VIROLE CONSEIL FORMATION
3 allée des tilleuls
92410 Ville dôAvray
denis@viroleconseil.fr

Protection de lôinformation et Sécurité Système dôinformation,

quelles sont les vertus dôune sensibilisation bien organisée

« Des acteurs non sensibilisés aux risques liés à lôusage des technologies de lôinformation et de la communication et non formés aux bonnes pratiques représentent une source majeure de vulnérabilité des systèmes dôinformation ».

Cette célèbre citation du Député Pierre Labordes, issue de la première recommandation de son rapport sur : « La sécurité des systèmes dôinformation, un enjeu majeur pour la France », rappelée dans le rapport d'information n° 449 (2007-2008) de M. Roger Romani, fait au nom de la commission des affaires étrangères, déposé le 8 juillet 2008, reste toujours dôactualité en 2015.

Les premiers axes de recommandation sont bien de sensibiliser, informer, responsabiliser, former les acteurs du Patrimoine Informationnel, utilisateurs du Système dôinformation. Ces recommandations formulées par le biais de règles fonctionnelles sont rappelées dans la nouvelle Politique Sécurité Système dôinformation de lôEtat du 17 juillet 2014.

Avant de définir les objectifs de la sensibilisation, responsabilisation, formation Sécurité Système dôinformation, il est nécessaire de formaliser le périmètre.

Aussi, pour être cohérent et plein de bon sens, la Sécurité Système dôinformation ne peut se réduire à la sécurité informatique ni même à la Sécurité des systèmes automatisés de lôinformation. Lôobjectif est bien la protection du Patrimoine informationnel (protection des informations sous quelque forme que ce soit, des processus qui les manipulent, des ressources qui les supportent et des acteurs qui les utilisent), afin de garantir le bon fonctionnement des missions et activités dans le respect des valeurs essentielles de lôentité.

Ces valeurs, qui devront être formalisées avec la Direction Générale, sont classiquement :

- la capacité à remplir sa mission et à fournir les différents services,
- la confiance des usagers ou des clients,
- la sécurité financière, le respect des intérêts des actionnaires,
- la responsabilité juridique,
- le respect des cultures et souverainetés des pays dans lesquels lôentité est implantée,
- lôengagement du respect déontologique des intérêts légitimes et justifiés des partenaires ou fournisseurs, la conformité aux standards, lôimage de lôentité à lôextérieur, le climat de confiance et social en interne,
- la protection des biens et des personnes,
- la protection environnementale (ces deux dernières concernant plus particulièrement les industriels), é

VIROLE CONSEIL FORMATION
3 allée des tilleuls
92410 Ville d'Avray
denis@viroleconseil.fr

- la protection du patrimoine historique et culturel de l'entité,
- é

La sensibilisation devra mettre en avant avec un maximum de recul et d'effort de modélisation, illustrée d'un grand nombre d'exemples concrets professionnels ou privés, qu'un incident (erreur, panne, malveillance) peut entrainer un dommage en Disponibilité, Confidentialité, Intégrité et Traçabilité et par conséquent une altération aux valeurs essentielles.

La technologie est donc nécessaire mais insuffisante. L'engagement de responsabilité individuel et collectif à respecter les règles est donc majeur pour la bonne réussite du projet sécurité.

La bonne formalisation du périmètre est fondamentale pour la définition des règles et bonnes pratiques comportementales (connaissance et savoir pouvant être transmis sous une forme orale, manipulation des documents papier et des outils classiques associés, manipulation des fichiers électroniques et des outils les supportant, utilisation d'extraits de produits industriels porteurs d'informations).

Ce patrimoine informationnel comprend les informations (professionnelles, administratives dont les données à caractère personnel, économiques, commerciales, techniques voire scientifiques dont l'entité est propriétaire ainsi que celles qui lui ont été remises par des tiers clients, partenaires et/ou fournisseurs).

La protection de l'information dans les entités s'est faite en plusieurs temps.

La première approche a consisté à installer des outils de protection additionnels sur les infrastructures techniques et applicatives. Ces outils aujourd'hui s'avèrent être suffisants, en effet comme dans tous les domaines de la sécurité, le facteur humain reste fondamental.

Le deuxième temps, concerne la sensibilisation, ressentie par tous les experts comme nécessaire voire incontournable, formalisée comme une exigence par toutes les normes de sécurité, et présentée comme obligatoire par le Code du travail, un employeur ne pouvant sanctionner un collaborateur pour le non-respect d'une règle si elle n'a pas été expliquée au préalable, les contrôles possibles devant être aussi présentés aux collaborateurs.

La sensibilisation doit donc permettre aux acteurs concernés d'engager leurs responsabilités dans le respect des bonnes pratiques.

Cette sensibilisation va reposer sur deux idées complémentaires.

1. **L'idée de base, reprise des environnements industriels (et pas toujours applicable dans certaines cultures d'entreprise ou d'administrations) est d'organiser une sensibilisation formation identique pour tous, obligatoire et récurrente (puisque les obligations légales, les menaces et les risques et donc les règles peuvent évoluer), tous profils mélangés.**

VIROLE CONSEIL FORMATION
3 allée des tilleuls
92410 Ville dôAvray
denis@viroleconseil.fr

Lôobjectif de ce « tronc commun » est donc dôêtre extrêmement clair : la sécurité repose sur non seulement le bon sens et la cohérence, mais elle nécessite avant tout un engagement de responsabilité de tous dans le respect dôune organisation, des procédures, règles, directives et lois.

Cette formation identique pour tous (comprenant bien sûr les sous-traitants) permet, de plus, aux Directions représentantes de la personne morale de lôentité, de démontrer la mise en place de moyens de protection techniques mais aussi organisationnels dans le respect de leurs obligations de moyens de sécurisation. En effet, en cas de dommages et/ou de plaintes, le non respect de ces obligations de moyens peut entraîner la condamnation civile ou pénale de la Personne Juridiquement Responsable, représentante délégataire de la Personne Morale.

Cette sensibilisation, analogue à un véritable permis de conduire, doit seulement informer sur les objectifs et les règles, mais aussi sur lôorganisation mise en place, les rôles des correspondants de sécurité qui doivent assister les utilisateurs.

A lôissue de cette formation de base chacun doit avoir une connaissance claire :

- Des obligations « disciplinaires » ou contractuelles, liées aux règlements et/ou statuts, les responsabilités civiles et pénales (CNIL, propriété intellectuelle, secret des correspondances, lutte contre la fraude, utilisation de la cryptographie, signature électronique, devoirs dôenregistrement de traces, é). Chacun a bien le devoir de respecter les lois, lôentité se trouvant dans le devoir de les rappeler.
- Des niveaux de classification des enjeux de disponibilité, intégrité, confidentialité et preuve.
- Qui doit classer, quoi, pour qui, comment, pour quelle durée ?

Ce chapitre est absolument majeur, côest lui qui permettra lôadhésion des métiers à la démarche et au respect des règles : Lôutilisateur comprendra quôil est le seul (sous la responsabilité de son manager) à être qualifié, compétent et légitime pour formaliser la sensibilité et les besoins des informations manipulées dans son activité, les règles et bonnes pratiques étant corrélées et consécutives à ces besoins. Les équipes techniques et sécurité ne peuvent avoir cette qualification et cette légitimité. Par contre elles sont bien évidemment compétentes pour définir les règles relatives aux besoins exprimés par les métiers.

- La formalisation des menaces et des risques permettra de bien démontrer que le non respect des lois, méthodes, procédures ou règles, (et ceci malgré la maturité des outils additionnels de protection), augmente considérablement la potentialité et les impacts de ces risques.
- Des règles concernant les comportements généraux à lôintérieur et à lôextérieur des établissements, les pratiques de manipulation des documents papier (en phases de conception et reproduction, dôéchanges et communication, dôarchivage et stockage et bien sûr de destruction), lôutilisation des

VIROLE CONSEIL FORMATION
3 allée des tilleuls
92410 Ville d'Avray
denis@viroleconseil.fr

outils informatiques (serveurs internes ou publics de type « en nuage » et stations) en phase de conception, d'installation et maintenance, d'échanges et communications, sauvegardes, archivages, stockages et éventuellement de destruction.

La connaissance et le respect de ces bonnes pratiques permettront de, non seulement limiter les erreurs mais aussi, de limiter les potentialités et les impacts de tous les risques.

Les difficultés classiques sont d'ordre psychologique et/ou culturel. La culture latine dont la France est un archétype réagit souvent spontanément et avec franchise, dans un esprit un peu frondeur. Le travail du pédagogue sera de bien montrer que les règles ont toujours été formalisées de manière relative à un contexte et à un enjeu et que le non respect de ces règles aura une conséquence directe opérationnelle.

Une autre réaction classique concerne les collaborateurs à forte valeur ajoutée. Ils risquent de ressentir ces règles comme une marque de défiance et ne comprennent pas, vu leurs expertises métier, toutes ces «contraintes ». Tout le travail du sensibilisateur sera de faire comprendre (qu'ils soient dans la maîtrise d'ouvrage ou dans la maîtrise d'œuvre), que ces règles sont en fait des exigences, que la maîtrise de leur environnement ne peut leur permettre de connaître toutes les menaces, toutes les vulnérabilités et donc tous les risques.

2. La deuxième idée complémentaire des formations responsabilisation doit répondre aux besoins spécifiques des différents profils et /ou métiers.

2.1. **Le premier besoin à prendre en compte est bien sûr la formation des Directions et responsables hiérarchiques.** Un des plus grands risques identifiés dans la mise en œuvre d'une politique de sécurité est de sous-impliquer les managers. Ils doivent comprendre leur rôle de garant de la mise en place des moyens et formaliser une organisation basée sur :

- La séparation des pouvoirs et devoirs, (il n'est pas acceptable à terme, dans une organisation mâture, qu'une même personne ou service se trouve dans la situation d'exprimer un besoin, de concevoir la réponse ou la solution à ce besoin et de contrôler la bonne application des procédures de sécurité),
- Une voie fonctionnelle de sécurité, « canal » fonctionnel complémentaire à la voie hiérarchique. Le double objectif sera de faciliter les remontées d'incident sans qu'ils ne soient ressentis comme culpabilisants, avant que ces incidents ne se transforment en crise et de faciliter les demandes d'arbitrage. En effet l'essentiel du besoin est bien là. Les Directions devront, après avoir compris

VIROLE CONSEIL FORMATION
3 allée des tilleuls
92410 Ville dôAvray
denis@viroleconseil.fr

comment assumer leurs responsabilités juridiques et comment faire appliquer les règles, identifier ces besoins dôarbitrage.

- Les plans dôaction de suivi, contrôle et audit avec les équipes internes ou sous-traitantes.

Il faut noter quôà ces objectifs des formations managers se rajoute la gestion des collaborateurs dans le contexte de la Sécurité des Systèmes dôInformation : Il est nécessaire de rappeler aux managers que la gestion des collaborateurs et sous-traitants nécessite aussi le respect de règles (disciplinaires, contractuelles, gestion des collaborateurs stratégiques et/ou affectés à des tâches sensibles).

Pour synthétiser, cette sensibilisation pour Directions doit leur donner les éléments nécessaires pour protéger non seulement les informations et ressources associées mais aussi pour assumer leurs responsabilités (juridiques civiles ou pénales et managériales) dans le cadre du Patrimoine informationnel.

2.2. Le deuxième besoin fondamental est donc dôexpliquer aux maitrises dôouvrage que la sécurité identique pour tous, (avec ses solutions de bon sens auto-justifiées et qui ne nécessitaient pas ou peu dôarbitrage,) a atteint ses limites et quôelle doit donc être adaptée et cohérente aux besoins spécifiques de chaque métier. Lôapproche dôautrefois qui consistait à rajouter des outils de sécurisation, certes nécessaires, sur des applications où la dimension sécurité nôétait pas prise en compte de manière native, (puisque les maîtrises dôouvrage ne formalisaient pas leurs besoins spécifiques de sécurité) ne peut plus répondre aux besoins et exigences spécifiques de chaque activité dans lôentité. Il faut donc, par ces formations sensibilisation, faciliter la relation « sécurité » maîtrise dôouvrage ï maîtrise dôô uvre :

- Comment intégrer la dimension sécurité dés la phase dôexpression de besoins ?
- Comment prendre en compte les exigences, menaces et risques spécifiques à chaque métier ?
- Comment participer à lôidentification des vulnérabilités ?
- Comment comprendre les objectifs de sécurité ?
- Comment déclencher les fonctions dôarbitrage si nécessaire ?
- Comment prendre en compte les besoins stratégiques, grader les besoins de plans de secours ?é
- Comment gérer la validation des risques résiduels par les directions voire homologation du SI ?

2.3. **Le troisième besoin complémentaire va être de donner aux maitrises dôô uvre** en charge des projets les éléments pour répondre aux besoins formalisés et arbitrés des maîtrises dôouvrage. Plus lôentité est mature plus cette relation est formalisée et structurée dans le cadre de la gestion de projet. Les maîtrises dôô uvre devront, grâce à ces formations sensibilisation, acquérir des méthodes structurées dôacquisition des besoins puis les règles de protection aussi bien pendant la vie du projet que pendant les cycles de fonctionnement des architectures cibles.

VIROLE CONSEIL FORMATION
3 allée des tilleuls
92410 Ville dôAvray
denis@viroleconseil.fr

2.4. **Un quatrième besoin pédagogique est bien sur dôexpliquer les règles spécifiques des assistantes de Direction.** De par leur rôle, les assistantes sont des éléments majeurs de la bonne protection de lôinformation. Elles sont des cibles de prédilection des agresseurs qui pratiquent lôingénierie sociale (lôincitation psychologique à dire, à faire, à se connecter, à détruire, à répéter, é), base de toute attaque, quôelle soit motivée par des raisons ludiques, cupides (cybercriminalité ou espionnage industriel) ou autres. Ces agresseurs ont très bien compris que les assistantes étaient au centre de la circulation de lôinformation, quôelles nôetaient pas toujours conscientes de la sensibilité des informations et quôelles constituaient un des vecteurs de récupération dôinformations exploitables (téléphone, mails, etc.), pour réaliser une attaque.

2.5. **Le cinquième besoin concerne plus particulièrement les acheteurs** qui émettent des appels dôoffre et gèrent les réponses par le biais dôinternet et de la dématérialisation des échanges. Il faudra ici identifier les exigences légales spécifiques et les bonnes pratiques en cohérence avec les outils disponibles.

2.6. **Le sixième besoin concerne les administrateurs de système dôinformation.** Il est majeur de les informer quôils nôutilisent leurs comptes privilégiés que pour les activités et besoins directement liés aux tâches dôadministration, dôexploitation ou dôassistance dont ils ont la charge, étant donné que toute action sur les systèmes dôinformation peut faire lôobjet dôune journalisation permettant leur imputabilité. Les administrateurs sont tenus au secret professionnel et, plus généralement, à une obligation de discrétion professionnelle qui leur interdit de divulguer les informations quôils auraient été amenés à connaitre dans lôexercice de leurs fonctions, notamment :

- Les informations couvertes par le secret des correspondances,
- relevant de la vie privée.

Les conditions dôintervention des administrateurs réseaux doivent être portées à la connaissance des employés et des organes représentatifs du personnel, par exemple :

- Lôutilisateur doit être informé au préalable de la finalité du contrôle.
- Le contrôle doit être conforme au principe de proportionnalité et respectueux du principe de finalité énoncé par la loi informatique et libertés.

Pour conclure il est bien clair que ces formations /sensibilisations devront toujours être adaptées aux spécificités et contexte de chaque entité, en cohérence avec les politiques et stratégies de chaque organisation et culture.

VIROLE CONSEIL FORMATION
3 allée des tilleuls
92410 Ville dôAvray
denis@viroleconseil.fr

Lôidée générale, encore une fois, est la prise en compte du facteur humain, complément majeur de la technologie où le sensibilisateur devra faire passer deux idées :

- **La nécessité dôun double engagement de responsabilité, celui de la personne morale de lôentité, de son délégataire et dôautre part celui de lôutilisateur et à tous les niveaux**
- **Le seul moyen de travailler de manière sereine et dôutiliser les composants informationnels (dans la sphère professionnelle et /ou privée), en dehors de toute paranoïa éventuelle est bien de connaître les valeurs des informations à manipuler, les risques potentiels, les dommages possibles mais surtout les bonnes pratiques à respecter.**

Denis VIROLE

denis@viroleconseil.fr