Cyber-Sécurité et PME : perception du risques, pratiques, besoins

Patrick Lallement
Université de Technologie de Troyes
Institut Charles Delaunay (UMR CNRS 6281)
10004 Troyes Cedex - France

21 mars 2014

1 Introduction

Dans le cadre du projet européen 2CENTRE[1], une étude a été réalisée pour évaluer la situation des PME vis-à-vis du risque cyber. Cette étude s'est appuyée sur un questionnaire en ligne, médiatisée par divers relais d'information. Cet article de synthèse (qui n'est pas le livrable final officiel du projet) est structuré de la manière suivante. On présente la situation particulière des PME (partie 1). La partie 2 explicite la méthodologie suivie, la partie 3 décrit et analyse les résultats. Ils sont discutés (partie 4) ainsi que la procédure suivie. Des recommandations sont avancées pour toute enquête ultérieure de même nature.

2 Le cas particulier des PME

2.1 Profil

Les PME sont des entreprises de moins de 250 salariées, dont le chiffre d'affaires annuel est inférieur à 50 millions d'euros, ou un total de bilan inférieur à 43 millions d'euros. La présente étude se limite au seul critère du nombre de salariés. Le profil cyber a priori est celui d'entreprises qui ne recrutent pas de compétences particulièrement dédiées à la sécurité. Cela a pour conséquence attendues une absence de politique de sécurité, des (bonnes) pratiques élémentaires (hygiène) absentes ou erratiques ou aléatoires, relativement à la protection des données, à la protection des serveurs, à la protection des postes de travail (antivirus, mots de passe). Les vulnérabilités dépendent des processus métiers, du secteur économique (part de la R & D, niveau de concurrence). Or, les PME couvrent un spectre d'activités très large, plus que les grandes entreprises : par ex. le secteur de l'exploitation agricole, de l'hôtellerie/restauration, le secteur social. On peut aussi supposer que ces PME investissent peu pour se protéger (en temps, en argent) mais qu'elles ne disposent pas de moyens de détection de la malveillance (intrusion, vol de données).

1. financement DG Home (2010-2013)

2.2 Les études relatives aux PME

Les enquêtes de type Symantec, McAfee, NSBA, relayées par de nombreux magazines, parlent même de cyber espionnage contre les PME : 1/3 des attaques en 2012, avec une augmentation de 42/Les enquêtes sur la perception du risque ont souligné depuis plusieurs années que peu de PME en Europe se sentaient concernées par la cyber criminalité. En 2008, 90/Le CLUSIF (Club de la Sécurité de l'information français) mène des enquêtes tous les deux ans sur le risque et les sinistres informatiques dans les entreprises mais cela concerne les entreprises de plus de 200 salariés. Seules les PME les plus importantes sont concernées.
On peut donc résumer les symptômes caractéristiques pointés par ces études : les PME ne se sentent pas concernées par le sujet. Elles se considèrent trop petites (donc non visibles), peu dignes d'intérêt. Certaines ont pourtant créées sur des niches technologiques (start-up). Beaucoup disposent de sites web avec des procédures de réservation / paiement en ligne. La plupart gèrent des données de savoir-faire, des données commerciales, des données comptables, des données logistiques.

2.3 Le rôle attendu des structures intermédiaires

En France, les pôles de compétitivité (pôles internationaux notamment) ont généralement un rôle de veille et de sensibilisation vis-à-vis des PME adhérentes. Leur argumentation reprend des chiffres d'études américaines le plus souvent. Le pôle PEGASE (Aéronautique et Spatial) affirme en juin 2012 que 50/Plusieurs livres blancs ont été mis à disposition en ligne pour permettre aux pme de se protéger en adoptant un minimum de bonnes pratiques. On ne sait pas quel en est l'impact ni même s'il est mesuré.
L'ANSSI (Agence Nationale de la Sécurité des Systèmes d'Information) met en ligne des documents de bonnes pratiques.
Les PME qui travaillent pour le secteur de la défense sont aussi sensibilisées par les pouvoirs publics. Celles qui travaillent dans des secteurs où la notion de confiance est très forte (aéronautique, banques) sont aussi soumises à des obligations en matière de sécurité.
La CGPME (Confédération Générale des Petites et Moyennes Entreprises), l'OSEO (organisme financeur des PME pour l'innovation), les Chambre des métiers, les chambres de commerce et d'industrie (CCI), les syndicats professionnels constituent des moyens potentiels de relai d'information (sensibilisation, veille, alertes). On s'attend à ce qu'ils jouent effectivement ce rôle.

3 Approche du problème

3.1 Référentiels existant

La norme ISO 27002 présente une série de préconisations pour répondre aux mesures définies dans un SMSI (ISO 27001). Elle définit un dictionnaire à 133 entrées (113 dans la version 2014) avec pour chacune une mesure de sécurité à prendre. Si on suivait le référentiel ISO 27002 d'analyse pour les PME, on se rend compte de trois niveaux d'inadéquation :

- Cette norme considère un même référentiel de sécurité valable pour toutes les entreprises or c'est loin d'être le cas notamment pour les TPE. Elle dé-

finit notamment 11 rubriques (Politique de sécurité (PSSI), organisation de la sécurité, gestion des biens, sécurité liée aux ressources humaines, sécurité physique, gestion de l'exploitation des télécoms, contrôles d'accès, acquisition/ développement/ maintenant des SI, gestion des incidents, gestion du Plan de continuation d'activités (PCA), conformité)
- elle considère que toutes les entreprises ont les moyens de comprendre et de s'auto gérer pour appliquer ISO 27002 : cela signifie comprendre les enjeux, les objectifs, identifier les moyens d'action.
- elle ne tient pas compte des nouveaux risques liés à l'apparition des terminaux nomades (risque BYOD, fuites de données) et à l'usage massif des réseaux sociaux (porosité dans la confidentialité des données personnelles).

3.2 Méthodologie suivie

Le comité de pilotage de l'étude a été constitué des représentants du consortium 2Centre (UTT, Gendarmerie Nationale, Université de Montpellier), aidé de représentants des Services Fiscaux, du CLUSIF, de l'intelligence économique (Jean-Paul Pinte). Il a défini comme mode d'action la mise en ligne d'un questionnaire en tenant compte des observations suivantes :
- les chefs d'entreprise sont plus sensibles à ce mode d'action.
- le niveau de perception des PME vis-à-vis du cyber risque est quasi nul. L'entreprise est ignorante du sujet, des enjeux. L'enquête doit donc tenir compte de ce facteur.
- d'autres enquêtes ont lieu (comme celle du CLUSIF) et il existe une certaine saturation des entreprises vis-à-vis des enquêtes en général. Il a donc été décidé de limiter le nombre de questions et de les rendre les plus simples possibles, donc facilement compréhensibles.
- d'autres enquêtes ont lieu (comme celle du CLUSIF) et il existe une certaine saturation des entreprises vis-à-vis des enquêtes en général. Il a donc été décidé de limiter le nombre de questions et de les rendre les plus simples possibles, donc facilement compréhensibles.

Les recommandations suivantes ont d'autres part été formulées :
- éviter les formulations anxiogènes (qui fassent référence à des chiffres comme ceux cités au §2 par ex.) et trouver le bon équilibre entre sensibilisation et désignation du risque.
- préciser que la gendarmerie est partenaire, ce qui peut avoir un effet rassurant.
- procéder par des questions simples, à réponse binaire :
- souligner ce que la participation à cette enquête va apporter (un rapport qui sera ensuite rendu public)

Il a été prévu de médiatiser l'enquête par des structures tierces citées plus haut, CCI départementales et régionales, CGPME, OSEO, pôles de compétitivité.

3.3 Structure du questionnaire

Il prévoit deux parties :
- Générique : une vingtaine de questions
- Spécifique : quelques questions en fonction de la nature des activités et du risque spécifique. Pour ces raisons il est prévu de renseigner dans les

premières questions la nature de l'activité de l'entreprise.

3.3.1 Questionnaire générique

Le questionnaire générique comprend plusieurs groupes de questions, relatifs :

- au profil de l'entreprise
- au profil informatique de l'entreprise
- à la politique de sauvegarde des données
- au comportement en cas d'incidents
- aux besoins (informations, documents, assistances)

3.3.2 Questionaire spécifique

Les questions spécifiques peuvent être regroupées et classées de la manière suivante :
G1 : questions relatives aux fichiers contenant des informations de savoir-faire : brevets, algorithmes, codes source, recettes, design, etc., tout ce qui constitue la spécificité de l'entreprise vis-à-vis de la concurrence
G2 : données personnelles. Il s'agit des données sur des personnes dont le dossier est traité par l'entreprise, typiquement le domaine social, médical, mais aussi médiatique (photo, vidéo).
G3 : site web, e-activité. Cela concerne les entreprises disposant d'un site web à des fins commerciales notamment. Mais cela concerne aussi les activités CRM [2] de l'entreprise (centre d'appels par ex.). La question doit cibler la vulnérabilité d'un tel système vis-à-vis d'attaques de type "Déni de Service (DoS)".
G4 : système automatisé de production. Cela concerne les activités de production en général avec des automates en réseau avec un serveur de supervision (type SCADA [3]). Cela concerne aussi les systèmes des opérateurs (énergie, eau).
G5 : Systèmes de contrôle centralisés. C'est un peu le même système que précédemment mais les applications sont différentes et concernent la protection des systèmes logistiques et physiques : réseaux de transport, contrôles d'accès. Cela peut dans l'absolu concerner toutes les entreprises qui ont mis en place un système de détection d'intrusion ou d'incident (capteurs, caméras)
G6 : données logistiques (fournisseurs, états des stocks, etc.). Ces données sont sensibles (surtout les stocks) car elles servent à déclencher des actions de production ou de réapprovisionnement. Toute falsification d'un état de stock a pour conséquence des dysfonctionnements de la supply chain (rupture de stock ou réapprovisionnement anticipé).
G7 : données clients. Dans l'absolu toute PME a des clients mais ce qui est visé ici, ce sont les activités pour lesquelles le fichier client représente une valeur en soi, pour la concurrence, pour des activités connexes : opérateur télécoms, assurances, banques, hôtellerie, etc. Ces données clients sont constituées de l'identité, de l'adresse, du numéro de tel, de l'adresse mail, voire même des coordonnées bancaire (un numéro de carte bancaire souvent demandé comme caution par certains hôtels, conservé combien de temps ?).
G8 : Données commerciales. Par définition les tarifs sont toujours publics mais

2. Customer Relationship Management
3. Supervisory Control and Data Acquisition

certaines données le sont moins comme les tarifs inter-entreprises, les tarifs promotionnels, les tarifs négociés. Les tarifs publics peuvent être falsifiés et publiés à tort. Des ventes traitées de manière automatique (e-commerce) peuvent alors s'effectuer très vite dès l'ors qu'un prix été falsifié à la baisse. Les tarifs négociés constituent eux une donnée stratégique pour la concurrence. Toutes les activités commerciales sont concernées.
G9 : E-dépendance. Il s'agit des activités qui dépendent de données consultées sur des sites spécialisés : cotations, données météo. Le monde agricole peut être concerné mais aussi les activités qui utilisent de la matière première : minerai, hydrocarbures, bois, etc.
G10 : historiques de données. Il s'agit d'historique et non d'archivages. Les historiques de données servent typiquement à faire des calculs de prévision. La falsification de ces données peut avoir pour conséquence des prévisions fausses. Sont concernées toutes les activités de production, l'agriculture, le commerce, etc.
G11 : Données physiques sur les biens, les infrastructures, les bâtiments (Documents relatifs aux plans, aux accès, ce qui représente une information sensible)
On voit que la plupart des questions se posent sur la protection des données mais qu'il existe des cas spécifiques auxquels il faut poser des questions précises, voire les formuler de manière adaptée. Par exemple les PME concernées par les études de marché tel le bâtiment ; ou encore le domaine de l'hôtellerie, parce qu'il constitue un sujet un peu spécifique.
D'autre part, certaines activités qui ne sont pas codifiées explicitement dans la typologie NAF [4], appartiennent à des sous-catégories, mais elles présentent une vulnérabilité particulière à cause des flux financiers qu'elles génèrent (ainsi la joaillerie).
Certaines entreprises cumulent plusieurs activités. Ainsi un propriétaire récoltant dans le vignoble champenois appartient à la catégorie Code NAF 01.21 (culture de la vigne) mais aussi 11.02 (production de vins) et généralement commerce de détail avec en plus un portail pour la vente en ligne. Il en est de même pour beaucoup d'entreprises de production / vente.
Le tableau 1 répartit les groupes de questions (Gi) par secteur d'activité renseigné dans le questionnaire générique.

4 Résultats par critères

Sur un total de 230 connexions, seules 83 entreprises ont rendu un questionnaire complet. Les autres n'ont apparemment rien sauvegardé. Ce sont ces 83 réponses que nous allons exploiter ici.

4.1 Profil des entreprises

Le tableau 2 renseigne sur l'origine des entreprises qui ont répondu, le tableau 3sur leur âge, le tableau 4 sur leur secteur d'activité, le tableau 5 sur leur taille.

On constate globalement que les entreprises répondantes sont jeunes. Leur taille est assez répartie. Les secteurs d'activité sont majoritairement l'industrie

4. Nomenclature d'Activités Français

Secteur	G1	2	3	4	5	6	7	8	9	10	11
Agriculture	X	X	-	-	-	-	-	-	X	X	-
Industrie	X	-	X	X	X	X	-	-	X	X	-
Artisanat	X	X	-	-	-	-	-	-	-	-	-
Prod./distri. eau/énergie	-	-	-	X	-	-	X	-	-	-	-
Traitement déchets/eaux usées	-	-	-	X	-	-	-	-	-	-	-
Commerce	-	X	-	-	-	X	X	X	-	X	-
Transport	-	-	-	-	X	-	-	-	-	-	-
Hébergement	-	X	X	-	-	-	-	X	-	-	-
Prod. culturelle	X	-	X	-	-	-	-	-	-	-	-
Finances	-	X	X	-	-	-	-	X	-	X	-
Télécoms/TIC	-	-	-	-	-	-	X	-	-	X	-
BTP/Génie civil	-	-	-	-	-	-	X	-	-	X	X
Dévelpt (hard/soft)	-	-	X	-	-	-	-	-	-	-	-
Sécurité privée	-	X	-	-	X	-	X	-	-	-	X
Juridique	-	X	-	-	-	X	X	-	-	X	-
Médical	-	X	-	-	-	-	-	-	-	X	-
Médico-social	-	X	-	-	-	-	-	-	-	-	-

TABLE 1 – Questions spécifiques par type d'activité

Origine	(%)
Héritage/transmission	3,6
Création chef d'entreprise	74,7
Autre	21,7

TABLE 2 – Origine des entreprises

Age de l'entreprise	(%)
Moins de 3 ans	13,25
De 3 à 5 ans	8,43
De 5 à 10 ans	19,28
De 10 à 15 ans	22,89
De 15 à 20 ans	10,84
De 20 à 25 ans	8,43
De 25 à 50 ans	9,64
Plus de 50 ans	7,23

TABLE 3 – Age des entreprises

Activité	(%)
Industrie	13,25
Juridique	2,41
Sécurité privée	6
Agriculture	1,2
BTP/Travaux publics	1,2
Médical	1,2
Développement TIC	49,4
Production culturelle	1,2
Distribution (eau, énergie)	1,2
Services financiers	3,61
Télécoms/TIC	7,23
Transport/logistique	3,61
Autre	8,43

TABLE 4 – Secteur d'activité des entreprises

Taille	%
1 salarié	3,61
De 1 à 10 salariés	19,28
De 10 à 50 salariés	33,73
De 50 à 100 salariés	14,46
Plus de 100 salariés	28,92

TABLE 5 – Taille des entreprises

et l'informatique.

4.2 Profil IT des entreprises

Le ratio PC/ employé est donné table 5.

PC / employé	%
Au moins 1	85,54
moins de 1	14,46

TABLE 6 – Taux d'informatisation du poste de travail

Les cas où le ratio est inférieur à 1 correspondent à des activités autres que celles liées à l'informatique ou aux TIC. Le tableau 7 montre l'usage applicatif que l'entreprise fait de l'informatique. Certaines réponses montrent que la question n'a pas forcément été bien comprise ou que le répondant n'avait pas de vue globale permettant de répondre complètement.

La plupart des entreprises interrogées disposent d'un réseau local (95%). Environ 82% disposent d'un serveur applicatif (type base de données).
L'ordinateur professionnel est aussi l'ordinateur personnel pour 25,3% des répondants. Environ 24% des entreprises limitent le nombre de postes connectés à internet. Pour les autres, tous les postes ont accès. Pratiquement toutes les entreprises disposent d'un site web. Les services de ces sites sont résumés tableau 8.

Comptabilité	GRH	Comm	Prod	%
N	N	N	Y	13,25
N	N	Y	N	4,82
N	N	Y	Y	8,43
N	Y	Y	Y	2,41
N	Y	N	N	3,61
Y	N	Y	N	6,02
Y	N	Y	Y	6,02
Y	Y	N	Y	1,2
Y	Y	Y	N	19,28
Y	Y	Y	Y	34,94

TABLE 7 – Usages de l'informatique

Usage	% Oui	%Non
Informer	89	11
Traiter des questions en ligne	14,5	85,5
E-commerce	16	84

TABLE 8 – Usage du site web de l'entreprise

Les ressources informatiques sont gérées de manière hétérogène (voir tableau 9). Pour plus de la moitié, il s'agit d'un salarié en particulier.

Qui ?	%
Dirigeant	12,05
Employé particulier	53,01
Externe	19,28
Personne en particulier	12,05
Autre	3,61

TABLE 9 – Chargé de l'infogérance

4.3 Pratiques de sécurité

Le tableau 10 synthétise le comportement des entreprises en matière de sauvegarde de leurs données. On peut être surpris du résultat (15% n'ont pas de politique en la matière) et on s'attend à ce que les entreprises qui ne sauvegardent pas ne sont pas sensibilisées au sujet. Or sur les 13 entreprises concernées, 10 travaillent dans le domaine informatique.

Les entreprises qui pratiquent la sauvegarde de données utilisent différents modes. Le tableau 11 montre que la majorité utilise la sauvegarde sur un serveur. La rubrique autre mentionne en réalité des modes de stockage comme : bande, baie dédiée dupliquée, disque dur externe + serveur raid sur chaque poste, cassette.

A la question : pratiquez-vous un stockage protégé physiquement (incendie, inondations, etc.) la réponse a été :

Fréquence sauvegardes	%
Au moins 1 / jour	42,17
Au moins 1/ semaine	22,89
Au moins 1 / mois	15,66
Au moins 1 / an	3,61
Jamais ou ne sait pas	15,66

TABLE 10 – Fréquence des sauvegardes

Mode	%
Externe	7,04
Serveur	56,34
Autre PC	4,23
Disque externe	22,54
Autre	9,86

TABLE 11 – Mode de sauvegarde

OUI : 45% NON : 25% N/A : 13%

A la question : Avez-vous déjà eu recours à ces sauvegardes ?, la réponse est synthétisée tableau 12. On voit que plus d'un tiers des répondants ne les ont pas utilisées et qu'un peu moins d'un tiers les ont utilisées plusieurs fois. La cause identifiée est explicitée tableau 13. L'erreur humaine est la cause à 45%. On ne sait pas vraiment ce que cela recouvre mais on peut imaginer des erreurs de manipulation ou des effacements involontaires. Les erreurs système sont l'autre grande cause identifiée (47,5%). La malveillance n'est identifiée qu'à 5% mais on peut s'interroger sur le niveau de détection et d'identification de cette malveillance. L'erreur système est un symptôme, l'erreur humaine et la malveillance sont des causes possibles.

Usage	%
Plusieurs fois	30,12
Une fois	18,07
Jamais	36,14
Ne sait pas	15,66

TABLE 12 – Usage des sauvegardes

Cause	%
Erreur humaine	45
Malveillance	5
Crash disque	47,5
Ne sait pas	2,5

TABLE 13 – Cause de l'utilisation de la sauvegarde

Si on interroge sur le niveau de confiance envers ces sauvegardes (gradué de N1 à N4) on s'aperçoit (tableau 14 qu'une grande majorité des répondants ne

se prononce pas.

Niveau de confiance	%
N1	2,41
N2	2,41
N3	6,02
N4	22,89
Inconnu	2,41
Ne sait pas	65,06

TABLE 14 – Niveau de confiance envers les sauvegarde

Une grande majorité des entreprises utilisent un anti-virus (environ 94%). Le niveau de sécurité perçu est donné tableau 15. Les deux tiers des répondants ne se prononce pas ou ne sait pas. Seuls 7% le considèrent comme sûr.
Pour les entreprises qui ont un site web (pratiquement toutes) environ 24,7% seulement ont dupliqué leur serveur pour pallier à une indisponibilité de leur serveur.
Près d'un tiers (31,3%) ont anticipé l'usurpation de leur nom de domaine.

Sécurité perçue	%
Mauvaise	3,61
Suffisante	22,89
Correcte	7,23
Ne sait pas	2,41
Ne peut dire	63,86

TABLE 15 – Niveau de sécurité perçu

4.4 Comportement en cas d'incidents

En cas d'incident constaté, les entreprises se comporteraient de la manière suivante (tableau 16).

Comportement	%OUI	%NON
Remettre en route le système	9,6	90,4
Evaluer soi-même la situation	45,8	54,2
Faire sa propre enquête	28,9	71,1
Porter plainte	65	35

TABLE 16 – Comportement en cas d'incident

4.5 Identification des besoins

Dans tous les cas, les besoins exprimés se répartissent de la manière suivante (tableau 17). On voit que l'information, la sensibilisation, le guide de bonnes pratiques restent les trois éléments prioritaires. Le besoin n'est pourtant pas unanime (moins des deux tiers). L'assistance et la formation ne sont pas les

priorités.

Suggestion	%OUI	%NON
Sensibilisation	58	42
Information	57	43
Partage avec des homologues	35	65
Conseil	37	63
Assistance	17	83
Guide pratique	57	43
Formation	29	71

TABLE 17 – Expression des besoins

4.6 Questions spécifiques

Compte tenu de la faible participation par activité, il est préférable de raisonner par type de question. a) Protection des données de savoir-faire La tendance qui se dégage des réponses pourtant sur ce point est la suivante :
Présence de ces fichiers : oui
Partage entre plusieurs acteurs ou services : plutôt non dans le domaine industriel
Sauvegarde spécifique : pas de tendance
Accès restreint : plutôt oui, parfois chiffrement
b) Protection des données personnelles
Présence d'un dispositif de protection : oui
Données sauvegardées : oui
Données protégées : non
c) Systèmes de production
Systèmes automatisés : plutôt non et s'ils sont présents ils ne sont pas particulièrement protégés
d) Système de contrôle
Systèmes automatisés : oui
Reliés à internet : oui
e) Données logistiques
Donnés protégées : oui (dans le domaine industriel)
f) Données des clients
Protection : plutôt oui (dans le monde financier)
g) Données commerciales
Globalement, elles ne sont pas protégées
h) E-dépendance
Oui dans le monde agricole (1 réponse) et il serait contraignant de ne plus accéder à des sites spécialisés.
i) Historiques de données
Il n'est pas sûr qu'elles bénéficient de protection particulière.
j) Données physiques
Aucune réponse n'a été fournie sur ce point.

5 Synthèse, discussion

5.1 Les limites en termes d'interprétation

Le nombre de réponses est globalement insuffisant. Compte tenu de la variété ciblée (17 catégories), il aurait fallu un millier de réponses pour les exploiter statistiquement et ensuite tirer des conclusions d'ensemble. De plus les réponses aux questions génériques sont quasiment inexploitables. Il faut mentionner ici que des intermédiaires n'ont pas joué leur rôle, soit par refus, soit par absence de réponse ou bien leur contribution n'a pas été perceptible. D'autres l'ont été d'avantage (anciens étudiants, listes personnelles) ce qui montre que le facteur confiance envers le requêtant est un critère majeur pour lire les mails et répondre à cette sollicitation.
On ne sait pas qui a répondu, il est possible que des questions aient été mal comprises ou que des réponses aient été données sans réelle connaissance de cause.
L'interprétation proposée ne tient pas compte du profil de l'entreprise, or ce sont potentiellement des facteurs qui peuvent soulever des interrogations quant à la perception du risque. Une entreprise de petite taille dispose peut-être de ressources moindres pour se protéger. Une entreprise plus ancienne aura peut-être une expérience en matière de cyber incident que n'a pas une entreprise plus récente.
Compte tenu du nombre de réponses, on peut a posteriori regretter le nombre de questions, peut-être trop important dont certaines n'ont pas vraiment été exploitées.
Une grande incertitude subsiste quant à la perception du risque d'autant qu'on ne sait pas vraiment si les entreprises ont les moyens de détecter les incidents.
Des questions orientées " intelligence économique " auraient sans doute été pertinentes. Par ex. Si vous constatez qu'un concurrent a mis sur le marché un produit ressemblant au votre ?

5.2 Propositions d'amélioration

Le taux de répondants par rapport au nombre de connexions laisse perplexe. Pourquoi des entreprises sont allées voir le questionnaire mais n'ont pas répondu ? Trop de questions ? Manque de temps ? Questions trop précises et trop techniques ? Les pistes d'amélioration portent sur le dispositif et le contenu.
Concernant le dispositif, peut-être faut-il faire une étude ciblée par type d'activité à condition de le médiatiser via des syndicats professionnels ou autre intermédiaire pertinent : par ex. le monde du bâtiment, de l'hôtellerie, de la santé, etc. Cela peut permettre de restreindre le nombre de questions et de porter un diagnostic par catégorie professionnelle (celle-ci étant en retour plus intéressée par le résultat).
Concernant le contenu, peut-être faudrait-il ne poser des questions techniques qu'à ceux qui savent y répondre ? Dans ce cas on pourrait adopter une évaluation du risque comme celui de la méthode MOS (Mean Opinion Score), très utilisée pour évaluer le niveau de qualité de service perçu dans les services de télécoms, ce qui permet une approche plus qualitative et d'exploiter les résultats plus quantitativement par la suite.

5.3 Corrélation des variables

Ce livrable ne procède à aucune étude statistique de dépendance entre des variables. Il faudrait pour cela une quantité de données plus importante. Mais on peut néanmoins se poser plusieurs questions, notamment quant à l'influence de plusieurs paramètres sur l'évolution du risque, à savoir :

- La taille de l'entreprise : plus elle est faible, plus la gestion du SI et donc de la sécurité devient hasardeuse (pas de personnel dédié, confusion entre outil de travail et outil personnel, manque d'implication sur le sujet). La sécurité risque d'être perçue comme un facteur de coût.
- Le secteur d'activité : plus on se place dans le domaine des services (plus le poste de travail comprend un PC et donc le nombre de PC tend vers le nombre de salariés). Dans le domaine industriel, le poste de travail correspond à une machine de production. La culture industrielle ne va pas toujours de pair avec la culture TIC dans les petites entreprises
- L'âge de l'entreprise : les entreprises récentes ont été créées par des personnes plutôt jeune avec une culture / formation en TIC plus élevée, ce qui est a priori un critère favorable à la prise en compte de contraintes de sécurité.

Une autre hypothèse mériterait d'être testée : la non perception du risque cyber n'est-elle pas le reflet du faible taux de numérisation des processus d'entreprises ? Autrement dit : la non perception des risques reflète la non perception des avantages. Ceci concerne les entreprises qui n'ont pas répondu à ce type de questionnaire, des entreprises qui répondent généralement qu'elles ne se sentent pas concernées.

5.4 Proposition d'un processus complet

Si on veut communiquer avec d'autres entités européennes pour conduire la même étude et exploiter des résultats, l'idéal est d'utiliser un référentiel commun pour le faire. Le respect de la norme ISO 27002 implique de poser 113 questions. Vis-à-vis d'une PME un questionnaire en ligne conforme à un tel référentiel n'est pas possible :

- Poser 113 questions représente environ 2H pour répondre en ligne.
- Les questions ne seront pas forcément comprises.
- On ne sait pas qui répond au questionnaire.

Compte tenu de l'expérience acquise lors de cette étude et notamment :

- Il est difficile d'intéresser et de mobiliser les PME (taux de réponses complètes sur nombre de connexion 1/3)
- On ne sait pas exactement qui répond au questionnaire et surtout s'il sait vraiment répondre.
- Les questions les plus simples (et donc compréhensibles) ne permettent pas forcément d'être en adéquation avec le référentiel ISO 27002

En conséquence, nous préconisons de sortir de cette relation frontale en aveugle (une personne qu'on ne connaît pas répond à un questionnaire automatisé) pour soit l'adapter de manière progressive, soit recréer une relation d'égal à égal. L'objectif final n'est pas de collecter des réponses à des questions mais de trouver les bons vecteurs pour disséminer les bonnes pratiques. Nous proposons deux approches : dans la première on reste dans un processus en ligne mais progressif. Dans le second, il s'agit d'un processus d'audit.

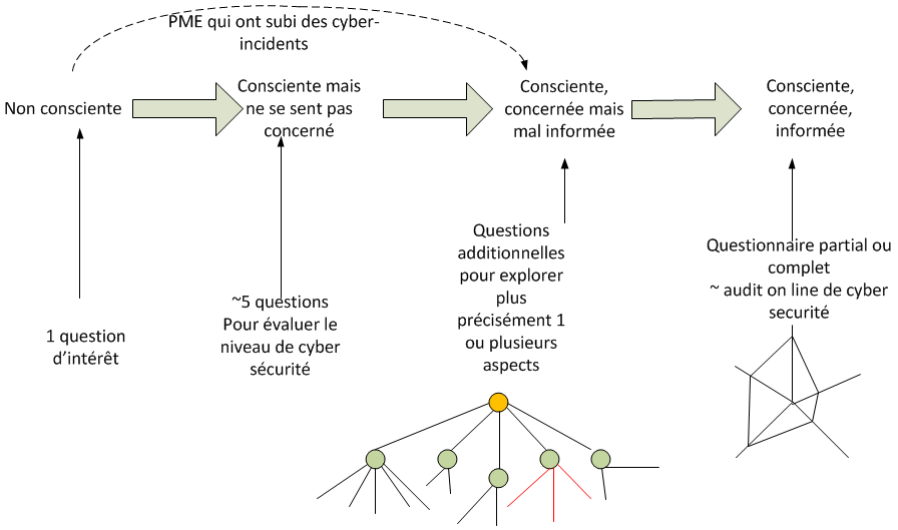

FIGURE 1 – Les niveaux de maturité relativement au cyber-risque

5.4.1 Processus progressif d'audit en ligne

Les entreprises ont un niveau de maturité relative à la sécurité qui est décrit figure 1.

On peut établir 4 classes, soit 4 niveaux, qu'il faut essayer de faire franchir par étape :

- Stade 0 : PME inconscientes du sujet : dans ce cas il faut procéder par une seule question du type : La sécurité informatique vous concerne, voulez-vous en savoir plus ? Pour ces entreprises des approches ludiques sont sans doute à envisager.
- Stade 1 : PME consciente mais qui ne se sent pas concernée : Dans ce cas il faut poser quelques questions de base (par ex. sur la protection des données). A ce niveau on peut détecter une ou plusieurs vulnérabilités potentielles. A ce niveau, on peut aussi adopter une démarche ludique par le biais d'un outil multimédia et d'un scénario de mise en situation dans lequel l'interrogé doit choisir entre plusieurs solutions.
- Stade 2 : PME consciente, concernée, mais pas ou peu informée : dans ce cas on explore plus systématiquement le ou les points de vulnérabilité détectés à l'état 1
- Stade 3 : PME consciente, concernée et informée : elle doit être capable de comprendre les questions et d'y répondre, c'est-à-dire de prendre du temps pour un audit en ligne qui lui permettra de situer son niveau de sécurité.

5.4.2 Processus d'audit in-situ

Ce cas concerne l'entreprise qui est au moins à l'étape 2.

- En réintroduisant le rôle du médiateur / auditeur qui formule les questions,

les explicite, interprète le contexte, recueille les réponses, les précise et remplit dans ce cas le questionnaire en ligne (à des fins statistiques)
- En proposant à l'entreprise de graduer son niveau de sécurité sur la totalité ou une partie des 11 points du référentiel ISO 27002. Ce qui n'empêche pas de le compléter et de l'adapter.

Dans ce cas le processus de relation avec l'entreprise PME n'est plus un processus automatisé en aveugle mais un processus de service de type audit. On pose 113 questions en présentiel (deux heures d'audit est insignifiant) ce qui permet de pouvoir expliciter les questions et de vérifier les réponses. L'outil en ligne ne sert qu'à enregistrer les réponses, les centralise à des fins statistiques, calcule un état de sécurité et le situe sur une échelle de référence, propose des points d'amélioration. Le processus est plus long (si on a des objectifs statistiques) mais il est plus avantageux et intéressant pour l'entreprise qui participe à son propre diagnostic et bénéficie d'une démarche pédagogique. Elle peut en effet découvrir des points de vulnérabilité qu'elle ignorait.

6 Conclusion

L'étude 2Centre a confirmé que les PME nécessitaient une approche adaptée à leur contexte (taille, âge, activité) d'autant plus grande que l'entreprise est petite. Il est à la fois nécessaire d'avoir une approche standardisée d'évaluation des risques et de leur perception afin d'échanger entre pays européens sur le sujet et en même temps, il faudrait adapter / compléter les standards existants qui ont été construit en ignorant que les PME n'ont pas de politique fonctionnelle, pas de politique de sécurité, faute de personnel dédié, de temps, de moyens. Il n'y a pas d'étude statistique crédible sur la perception du risque cyber par les PME. Sans remettre en cause l'intérêt de l'approche statistique nous pensons qu'il faut l'intégrer dans une démarche concrète de diagnostic et d'amélioration appliquée très tôt, auprès des entreprises volontaires qui leur permettent à moindre coût de se situer dans un référentiel de sécurité.
Le centre français F-CCENTRE devra continuer cette étude en choisissant un mode d'action adapté et en construisant l'outil pour alerter les PME, recueillir des données.

7 Références

SYMANTEC, *Global SMB Survey*, 2013
McAfee, *Small Business Security Survey*, 2013
National Small Business Administration (NSBA), *2013 Small Business Technology Survey*, 2013
CLUSIF, *Menaces informatiques et pratiques de sécurité*, rapport, 2012
ISO/IEC 27002 :2005, *Technologies de l'information, Techniques de sécurité, Systèmes de management de la sécurité de l'information, Exigences*, révisé en 2013
ISO/IEC 27002 :2005, *Information Technology, Security Techniques, Code of Practice for Information Security Management*, 2005