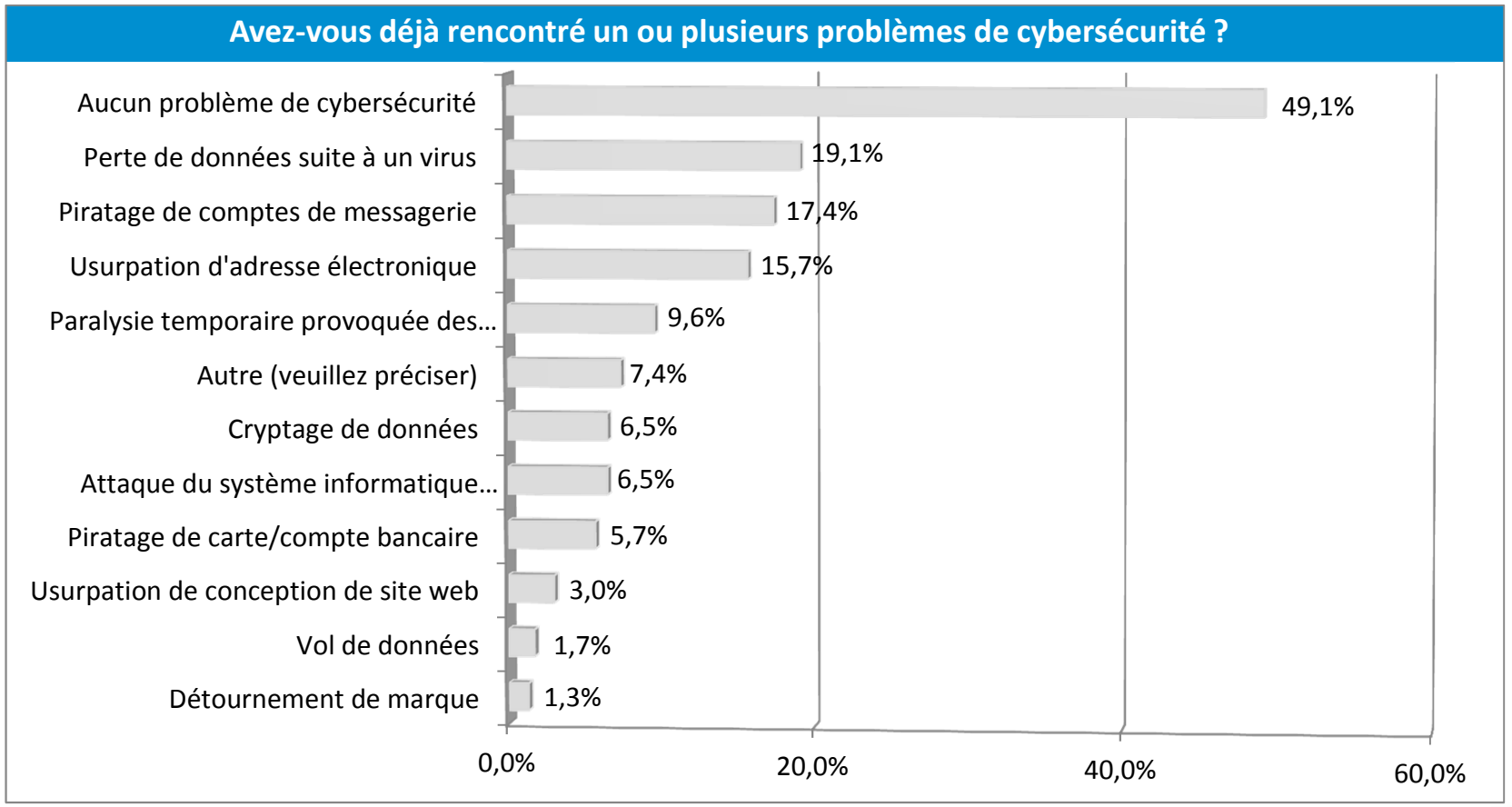
Les pratiques en termes de cyber-sécurité des PME interrogées sont encourageantes même si des pratiques à risque sont encore présentes.

Usage privé



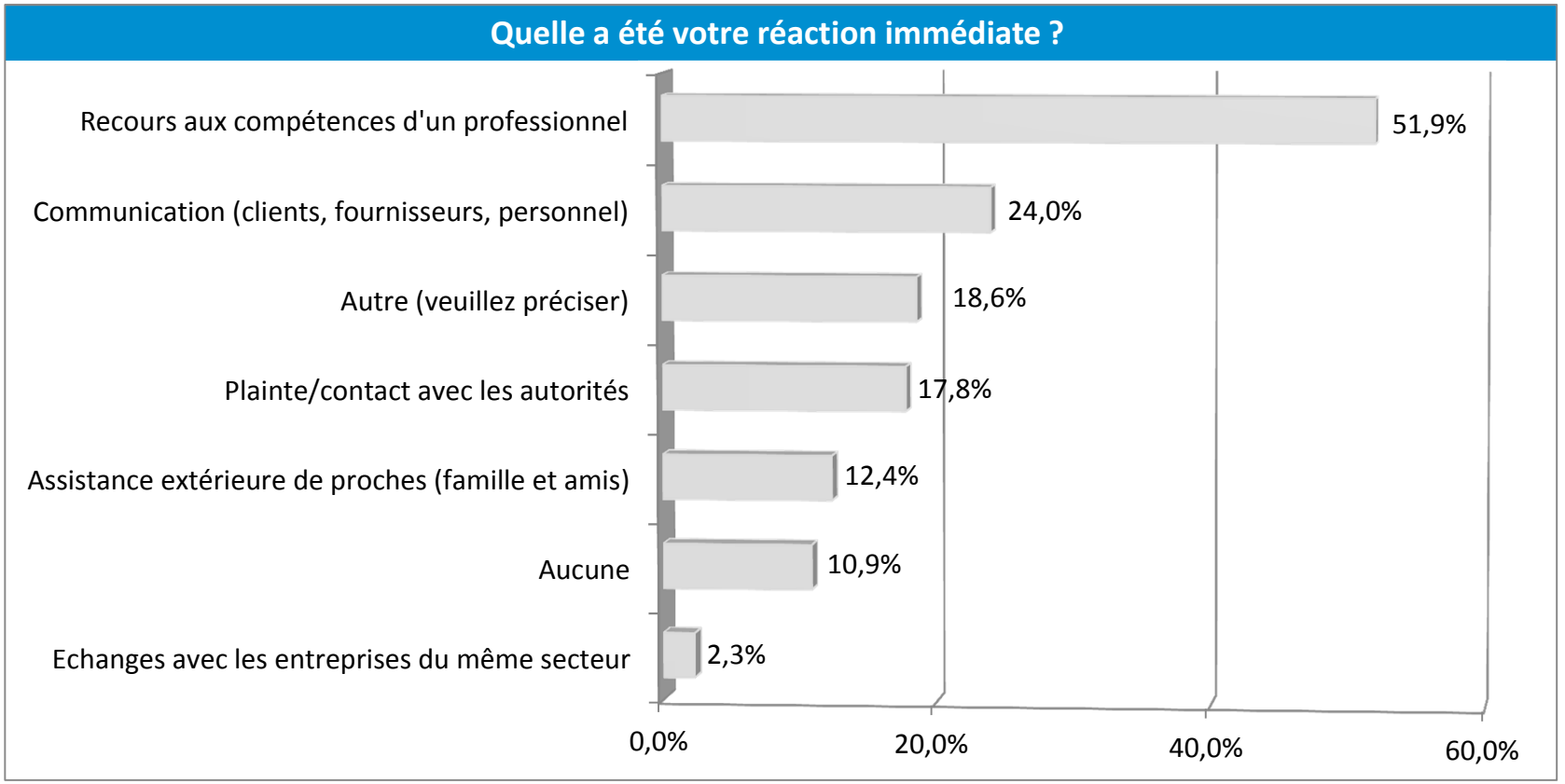
Une part importante des répondants (61,3%) utilisent régulièrement ou tout le temps internet à des fins privées.

Problèmes rencontrés



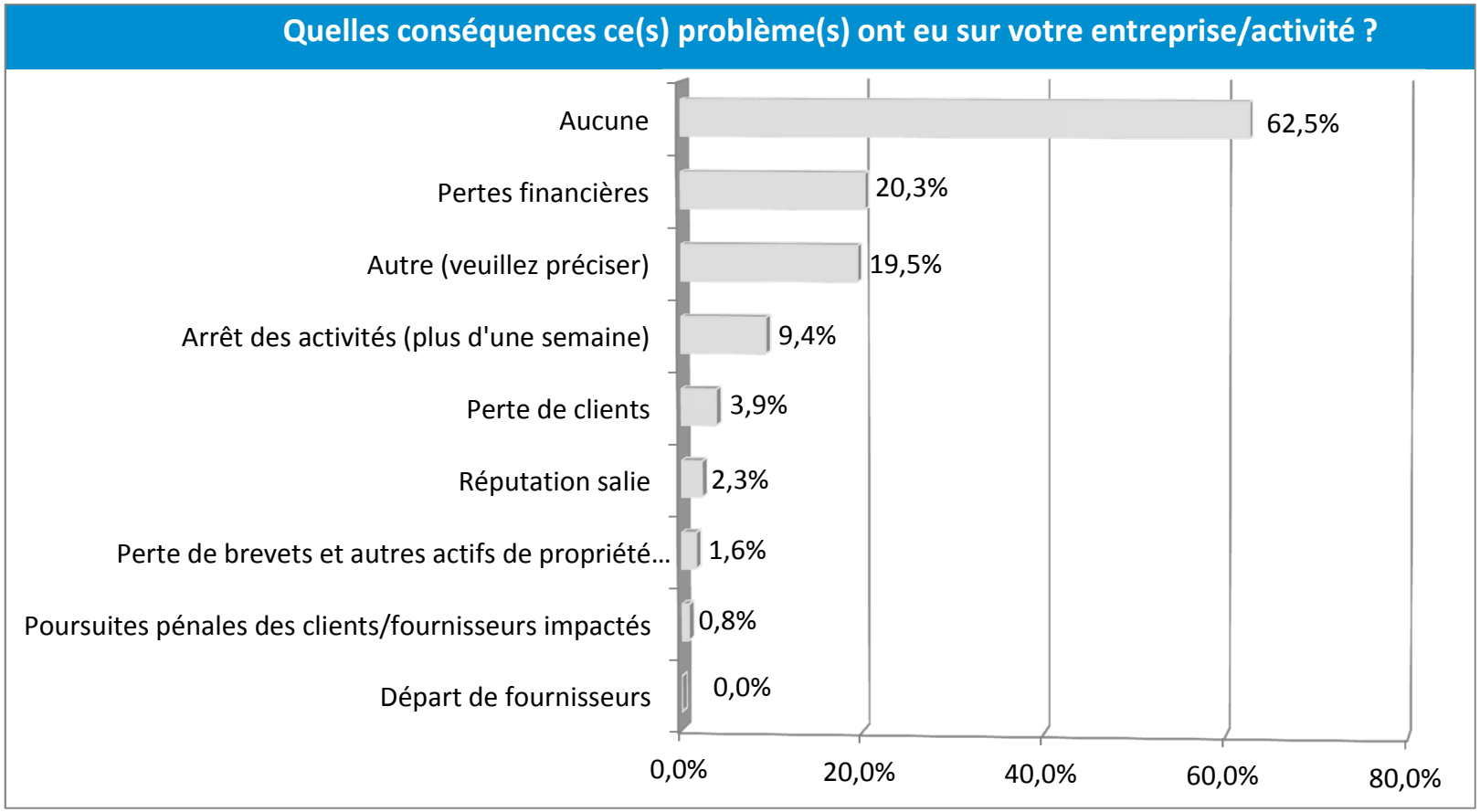
Plus de la moitié des PME interrogées (51%) a rencontré un problème de cyber-sécurité

Réaction adoptée



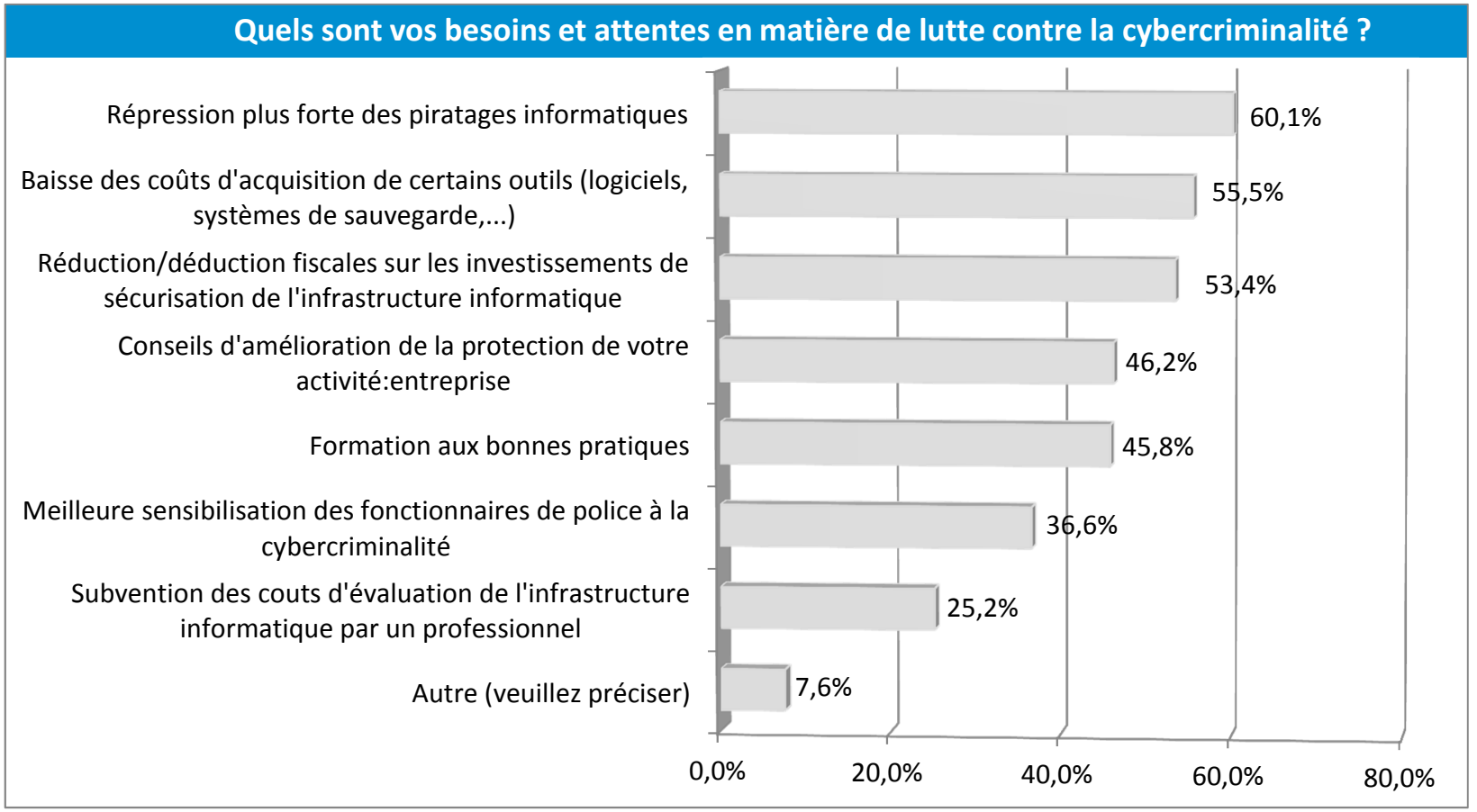
Moins d'un indépendant ou PME sur cinq a porté plainte auprès des autorités suite à un problème de cyber-sécurité qu'il a rencontré.

Conséquences



On constate de manière assez rassurante que deux tiers des entreprises qui ont rencontré un problème de cyber-sécurité n'en ont subi aucune conséquence.

Attentes / besoins



Trois priorités se dégagent : répression plus forte des piratages informatiques, baisse des coûts de certains outils et réductions/déductions fiscales.

Recommandations aux entrepreneurs

- ✓ Faire un backup journalier de ses données, cela reste la meilleure manière de limiter les conséquences de la plupart des problèmes qu'on peut rencontrer.
- ✓ S'assurer que les backups sont stockés dans des endroits distincts et de préférence éloignés des sources copiées et non connectées au poste de travail principal.
- ✓ Mettre régulièrement ses logiciels et en particulier son anti-virus à jour afin d'être protégé contre les nouvelles menaces.
- ✓ Sécuriser ses accès Wifi & doter ses appareils mobiles (Gsm, smartphone, tablette…) de mot de passe.
- ✓ Etre vigilant avec les clés USB et disques durs externes qui contiennent des données sensibles.
- ✓ Utiliser des mots de passe complexes et les modifier régulièrement. Et surtout ne pas les écrire en particulier sur un support qui se trouve à proximité de l'outil qu'il protège.
- ✓ Eviter d'utiliser à des fins personnelles des outils professionnels en particulier lorsqu'il s'agit de télécharger des logiciels ou d'acheter en ligne.
- ✓ Suivre une formation en intelligence stratégique de l'AEI qui comprend un volet sur la protection de l'information dont la cyber-sécurité.
- ✓ Recourir aux points de contacts et outils existants en matière de « cyber-criminalité » (CERT) en cas d'incident et déposer plainte au niveau de la police.

Recommandations aux pouvoirs publics

- Renforcer l'investissement des pouvoirs publics en matière de lutte contre la cybercriminalité via un renforcement des moyens consacrés par les services de police au traitement des plaintes dans ce domaine et investir dans la coopération transfrontalière dans ce domaine.

- Faire connaitre les points de contacts et ressources existantes (guides et autres) et s'assurer que ce type de point de contact puisse également fournir une information de première ligne pour les PME impactées par des problèmes de cyber-sécurité sous forme d'un « hotline » à contacter en cas de problème.

- Sensibiliser les PME / indépendants aux bonnes pratiques en matière de cyber-sécurité via : des modes de communication adaptés : web, newsletter…. un guide pratique reprenant les conseils à suivre pour prévenir les problèmes de cyber-sécurité et réagir de manière adaptée en cas de problème. des outils d'auto-évaluation des entreprises par rapport à leur niveau de cyber-sécurité.

- Développer des formations adaptées (en termes d'horaire et de contenu) ciblées sur les problèmes rencontrés par les PME : éviter la perte de données et mise en place d'un système de sauvegarde efficace, éviter le piratage des comptes de messagerie et l'usurpation d'identité. Ce type de formation serait complémentaire à l'accompagnement par des experts qualifiés.

- Intégrer la consultance en matière de sécurité informatique dans les dispositifs petites aides wallonnes avec un taux d'intervention plus élevé pour les TPE afin qu'elles puissent bénéficier plus facilement de l'accompagnement d'experts qualifiés dans ce domaine.

- Faire connaitre l'incitant fiscal fédéral en matière d'investissement en sécurité informatique et intégrer dans la liste des investissements éligibles les systèmes de sauvegarde de données adaptés aux indépendants et aux PME ou d'autres outils adaptés pour éviter l'usurpation d'identité par exemple.