



Pourquoi infogérer la sécurité du système d'information ?

Impacts organisationnels
et managériaux.

Avant-propos	5
Introduction	6
Chiffres et tendances	7
Expériences de RSSI, DSI et experts	
Colonel Eric Freyssinet	8
Chef de la mission numérique - Gendarmerie Nationale	
Michel Juvin	10
Chief information security officer Club des experts de la sécurité de l'information et du numérique (Cesin)	
François Beaume	12
Administrateur - AMRAE	
Mahmoud Denfer	14
Chief information security officer - Groupe Vallourec	
Sandro Lancrin	16
Responsable de la sécurité des systèmes d'information Radio France	
Didier Pawlak	18
Directeur des systèmes d'information - Pénélope	
Philippe Caille	20
Chief security officer - Laboratoires Pierre Fabre	
Benjamin Guiroy	22
Responsable de la sécurité des systèmes d'information Groupe Labeyrie Fine Foods	
Mathieu Rigotto	24
Directeur du Pôle Cybersécurité - IMS Networks	



” La résilience passe par des réactions plus rapides, agiles et transversales ”

Dans le contexte actuel, il n'a jamais été plus facile d'attirer l'attention des décideurs sur les sujets relatifs à la cybersécurité. Pour autant la prise de conscience ne suffit pas face à un changement de paradigme de la sécurité des systèmes d'information et de l'environnement digital qui est le nôtre. Protéger nos entreprises, nos organisations, est devenu plus complexe et demande la prise en compte d'une gestion du risque en se départissant de vieux travers qui ont donné, pendant des années, l'image aux responsables de la sécurité d'être rangés comme simples experts techniques voire empêcheurs de tourner en rond de leur organisation.

L'image qui se dégage progressivement d'un contexte de cyberattaques permanentes, c'est que la résilience des entreprises passe par une capacité de réaction beaucoup plus rapide, agile, transversale... Les dirigeants sont convaincus qu'il s'agit là des caractéristiques clés de la transformation digitale de leur organisation. Il en va de même pour la transformation de leur sécurité.

Et quand on aborde ces sujets, la question qui revient souvent est : avec qui est-il possible d'atteindre ces

objectifs de façon réaliste ? L'externalisation a pris une place prépondérante dans les visions qu'ont les entreprises de leur système d'information, mais subsiste souvent l'interrogation sur la capacité à être agile et efficient, quand on fait appel à un tiers. En matière de sécurité pourtant, certains le font au quotidien. Des entreprises de toutes tailles s'appuient sur des partenaires de confiance pour augmenter drastiquement la qualité de leur supervision et de leur réponse à incident, accéder à de l'expertise mutualisée et partager les risques. Le témoignage sur leurs expériences, la mise en avant de leurs spécificités et de leurs opinions, nous paraît aujourd'hui plus important que jamais.

En vous souhaitant une bonne lecture.



Thierry Bardy
Président d'IMS Networks

" Capitaliser sur la force des écosystèmes "

Il ne se passe désormais plus une semaine sans que des attaques et incidents de sécurité numérique soient largement médiatisés, y compris auprès du grand public. Au-delà de la gravité de ces événements et de la prise de conscience qu'ils peuvent provoquer, cette accélération contribue surtout à démontrer que la cybersécurité n'est plus (seulement) un sujet de technologies et d'outils, mais bien un enjeu culturel, organisationnel et managérial.

En ce sens, les entreprises font face à de plus en plus de choix complexes. En effet, elles sont clairement confrontées à une pénurie de ressources, avec notamment une difficulté à recruter efficacement sur ces sujets. D'autant plus que la variété et l'évolutivité nécessaires des compétences en la matière sont telles, que se tenir à jour est un enjeu à part entière pour les équipes en place. Celles-ci sont mises sous pression par l'exigence « 24/7 » d'un grand nombre de leurs missions ; une vigilance constante difficile à tenir pour de nombreuses organisations qui ne sont pas pensées à l'origine pour de telles contraintes. Et les évolutions réglementaires ne font que rendre ces problématiques plus aiguës. Si le RGPD est aujourd'hui sur toutes les langues du fait de son entrée en application en mai 2018, ses impacts organisationnels et managériaux sont encore loin d'être maîtrisés par tous.

Dans ce contexte, le souci légitime d'assurer la continuité de leur activité pousse les dirigeants à faire jouer tous les avantages qu'ils ont à disposition. L'externalisation d'une partie opérationnelle de la sécurité des systèmes d'information est donc bien souvent considérée avec attention. Celle du SOC notamment, pose aux entreprises de nombreuses questions. Loin d'être seulement un sujet pour les Opérateurs d'Importance Vitale, suivi de près par l'Anssi, la question se pose aujourd'hui à toute entreprise. « L'externalisation est un must have » résume de façon explicite Mahmoud Denfer, CISO Group de l'industriel Vallourec (*voir interview p.14*).

Plus qu'un choix tactique efficace cependant, cette démarche d'externalisation met en valeur la force des écosystèmes qui apprennent à se défendre conjointement, plutôt que d'être isolés face aux menaces. « Vu le contexte global aujourd'hui, la priorité pour les entreprises est de devenir " plus fortes ensemble " » reconnaît ainsi Michel Juvin, CISO dans une grande entreprise du secteur du luxe (*voir interview p.10*). Mutualisation, proximité, liens forts entre les organisations et entre les individus... le champ lexical qu'utilisent les acteurs qui témoignent dans ce recueil est celui de la communauté, sous ses aspects les plus protecteurs. Un discours qui a le mérite de trancher de manière constructive avec les messages de peur qui paralysent encore trop l'action des entreprises.

**Pour télécharger l'intégralité de ce carnet d'expérience,
et lire les interviews des 9 responsables de sécurité qui partagent
leurs visions et expériences sur l'externalisation du SI,
rendez-vous sur cette page :**

<http://experiences.alliancy.fr/landing/experiences-infogerance-securite/>



Les carnets « Expériences Transformation » du magazine Alliancy

La transformation numérique est sur toutes les lèvres. La question n'est plus « Pour quoi faire ? » mais « Comment et avec qui ? ». Alliancy a souhaité y répondre à travers la collection « Expériences transformation ». Des carnets thématiques qui facilitent le partage d'expériences concrètes. Retrouvez l'ensemble de la collection sur experiences.alliancy.fr.

D'un secteur à l'autre, d'un métier à l'autre, vous découvrirez dans cette collection des témoignages, des idées, des stratégies ou des bonnes pratiques de professionnels qui, au jour le jour, font bouger les lignes dans leur entreprise.

Stratégies, organisation et management, place de la data, nouveaux écosystèmes IOT, importance de la sécurité, gouvernance du SI... Alliancy est un magazine engagé en faveur du « travailler ensemble pour innover plus vite » et interroge les leviers de la transformation numérique pour qu'ils s'invitent peu à peu dans votre quotidien. alliancy.fr