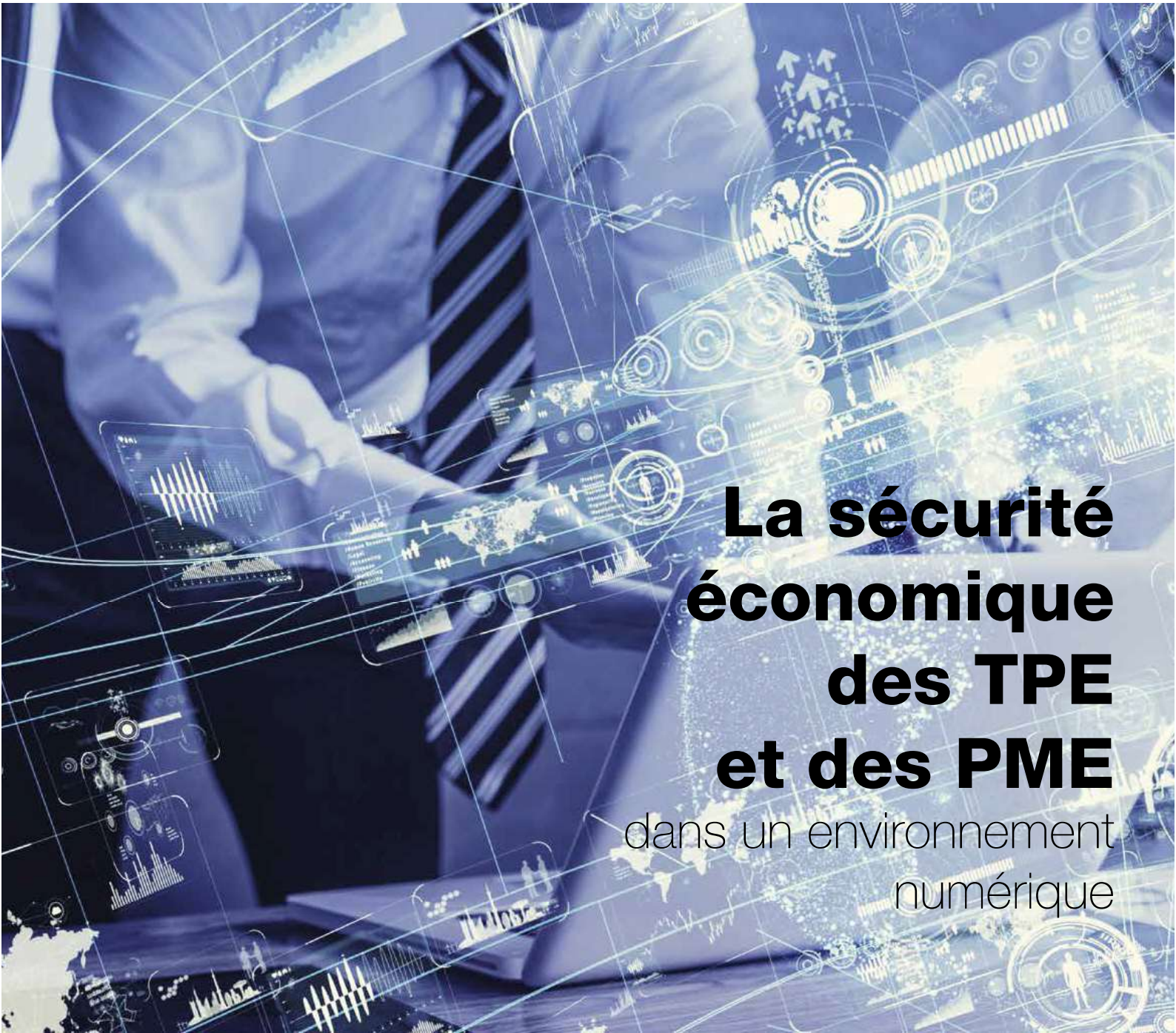
CYBERATTAQUES >
Les TPE-PME : les oubliées de la cybersécurité

DOSSIER > France Num, nouvelle initiative nationale d'assistance aux TPE-PME

DROIT > Secret des affaires : un outil de protection numérique

REVUE
de la gendarmerie nationale

REVUE TRIMESTRIELLE / AVRIL 2019 / N° 264 / PRIX 6 EUROS



La sécurité économique des TPE et des PME
dans un environnement numérique

SOMMAIRE

NUMÉRO 264

PME ET CYBERATTAQUES

DOSSIER

DROIT

TPE-PME : les oubliées de la cybersécurité

Par François Cazals

Les TPE-PME représentent un potentiel essentiel pour la France. Leur contribution humaine, économique, sociale et leur dynamisme en font de véritables accélérateurs du développement national. Sont-elles suffisamment armées pour relever les défis de la cybersécurité, qui représentent aujourd'hui un enjeu crucial pour leur pérennité ?

Après quelques définitions initiales, nous verrons le poids stratégique de ces entreprises pour notre pays. Dans un second temps, nous évaluerons la situation, les enjeux et les défis de la cybersécurité des TPE-PME. Finalement, nous proposerons quelques pistes pour élaborer une véritable stratégie Cyber, adaptée à leur taille et à leurs spécificités.

FRANÇOIS CAZALS

Professeur adjoint HEC Paris
Lieutenant-colonel Réserve citoyenne de la gendarmerie

Les TPE-PME : des atouts capitaux pour la France

Commençons par définir les concepts de TPE et PME. Les TPE sont des entreprises ayant moins de 10 salariés et un chiffre d'affaires annuel ou un bilan total inférieur à 2 millions d'euros. Depuis la loi n° 2008-776 du 4 août 2008 de modernisation de l'économie, les TPE sont renommées microentreprises (attention, toutefois, à ne pas confondre avec le régime fiscal de la micro-entreprise qui est le nom donné à l'auto-entreprise) [1]. Les PME, quant à elles, sont des entreprises qui occupent moins de 250 personnes, et qui ont un chiffre d'affaires annuel inférieur à 50 millions d'euros ou un total de bilan n'excédant pas 43 millions d'euros[2].

(1) https://www.l-expert-comptable.com/a/51980-qu-est-ce-qu-une-tpe-tres-petite-entreprise-ou-microentreprise.html

(2) https://www.insee.fr/fr/metadonnees/definition/c1962

Les 3,1 millions de TPE-PME représentent l'immense majorité des entreprises, en

France (99,8 %). Elles réalisent 1 300 milliards d'euros de chiffre d'affaires annuel (36 % du total français) et 44 % de la valeur ajoutée du tissu productif français. 360 000 (11,7 % du total) sont des entreprises exportatrices. Par ailleurs, elles pèsent pour 49 % de l'emploi salarié en France, même si 55 % d'entre-elles n'emploient aucun salarié (entreprises individuelles) [3].

(3) INSEE, Les Entreprises en France 2014 (données 2011) et Etude Ipsos pour Randstad (données 2016).

Néanmoins, elles sont en retard en matière de transformation digitale. Selon l'indice DESI (Digital Economy and Society Index) 2017 publié par la Commission européenne, les TPE et PME de l'hexagone se positionnent seulement à la 16e place du classement européen, même si 76 % d'entre-elles ont un site Web et 74 % assurent une présence sur les réseaux sociaux[4].

(4) https://www.francenum.gouv.fr/comprendre-le-numerique/20-chiffres-cles-sur-la-presence-sur-internet-des-tpe-pme-en-2018

Dans ce panorama, la cybersécurité représente évidemment un enjeu crucial de développement.

Cybersécurité des TPE-PME : le défi de la taille

Avant d'aller plus loin, définissons rapidement les principaux concepts de la cybersécurité. Voici la définition officielle donnée par l'ANSSI (Agence Nationale de la Sécurité des Systèmes d'Information) : « État recherché pour un système d'information lui permettant de résister à des événements issus du cyberespace susceptibles de compromettre la disponibilité, l'intégrité ou la confidentialité des données stockées, traitées ou transmises et des services connexes que ces systèmes offrent ou qu'ils rendent accessibles. La cybersécurité fait appel à des techniques de sécurité des systèmes d'information et s'appuie sur la lutte contre la cybercriminalité et sur la mise en place d'une cyberdéfense.[5] »

(5) https://www.ssi.gouv.fr/entreprise/glossaire/c/

(6) https://www.market-inspector.fr/blog/2017/06/cybersecurite-et-pme

Faisons un rapide bilan de la résilience des TPE-PME à ces risques Cyber[6] : celui-ci fait apparaître une situation plutôt inquiétante. Ainsi, 74 % des TPE-PME ont déjà pâti d'une cyberattaque. Le type d'attaques les plus subies par les entreprises reste la demande de rançon (Ransomware), à 80 %. Viennent ensuite les attaques par déni de service (40 %), les attaques virales généralisées (36 %) et la fraude externe (29 %). Paradoxalement, 83 % d'entre-elles se sentent peu ou pas exposées aux risques Cyber ! Ce décalage de perception montre le risque encouru.

Et pourtant, l'enjeu économique est très significatif, puisqu'il est évalué, en moyenne, à 242 000 euros, ce qui représente près de 50 % du chiffre d'affaires de la TPE moyenne, ce qui est considérable. Au-delà des conséquences financières, la réputation des entreprises est évidemment

© Elite hacker entering a room in turquoise par beebright

La problématique fondamentale est l'inadéquation entre le risque ressenti par les dirigeants quant aux valeurs de leur entreprise et la fréquence de cyberattaques frappant les petites et moyennes structures notamment celles qui recèlent des expertises techniques ou des bases de données personnelles.

affectée par un sinistre Cyber. Ainsi, 50 % des français sont prêts à poursuivre en justice les entreprises pour négligence sur leurs données personnelles. Les nouvelles règlementations européennes (RGPD[7]) renforcent, par ailleurs, les responsabilités des entreprises sur le sujet.

(7) RGPD - https://www.cnil.fr/fr/principes-cles/rgpd-se-preparer-en-6-etapes

Les causes de cet état des lieux inquiétant s'expliquent assez logiquement par des problématiques de taille, de moyens et de maturité organisationnelle. 5 à 10 % du budget global de l'entreprise devrait être alloué à la cybersécurité. C'est en tout cas l'estimation de Guillaume Poupard, directeur de l'Agence nationale de la sécurité des systèmes d'information (ANSSI). Il précise : « Oui, la sécurité a un coût, mais ce n'est pas grand-chose comparé au prix à payer lorsqu'on est victime d'une attaque informatique » [8]. Il est clair qu'il s'agit d'un effort difficilement accessible pour de petites structures, singulièrement les TPE. L'autre enjeu principal est humain, assez logiquement. Ainsi, 1 TPE-PME sur 3 confie la cybersécurité à des employés inexpérimentés. Dans le même registre, 16 % des TPE et PME laissent leur personnel stocker des informations client personnelles identifiables sur leurs propres appareils, qu'ils utilisent pour le travail[9]. Que le mobile soit financier (73 % des attaques selon le baromètre Verizon) ou l'espionnage (21 %), l'attaquant exploite la faiblesse du maillon humain dans le

(8) https://experiences.microsoft.fr/business/confiance-numerique-business/cybersecurite-chiffres-cles/

(9) https://itsocial.fr/enjeux/securite-dsi/

dispositif : la cybersécurité, c'est 20 % de technologie, 80 % de management[10].

(10) https://www.lesechos.fr/pme-regions/

Quelques pistes nous semblent réalistes pour réduire cette grande vulnérabilité Cyber des TPE-PME et renforcer leur potentiel numérique.

Renforcer la cybersécurité et concevoir une stratégie numérique des TPE-PME

Trois enjeux se dégagent pour assurer la sécurité et le développement numérique des TPE-PME.

Le premier enjeu est celui de la prise de conscience des dirigeants et de la formation des collaborateurs. Aujourd'hui, il n'est plus possible pour une entreprise, quelle que soit sa taille, de négliger la dimension numérique de son organisation. Les relations avec les services de l'État et les organismes sociaux lui imposent déjà des interactions essentiellement virtualisées (déclarations fiscales et sociales en ligne, par exemple). Par ailleurs, la visibilité sur Internet est aujourd'hui capitale pour se faire connaître. Le concept ZMOT (*Zero Moment of Truth*, le moment zéro de vérité[11]), développé par Google, postule que la recherche d'information dans un processus décisionnel commence essentiellement sur le Web. Il convient donc d'imaginer et de concevoir une véritable stratégie numérique intégrant une dimension offensive, pour se développer et défensive, de cybersécurité. Une réflexion et des outils théoriques accessibles à des petites structures permettent aujourd'hui d'aborder cet enjeu[12]. La formation des collaborateurs constitue également un défi important. De manière générale, l'effort de formation est assez faible dans les TPE-PME. Si 48 % des salariés ont suivi une formation en 2015, cette proportion s'échelonne de 25 % dans les plus petites à 63 % dans les plus grandes[13]. Le manque de disponibilité et le coût des formations expliquent facilement cette situation. Néanmoins, des solutions innovantes permettent aujourd'hui de surmonter ces difficultés. L'état met à disposition une formation en ligne sur la cybersécurité : le MOOC[14] de l'ANSSI[15]. Cette formation de 16 heures est certifiante et gratuite. D'autres formations en ligne gratuites permettent d'approfondir des aspects spécifiques de la cybersécurité, notamment au plan des risques juridiques[16].

(11) https://www.thinkwithgoogle.com/marketing-resources/micro-moments/zero-moment-truth/

(12) Stratégies digitales : la méthode des 6C (Cazals, De Boeck, mai 2018).

(13) https://www.cpformation.com/formation-tpe/

(14) L'acronyme MOOC signifie « Massive Open Online Course » que l'on peut traduire par « cours en ligne ouvert et massif » : https://moocs.unige.ch/presentation/

(15) https://secnumacademie.gouv.fr/

(16) https://www.my-mooc.com/fr/mooc/maitrisez-les-risques-juridiques-lies-au-numerique/

L'enjeu technologique est évidemment réel. Au-delà des dimensions élémentaires de la cybersécurité (logiciels de protection, pratiques de sauvegardes, sécurisation des postes de travail, …), la migration des systèmes d'information vers le Cloud permet

un renforcement significatif de la cybersécurité. Si les grands leaders mondiaux sont américains (Amazon/AWS, Microsoft/Azure, …), des solutions françaises permettent de garantir une souveraineté des données sur le territoire national (OVH, Orange, …). Ajoutons qu'il est aujourd'hui possible de choisir des solutions Web totalement respectueuses de la vie privée et qui permettent d'avoir accès à toutes les fonctionnalités Internet de base. Le moteur de recherche français QWANT se développe significativement sur cette promesse[17].

(17) https://www.qwant.com/?l=fr

(18) https://framasoft.org/fr/

Dans la même veine, le projet FRAMASOFT[18] propose 32 services numériques libres et sécurisés.

Le troisième enjeu est public : celui de la sécurité nationale des données. Cybermalveillance.gouv.fr est le programme gouvernemental assumant un rôle de sensibilisation, de prévention et de soutien en matière de sécurité du numérique auprès des particuliers, des entreprises ou des collectivités territoriales. La plateforme en ligne du dispositif est là pour accompagner les victimes d'une cybermalveillance : établissement d'un diagnostic précis de la situation, mise en relation avec les spécialistes et organismes compétents proches des victimes et mise à disposition d'outils et de publications dispensant de nombreux conseils pratiques. La gendarmerie nationale s'est évidemment engagée résolument, ces dernières années, dans la lutte contre ces nouvelles formes de criminalité, en rapport notamment avec l'utilisation de l'Internet. Cette nouvelle typologie de crimes et de délits a conduit à mettre en place aux niveaux central et territorial des formations et des moyens spécifiques[19].

(19) https://www.gendarmerie.interieur.gouv.fr/Zooms/Cybercriminalite

Conclusion

La transformation numérique de la société touche évidemment les TPE-PME. Celles-ci doivent intégrer de nouveaux enjeux : saisir les opportunités technologiques pour se développer et se prémunir de risques nouveaux. Cette reconfiguration passera par la prise de conscience des dirigeants et un effort de formation important des salariés. Dans ce contexte, l'appui de l'État sera déterminant. La gendarmerie nationale, quant à elle, va certainement devoir intégrer une nouvelle mission : à la sécurité des personnes et des biens, il faudra ajouter la sécurité des données.

L'AUTEUR

François Cazals est professeur adjoint à HEC Paris. Spécialiste des stratégies numériques et de la valorisation des données (Big Data, Data Science, intelligence artificielle), il dirige également un cabinet de conseil en stratégie. Il a rédigé de nombreux ouvrages et articles, en particulier « Stratégies digitales : la méthode des 6C » (De Boeck, mai 2018, 2e édition).
Il est également lieutenant-colonel (réserve citoyenne) de gendarmerie, affecté au cabinet du directeur général.