LES CYBERATTAQUES ET LEURS PRÉJUDICES SUR LES ENTREPRISES
QUANTIFICATION ET QUALIFICATION

PROJET DE RECHERCHE

IRT-SYSTEMX

Aller au-delà des idées reçues

Programme « Internet de Confiance »

POUR TOUT RENSEIGNEMENT CONCERNANT CE RAPPORT, VOUS POUVEZ CONTACTER L'IRT SYSTEMX AUX COORDONNÉES CI-DESSOUS :

IRT SystemX

8, avenue de la Vauve

CS 90070 – 91127 Palaiseau Cedex

Site internet : www.irt-systemx.fr

Courriel : gilles.desoblin@irt-systemx.fr (Directeur Programme « Internet de Confiance »)

VERSION	NOM	DATE	Modification
ISX-IC-Cyber-Risque-v1.4	Philippe LAURIER	19/09/2017	Version initiale

Corriger plusieurs « idées reçues » sur les attaques informatiques

- Le taux d'attaques réussies concernant les cryptovirus s'avère n'être pas faible : il dépasse nettement 1 % de victimes parmi les entreprises de moins de 50 employés, et par an.
- Le coût moyen constaté chez les victimes de cryptovirus reste actuellement peu élevé : il est pour une TPE d'un montant en milliers d'euros par attaque réussie.
- Le préjudice humain occasionné par ces attaques subit une habituelle sous-estimation très forte.
- Inversement, le préjudice sur l'image des entreprises touchées, souvent superficiel et passager, subit une fréquente surestimation.
- Quoique les relations entre entreprises partenaires se confirment être un des grands vecteurs d'attaque et de leurre, une part prépondérante de la fragilité provient non pas des donneurs d'ordre ou sous-traitants de la *supply chain*, mais de l'écosystème de toute entreprise constitué par les fournisseurs qui concourent à son bon fonctionnement quotidien (opérateurs télécoms, maintenance informatique, services tertiaires …).
- Les modèles économiques qui structurent l'offre assurantielle et le contenu des contrats d'assurance sont en décalage avec plusieurs attentes majeures constatées auprès des victimes, en ce qu'ils s'attachent à bien répondre à des besoins secondaires.
- Les attaques informatiques se prêtent mal à une assimilation aux modèles types d'évaluation des catastrophes naturelles ou encore des pandémies, mais appellent des modèles hybrides.
- L'addition des préjudices individuels ne livre pas spontanément le calcul du préjudice pour la collectivité.
- Rapporter le coût des attaques au PIB est de peu d'utilité.
- La centralisation de la collecte et la rediffusion d'informations sur les piratages n'atteint pas l'efficacité espérée, et trouvera un complément dans une gestion locale des crises au niveau de « micro-territoires ».
- L'offre des prestataires en sécurité informatique ne souffre pas tant d'un manque de vecteurs de mise en relation avec la demande, que d'une hétérogénéité excessive des compétences et d'une faible transparence sur le niveau réel de chaque prestataire.
- L'espoir d'une amélioration notable de la sécurité informatique est illusoire, s'agissant de systèmes d'information et de briques logicielles *fragiles par conception*.

Consacrée à des cas réels d'attaques informatiques, cette étude de terrain a pour objectif de mesurer les préjudices causés au tissu économique, puis d'élaborer des modèles de calcul de l'exposition d'une entreprise au risque ainsi que des coûts induits, dans la perspective d'aboutir à des grilles d'auto-évaluation simplifiées. Elle vise également à compléter les recommandations de protection usuelles, par des solutions et des bonnes pratiques observées chez ces récentes victimes. Un objectif parallèle est de collecter des *signaux faibles*, non mesurables en soi mais révélateurs de paramètres nouveaux.

Sur une durée d'un an, plus d'une cinquantaine de victimes ont été interviewées et rencontrées -pour la plupart des TPE/PME, mais aussi quelques associations loi 1901 et établissements publics. 90 % sont des structures de moins de 50 employés. Une accentuation volontaire a été faite sur le rançonnage par cryptovirus et les fraudes au président. Les autres catégories d'attaques étudiées étant : prise de contrôle de messagerie, piratage téléphonique, caméras mal protégées, défaçage, fraude aux sentiments, usurpation d'identité, captation de nom de domaine, attaque par déni de service.

Plusieurs idées reçues ont été infirmées par le présent travail de terrain, qui modifie la vision à porter sur le cyber-risque, à savoir l'image entretenue d'un type d'évènement en voie d'extension mais encore rare à ce jour, et au préjudice nécessairement élevé :

- Fréquence des attaques réussies concernant les cryptovirus : pour une entreprise de moins de cinquante employés, cette fréquence a quitté le niveau des évènements rares. Pour repère, rapporté au nombre total d'entreprises et d'associations en France, **un pourcentage de 1 % de victimes par an correspondra à 50 000 entités, chiffre aujourd'hui dépassé** (particuliers non inclus). La probabilité d'être ciblé et de faire l'objet de tentatives présente quant à elle peu d'intérêt puisqu'elle confine à la certitude, *a fortiori* quand on a déjà été victime donc remarqué par les pirates : une d'elle a observé suite à son premier piratage subi, une hausse des tentatives qu'elle a estimée chez elle de l'ordre de 400 %, durant une longue période. La plupart des témoignages confirment cette récurrence de nouvelles tentatives, y compris dans la régularité de son cadencement qui exprime une automatisation du mode opératoire. La probabilité d'occurrence des tentatives les inscrit dans le quasi-quotidien des petites entreprises, pour se hisser chez les grandes à des volumes par dizaines, centaines ou milliers qui attestent de leur « épandage » à grande échelle.

- **Le coût moyen constaté chez les victimes de cryptovirus s'avère être pour une TPE d'un montant en milliers d'euros par attaque réussie**. Il révèle ou précise trois autres caractéristiques :
    - La progression des coûts n'est pas proportionnée seulement à celle de la taille d'une entreprise, car elle subit des inflexions à la hausse ou à la baisse explicables grâce à quelques autres facteurs identifiés. Ces inflexions se retrouvent avec des courbures très similaires sur la quasi-totalité des cas étudiés, ce qui autorise une certaine formalisation.
    - La progression des coûts n'est pas linéaire avec le temps mais connaît des successions de hausses parfois brutales et de plateaux, explicables pour l'essentiel par le profil, le métier et le mode d'organisation interne de l'entreprise, donc à nouveau formalisables pour partie.
    - Concernant cette progressivité des coûts, les grandeurs et les seuils restent assez cohérents d'un cas à l'autre tant qu'ils restent circonscrits à des activités « de bureau » (paye, comptabilité, facturation …) ; toutefois enregistre-t-on un fréquent changement d'échelle et une plus grande disparité dès que des activités productives ou de conception sont touchées, en particulier avec des machines-outils ou des process industriels en continu.
      Thème clé n°1 pour le proche avenir : l'exposition de l'outil productif.

- Un grand nombre d'attaques réussies trouvent des solutions à faible prix, particulièrement quand les sauvegardes n'ont pas été affectées. **De ce fait, la *médiane* constatée est basse** (ainsi que le *mode*, au sens statistique) **et se situe nettement au-dessous de la *moyenne***.
  Thème clé n°2 pour le proche avenir : la fragilité de ces sauvegardes.

  Cette distribution des préjudices éclaire aussi le fait que ces chocs, parce qu'ils concentrent leurs déflagrations les plus violentes sur un nombre très minoritaire d'entreprises, y deviennent potentiellement mortels. Information utile pour caractériser les cyberattaques et raisonner en termes d'investissement préventif : celle qu'un entrepreneur subira demain a une probabilité majoritaire de rester bénigne –donc de ne pas réapparaître dans des statistiques publiques ou de compagnie d'assurance-, mais ne connaît pas de plafond espérable en matière de malignité, autre que le décès de sa société. Ce type d'exposition fait ressortir la coordination indispensable à terme entre les volets techniques, organisationnels et assuranciels d'une bonne sécurité des systèmes d'information de l'entreprise.

Deux enseignements jumeaux méritent une attention particulière, car ils traduisent la possibilité d'un basculement des rapports de force entre le bouclier et l'épée, vers une *nouvelle donne* soit dégradée soit améliorée :

- **Les dégâts constatés chez les victimes**, lorsqu'ils sont -par scénarisation- comparés à ceux qui auraient pu advenir, **montrent qu'un léger accroissement de « l'efficacité » de l'attaquant aurait souvent entraîné une hausse plus que proportionnée du préjudice**. Le volume de richesse supplémentaire aisément destructible est très élevé, parallèlement à l'existence de failles informatiques latentes excessivement nombreuses ; la coexistence de ces deux éléments ouvre des perspectives inquiétantes, qui appellent à dépasser le traditionnel discours salvateur via les seules mises à jour de systèmes, qui sont en réalité *fragiles par conception*.
- A contrario, **un léger accroissement de « l'efficacité » de la défense sur quelques points névralgiques, aurait entraîné une baisse plus que proportionnée des préjudices**. Ce potentiel d'amélioration est palpable à travers le fait que quantités de solutions techniques de sécurité à coût modéré voire quasi-nul, ne sont actuellement pas déployées au sein des entreprises (messageries inter-entreprises mieux cloisonnées et isolées, signatures électroniques et autres formes de marquage des flux, etc.).
  Thème clé n°3 : une mise à disposition de « boîte à outils » basiques de sécurité pour le tissu des TPE et PME.

Concernant les cryptovirus, l'addition des **coûts subis par l'ensemble des victimes de moins de cinquante employés - entreprises ou associations- aboutit en première estimation à un montant supérieur à 700 millions d'euros par an pour la France**. Pour rappel méthodologique, deux malentendus usuels ont été mis en relief lors de la comparaison de nos chiffrages avec d'autres sources :

- **Croire à tort que l'addition des préjudices individuels livrera spontanément le calcul du préjudice pour la collectivité**. Or, entre autres exemples, une part des clients d'une entreprise piratée reporteront tout ou partie de leurs achats sur d'autres fournisseurs ; le calcul doit s'attacher par conséquent aussi aux transferts de richesse – entre les victimes, les non victimes, les pirates, etc.- et raisonner en termes de flux financiers.
- **Rapporter le coût des attaques** à la « valeur ajoutée », donc **au PIB** pour le niveau national, **est de peu d'utilité**, autrement que pour des comparaisons dans le temps et dans l'espace. Nos conclusions proposent de rapporter préférentiellement les mesures d'impact à d'autres agrégats, notamment :
  - l'investissement productif, au niveau des entreprises aussi bien que de la collectivité (FBCF), beaucoup plus révélateurs du volume effectif d'emplois et de richesse détruits dans le temps ;
  - la trésorerie des entreprises, où se constatent des tensions rapides chez la plupart des petites entreprises. Ces petites sociétés subissent des difficultés d'accès à des ressources externes de secours et sont, de ce fait, très exposées à toute perduration de l'attaque ou de son impact.
    Thème clé n°4 : les moyens d'améliorer la capacité des TPE et PME à surmonter ces tensions temporaires sur leur trésorerie.

Dans cette observation des transferts de richesse, le gain enregistré par les pirates déroge à l'image communément admise. La sortie de capitaux de France, due conjointement aux cryptovirus et aux fraudes au président, qui apparaît dépasser 200 millions d'euros par an, masque des modèles économiques très différents entre ces deux formes de criminalité. Au sujet des cryptovirus, les calculs menés avec les sociétés rencontrées ont fait ressortir un **ratio entre argent rançonné (sommes effectivement versées aux pirates) et préjudice total pour l'ensemble des victimes de l'ordre de 1/25, chez les petites entreprises**. A contrario, les fraudes au président, malgré leur recours accentué à des acteurs humains et à l'ingénierie sociale, laisse entrevoir des marges finales nettement plus élevées pour l'assaillant.

Thème clé n°5 : l'anticipation de l'évolution de ces divers modèles économiques.

Au rang des représentations contredites par la présente étude, ressortent encore :

- Une habituelle **sous-estimation très forte du préjudice humain** occasionné par ces attaques. Cette dimension transparaît dans les nombreux cas de fragilisation des personnes ou de la cohésion des groupes. Elle est manifeste aussi à travers le besoin d'assister les décideurs d'une entreprise durant les heures, jours ou semaines que durera l'impact de l'attaque, période où ils sont amenés à prendre des décisions et mener des arbitrages en situation de forte incertitude.
  Thème clé n°6 : l'assistance en matière d'aide à la décision et à la gestion de crise.

- Une **surestimation du préjudice sur l'image des entreprises touchées, souvent superficiel et passage**r sur les cas observés.

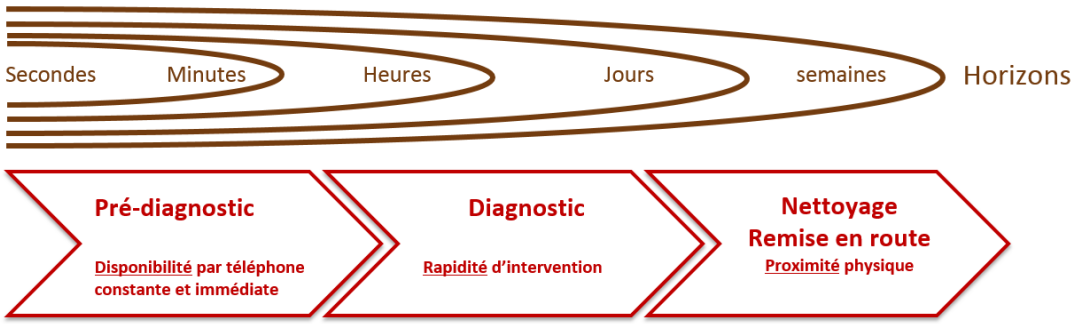
Ces points mènent à la prise en compte accrue de plusieurs facteurs :

- Le facteur humain, en tant que conséquence aussi bien que contributeur aux attaques réussies –ou à la gravité d'une attaque réussie-. Parmi les surprises rencontrées, **ni le niveau de compétence informatique ni l'âge moyen des employés ne semblent avoir d'influence prépondérante sur le niveau effectif de sécurité informatique d'une entreprise** ; inversement, **le taux de rotation des effectifs et la nature –notamment la précarité- des relations contractuelles avec les employés paraissent plus signifiants d'une situation de risque**.

- Le facteur temps, qui est apparu jouer directement sur le niveau d'impact. Avec une importance à accorder aux deux extrêmes du très court terme comme du long terme (deux profils d'entreprises se distinguent nettement, entre celles où le préjudice lors de l'attaque s'estompera avec le temps, et d'autres où il perdurera voire s'accentuera dans le temps, menant parfois à l'asphyxie de l'entreprise[1]).

- Le facteur géographique, où les **actuelles tendances à centraliser la collecte et la rediffusion d'information sur les piratages s'avèrent à rééquilibrer**. L'étude souligne une déperdition d'information élevée dans les deux sens, et l'utilité de **raisonner complémentairement autour de *micro-territoires*, couvrant quelques milliers d'entreprises** -éventuellement quelques dizaines de milliers-, chez lesquels la connaissance du contexte est un atout irremplaçable avant (prévention, sécurisation …), pendant et après tout évènement. Ces micro-territoires pouvant s'organiser autour de quelques acteurs locaux légitimés par leur proximité avec les entreprises et par leur capital confiance (selon le contexte : instances consulaires, associatives, socio-professionnelles, collectivités locales, etc.) ; de tels acteurs faisant guichet pour l'accueil puis l'accompagnement des entreprises victimes, et pouvant capitaliser les enseignements issus de chaque cas pour améliorer cet accompagnement.

Les modèles organisationnels doivent ainsi croiser les facteurs temps et espace. L'approche temporelle, rapportée aux coûts constatés, éclaire par ailleurs l'importance cruciale des premières minutes d'une attaque. L'expression de ces horizons sous forme de poupées gigognes rappelle cependant que chacun d'eux attend des types d'assistance qui lui sont propres et adaptés, entre centralisation et décentralisation, pour répondre aux besoins tantôt d'immédiateté tantôt de proximité du soutien.



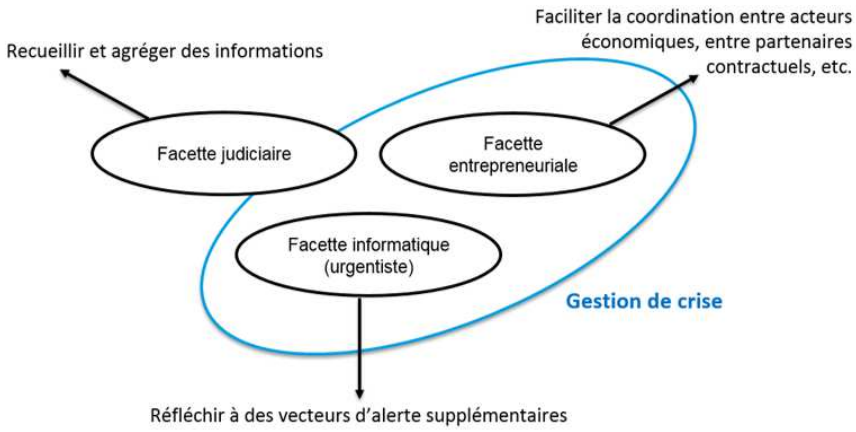
Parmi les autres constats, une imperfection des procédures employées se révèle sur deux volets :

- Les modèles économiques qui structurent l'offre assurantielle et le contenu des contrats d'assurance se montrent en décalage avec plusieurs attentes majeures constatées auprès des victimes. En particulier, les clauses de protection proposées, parce qu'elles ne sont pas suffisamment en phase avec le caractère potentiellement létal des attaques, contribuent certainement à la lenteur de la pénétration de ces offres auprès des entreprises.

[1] Les cas d'espionnage industriel relèvent fréquemment de cette seconde catégorie. Quoique peu recensés –car préalablement peu détectés- durant l'étude, on remarque en parallèle que le nombre élevé de cas de captation de mots de passe de messageries rend patentes de telles facilités d'interception ou de pénétration. Un effort reste à accomplir pour mieux mesurer et formaliser la part aujourd'hui invisible de ces vols d'informations sensibles.

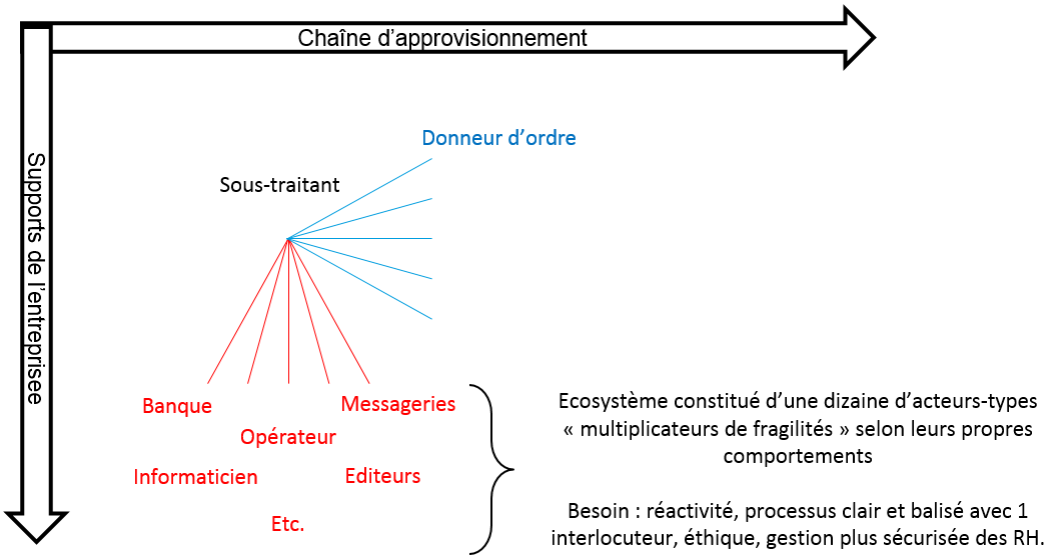
- Les requêtes ou questionnaires adressés aux entreprises en matière de cyberattaques, émanant d'autorités judiciaires, d'organismes statistiques, d'assureurs ou certificateurs, souffrent d'une profusion handicapante qui traduit aussi une relative méconnaissance des aspects véritablement prioritaires, lors du recueil d'informations.
  Thème clé n°7 : une rationalisation des procédures, recentrées sur l'information utile et fiable.

De même, nos actuels modes de gestion de crise en cas d'attaque sur une entreprise locale, pèchent par une faible articulation entre les trois facettes technique, judiciaire et entrepreneuriale.



Sur la facette informatique de cette gestion de crise, est à rapporter une situation très contreproductive : **une forte disparité du niveau des prestataires informatiques qui se déclarent compétents en sécurité**. Quoiqu'il s'agisse d'une « photographie » ponctuelle, un comparatif établi par une des entreprises victimes et en demande d'intervention, a établi qu'une seule des trois sociétés prestataires testées avait un niveau d'expertise satisfaisant. D'autres signalements ont confirmé cette hétérogénéité et le manque de transparence qui s'y attache, avec leur impact final sous forme d'insécurité ignorée. Ce problème d'affichage et de qualité –y compris la disponibilité et la réactivité en cas d'urgence- trouverait une part de réponse via les *micro-territoires* et leurs guichets d'orientation, mieux à même d'effectuer un pré-tri des ressources ayant des compétences réelles et une éthique.

Toujours sur cet aspect organisationnel, si **les relations entre entreprises partenaires se sont confirmées être un des grands vecteurs d'attaque et de leurre**, l'observation plus fouillée fait ressortir qu'une part très importante de cette vulnérabilité provient d'interlocuteurs qui ne participent pas à la transformation d'une matière première, à la fourniture d'un produit semi-fini ou d'un composant pour un produit final ; ce ne sont pas des fournisseurs au sens d'une chaîne logistique (« supply chain ») *stricto sensu*. Ce sont des acteurs de l'**écosystème** de toute entreprise, qui concourent à son bon fonctionnement quotidien : prestataire ou éditeur informatique, opérateur télécom, fournisseur de messagerie, expert-comptable mais aussi banquier (transferts financiers, ouvertures de compte …), etc. Ils forment un autre amont déconnecté du fait que l'entreprise victime fabrique des avions ou des plats cuisinés.



Il est apparu que les déficiences ou le manque de réactivité de nombreux acteurs de ces *écosystèmes supports* alimentent le présent problème dans des proportions au moins comparables à celles engendrées par les déficiences chez la victime elle-même :

En matière de cause : assez souvent sont-ils auteurs de fragilités et de failles donc d'une attaque ;

En matière de conséquences : très souvent sont-ils contributeurs d'une envolée des coûts consécutifs à une attaque, quelle qu'en soit l'origine.

Cet état de fait se décrira de deux manières :

- Intérieur/extérieur : à la question, pour une entreprise, de savoir si les principaux abaissements des dégâts en cas d'attaque seront gagnables à l'intérieur ou à l'extérieur, la balance penche fréquemment vers l'extérieur. D'autant que la tendance contemporaine à externaliser de nombreuses fonctions hors de l'entreprise déporte une part croissante de l'impératif de qualité et de sécurité vers l'extérieur.
- Amont/aval : une procédure inadéquate, laxiste ou fautive chez tel ou tel grand prestataire, partie prenante de l'écosystème de milliers ou millions d'entreprises, se voit démultipliée dans ses effets. Le même levier sera inversable, où chaque amélioration amont bénéficiera d'un effet multiplicateur en aval.

A gains de niveau équivalent en sécurité, l'évangélisation des petites entreprises afin qu'elles investissent dans la sécurité représente, dans son addition, des sommes infiniment plus lourdes que les frais à consentir chez certains de ces grands prestataires pour réduire la non-qualité, la non-réactivité voire le caractère insécure de leurs prestations. La disproportion des coûts/rentabilité entre ces deux niveaux d'intervention plaide pour accélérer en premier lieu celle sur cet environnement.

➔ La sécurité d'une entreprise se mesurera pour une part importante à la qualité de son environnement, autant qu'à ses pare-feu, antivirus ou autres outils et dispositifs internes.

Cette interdépendance particulière entre entreprises, avec ses effets démultiplicateurs, mène à remettre en cause les références habituelles aux types d'évènements déjà connus des assureurs, que sont les catastrophes naturelles ou encore les pandémies. Ajoutées à la présence du facteur humain pour sa survenance, et au caractère techniquement mutant de la

menace, les travaux engagés aboutissent à des modèles hybrides, mieux à même de séparer les mesures de l'ampleur de la cause, l'ampleur de sa diffusion et l'ampleur des conséquences.

Thème clé n°8 : élaborer des modèles mieux représentatifs du mode de propagation des attaques informatiques, pour en jauger le caractère potentiellement systémique.

De telles menaces ne sont pas « toute chose égale par ailleurs », puisque les réflexes contemporains de tout numériser, tout connecter, voire tout centraliser une fois numérisé & connecté, amplifient ces fragilités et ces interdépendances. Ces tendances débouchent sur des conséquences lourdes en termes d'exposition et de montant des préjudices. Des grilles d'analyse sont élaborées, afin de confronter objectivement les gains d'efficacité et les coûts collatéraux induits par ces tendances de fond.

Thème clé n°9 : évaluer en tendance les conséquences de la propension à numériser et connecter, au sein des entreprises ou entre entreprises, pour identifier des effets de seuil.

Thèmes clés

N°1 : l'atténuation de l'exposition de l'outil productif.

N°2 : la diminution de la fragilité des sauvegardes informatiques.

N°3 : une mise à disposition de « boîte à outils » basiques de sécurité pour le tissu des TPE et PME.

N°4 : l'amélioration de la capacité des TPE et PME à surmonter les tensions temporaires sur leur trésorerie, en cas d'attaque.

N°5 : l'anticipation de l'évolution des divers modèles économiques d'attaques informatiques.

N°6 : l'assistance en matière d'aide à la décision et à la gestion de crise, pour les entreprises victimes.

N°7 : une rationalisation des procédures d'enquête, recentrées sur l'information utile et fiable.

N°8 : l'élaboration de modèles de propagation des attaques informatiques, pour en jauger le caractère potentiellement systémique.

N°9 : l'évaluation en tendance des conséquences de la propension à numériser et connecter, au sein des entreprises ou entre entreprises, pour identifier des effets de seuil.