Sensibilisation des organismes financiers à la sécurité de l'information

Novembre | 08

enisa
European Network and Information Security Agency

À propos de l'ENISA

L'Agence européenne chargée de la sécurité des réseaux et de l'information (ENISA) est une agence de l'Union européenne créée en vue de promouvoir le fonctionnement du marché intérieur. Centre d'excellence pour les États membres et les institutions européennes en matière de sécurité des réseaux et de l'information, l'ENISA dispense des avis et des recommandations et intervient en tant que pôle d'information pour les bonnes pratiques. Par ailleurs, l'agence facilite aussi les contacts entre les institutions européennes, les États membres, le monde des affaires et de l'industrie.

Coordonnées:

Pour prendre contact avec l'ENISA ou pour toutes demandes générales concernant la sensibilisation à la sécurité de l'information:

E-mail: Isabella Santa, experte de haut niveau en sensibilisation — awareness@enisa.europa.eu

Internet: http://www.enisa.europa.eu/

Sensibilisation des organismes financiers à la sécurité de l'information

Novembre 2008

Remerciements

Plusieurs parties ont soutenu et ont contribué, directement ou indirectement, à cet ouvrage et ce, de différentes façons. Parmi les informations figurent des contributions de membres du groupe de travail virtuel (GTV) de l'ENISA sur «Comment organiser des campagnes de sensibilisation dans les organismes financiers». Le GTV et ses membres font partie de l'Awareness Raising Community de l'ENISA.

L'ENISA voudrait mentionner et remercier M. Thomas Schlienger, dont le soutien et la coopération initiaux ont influencé certains aspects clés du présent projet, les membres du GTV et leurs organisations, M^me^ Kate Dodds de Sai Global, M. Mathieu Gorge de VigiTrust, M. Jorge Pinto de Banco Credibom, M. Thomas Schlienger de TreeSolution Consulting GmbH, M^me^ Paula Davids de Sai Global, M^me^ Sissel Thomassen d'InfoSecure, M. Stefan K. Burau de Clariden Leu pour leur aide rapide, leur contribution précieuse et les données qu'ils ont fournies pour l'élaboration de cette publication.

Enfin, l'auteur voudrait remercier M^me^ Kate Dodds de Sai Global, M^me^ Colette Hanley de Betfair, M^me^ Isabel Milu de Banco Credibom, M. Luke O'Connor de Zurich Financial Services, M^me^ Tone Thingbø de la Norges Bank, qui ont contribué à cette publication par leurs analyses et leurs précieuses contributions, observations et suggestions. Le contenu de ce document aurait été incomplet et incorrect sans leur aide.

TABLE DES MATIÈRES

Résumé analytique

Le présent rapport est destiné aux décideurs et au personnel impliqué dans l'élaboration de programmes de sensibilisation à la sécurité de l'information au sein des organismes financiers, un secteur de plus en plus menacé par les failles de sécurité de l'information. Les pertes moyennes occasionnées par les vols d'informations sur la clientèle sont en augmentation, tout comme les frais engagés pour réagir aux incidents de sécurité. Non seulement les violations de la sécurité dans les organismes financiers portent préjudice à leur réputation, mais elles entraînent aussi de lourdes pertes financières dont il peut être difficile de se remettre.

Selon le rapport 2008 de l'autorité des services financiers britanniques (FSA, *Financial Services Authority*), les entreprises de services financiers pourraient améliorer de manière significative leurs contrôles afin d'éviter la perte ou le vol de données. De plus, les employés sont aujourd'hui considérés comme la cause numéro un d'incidents de sécurité, comme le confirment bon nombre d'enquêtes internationales, dont le sondage *Global State of Security* 2007 et l'enquête BERR 2008. Les solutions techniques ne sont désormais plus la panacée qu'elles ont pu être par le passé. Les efforts déployés pour minimiser les risques de sécurité liés au facteur humain sont de plus en plus conséquents et représentent un engagement financier important pour n'importe quel organisme.

La présente publication vise à expliquer l'importance de la sensibilisation à la sécurité de l'information au sein des organismes financiers, à analyser l'environnement et les facteurs commerciaux susceptibles d'influer sur ces programmes et à proposer un cadre de communication permettant de mieux organiser les initiatives de sensibilisation. Des études de cas et des recommandations sont proposées comme point de départ aux professionnels et aux équipes de sensibilisation.

La première partie du rapport consiste en une analyse de l'environnement des organismes financiers et de leurs principaux facteurs commerciaux. Dans ce type d'environnement, la sensibilisation à la sécurité de l'information doit prendre en considération les exigences de conformité et de sécurité fixées par les autorités législatives ou sectorielles. L'organisation d'initiatives de sensibilisation à la sécurité de l'information est une activité extrêmement difficile, mais qui, en même temps, garantit la continuité des affaires et la récupération en cas de catastrophe dans un milieu opérationnel aussi exigeant. En effet, dans ce type d'activité, les flux de données, qui nécessitent un niveau élevé de protection, ne peuvent ni être arrêtés, ni être réduits, même pour une courte période de temps.

Cette publication a donc pour but de fournir un panorama des normes internationales, des législations fondamentales actuellement en vigueur et des objectifs de certification, tout en dressant un bilan des grands risques, des menaces et des comportements des utilisateurs finals en matière de sécurité de l'information. Plusieurs paramètres définissent la stratégie de sensibilisation à adopter, parallèlement à ceux mentionnés ci-dessus, comme par exemple la segmentation du public, les rôles et les fonctions exercés, la situation géographique, le multiculturalisme, etc.

La seconde partie traitera des différentes phases de mise en œuvre des programmes de sensibilisation dans les organismes financiers ainsi que de l'évaluation des résultats. Afin de garantir que la sensibilisation à la sécurité de l'information corresponde aux objectifs d'une institution financière, elle devra être un processus continu en perpétuelle évolution. Les facteurs à prendre en considération lors des phases de planification, de conception et de mise en œuvre sont présentés dans ce chapitre, ainsi que les instruments de mesure de la réussite des initiatives de sensibilisation.

La troisième partie se compose de conseils pratiques, de recommandations et d'études de cas proposés par un certain nombre d'organismes privés.

L'ENISA espère que cette publication constituera un outil précieux pour les organismes financiers qui leur permettra de mieux comprendre l'importance d'une perte de données et de préparer et de mettre en œuvre des programmes de formation et de sensibilisation. Sensibiliser à la sécurité de l'information représente en soi un défi majeur pour n'importe quelle entreprise et sensibiliser ce secteur industriel particulier est une première étape importante pour relever ce défi.

PARTIE 1: ENVIRONNEMENT COMMERCIAL ET GRANDS FACTEURS

Introduction

Les gouvernements et législateurs ont tenté de répondre aux menaces pesant sur la sécurité de l'information en mettant en œuvre une série d'instruments législatifs et règlementaires, tels que les lois sur la protection des données à caractère privé, les lois sur l'usage impropre de l'informatique, la loi Sarbanes Oxley, etc.

Ne pas utiliser et protéger de manière adéquate les biens d'information d'un organisme peut constituer une violation d'une ou plusieurs de ces lois et peut aussi entraîner une publicité négative due à l'usage impropre des informations ou des ressources, pouvant éventuellement supposer également une perte de clientèle et de confiance des actionnaires. Les sanctions sont de plus en plus sévères et diversifiées: par exemple, les amendes au titre de la loi Sarbanes Oxley peuvent se monter jusqu'à 15 millions de dollars et s'accompagner de poursuites contre les dirigeants de la société et les normes de Bâle II peuvent donner lieu à un durcissement des exigences en matière d'adéquation des fonds propres, avec de sérieuses conséquences sur la rentabilité.

En pratique, la plupart des risques de sécurité dérivent d'un manque de connaissances bien définies et gérées en matière de sécurité de l'information. Les erreurs et les violations sont en effet souvent attribuables à des erreurs humaines et à un non-respect des procédures. Le *Department for Business, Enterprise and Regulatory Reform* britannique (BERR) indiquait dans son enquête 2008 sur les violations de la sécurité de l'information que dans 47 % des grandes entreprises du Royaume-Uni, le personnel n'utilisait pas correctement les systèmes d'information([1]).

Les chiffres sont sans appel: les pertes moyennes résultant d'un vol d'informations protégées par un droit de propriété sont en augmentation, tout comme les coûts exposés pour répondre aux incidents de sécurité. L'enquête BERR 2008 a indiqué que 77 % des entreprises britanniques consacraient leur budget pour la sécurité de l'information à la protection des informations sur la clientèle, tandis que 72 % privilégiaient le maintien de l'intégrité des informations. Le coût total moyen du plus grave incident connu par une entreprise britannique se situe entre 10 000 et 20 000 GBP, avec des pertes financières directes (perte de biens, amendes, etc.) chiffrées entre 500 et 1 000 GBP.

En 2007, la division Stratégie et renseignement sur la criminalité financière (FCID) de l'Autorité britannique des services financiers a traité 187 affaires de criminalité financière, dont 56 impliquaient une perte de données. En raison de la nature de leurs activités, les organismes financiers qui gèrent mal la sécurité de leurs données s'exposent à des risques conséquents. Ils détiennent en effet généralement de gros volumes de données personnelles et financières sur leurs clients: noms, adresses, dates de naissance, coordonnées bancaires, historique des transactions,

(1) BERR, *2008 Information Security Breaches Survey* [Enquête 2008 sur les violations de la sécurité de l'information], *consultable en anglais à l'adresse suivante: http://www.security-survey.gov.uk (dernière visite le 22 juillet 2008).*

codes PIN, numéros d'assurance sociale, etc.([2]) Protéger ces données personnelles et financières constitue donc l'une des responsabilités clés du secteur des services financiers.

Introduire davantage de technologie ne suffira pas à résoudre ces problèmes. Une approche plus holistique, tenant compte des comportements et de la culture, en plus de la technologie, est nécessaire. Si les politiques et les contrôles techniques sont sans aucun doute essentiels à tout programme de sécurité de l'information (SI), ces mesures à elles seules ne peuvent suffire à garantir une protection concrète des informations. Pour être efficaces, les programmes de sensibilisation à la sécurité de l'information doivent se baser sur les actions des individus évoluant au sein de l'organisme. Les employés sont, bien entendu, les véritables acteurs du réseau de l'organisme et leur comportement est un aspect essentiel de la situation globale en matière de sécurité.
Les recherches et analyses effectuées par l'ENISA laissent entendre qu'une sensibilisation efficace des employés, dans laquelle non seulement ceux-ci comprennent leurs obligations, mais les mettent en pratique au quotidien, est l'une des méthodes les plus efficaces pour gérer les risques de sécurité de l'information menaçant aujourd'hui toutes les grandes organisations.

Finalité

L'ENISA estime que l'inadéquation de la sécurité des données est un problème sérieux et répandu. Elle reconnaît qu'une sensibilisation efficace des employés à la gestion des risques de sécurité de l'information est essentielle, surtout au sein d'organismes financiers. Le présent livre blanc constitue donc une introduction à l'importance de la sécurité de l'information dans ce secteur spécifique. Il entend également apporter de précieux conseils sur la préparation et la mise en œuvre des initiatives de sensibilisation à la sécurité de l'information.

Ce document est divisé en trois parties abordant les thèmes suivants:

- ✓ analyse de l'environnement des organismes financiers et de leurs principaux facteurs commerciaux;
- ✓ programmes de sensibilisation dans les organismes financiers;
- ✓ conseils pratiques, recommandations et études de cas proposés par un certain nombre d'organismes privés et modèles.

Objectifs

Cette publication vise à permettre à l'ENISA:

- ✓ d'expliquer l'importance de la sensibilisation à la sécurité de l'information dans les organismes financiers;
- ✓ d'analyser l'environnement et les facteurs commerciaux susceptibles d'influer sur ces programmes;
- ✓ de présenter des études de cas et des recommandations servant de point de départ à l'équipe de sensibilisation;
- ✓ de contribuer au développement d'une culture de sécurité de l'information et de favoriser le partage de connaissances entre États membres.

Publics

Ce livre blanc est destiné à être utilisé par le personnel et les dirigeants des organismes financiers, durant la mise en œuvre de programmes de sensibilisation à la sécurité de l'information. Il vise également à sensibiliser les différents acteurs à l'importance et au caractère critique d'un mouvement de sensibilisation à la sécurité de l'information au sein de leur organisme.

([2]) Autorité britannique des services financiers, *Data Security in Financial Services* [Sécurité des données dans le domaine des services financiers], Royaume-Uni, avril 2008.

Historique

L'Awareness Raising (AR) Community est une communauté gratuitement accessible ouverte aux experts concernés par la sensibilisation à la sécurité de l'information au sein de leur organisation. L'AR Community a été lancée en février 2008 en vue de collaborer avec la section «Sensibilisation» de l'ENISA dans le cadre de sa mission de promotion d'une culture de la sécurité de l'information – dans le but de soutenir la section dans ses activités.

Les contributeurs à la présente publication présentent une large gamme de compétences et de connaissances, ainsi que divers intérêts, une série de domaines d'expertises et une panoplie de priorités commerciales. Leur analyse combinée permet à l'AR Community de jouer un rôle majeur dans l'échange de bonnes pratiques en matière de sécurité de l'information à travers toute l'Europe.

Dans le cadre de son rôle de point de contact pour les questions ayant trait à la sensibilisation à la sécurité de l'information, l'AR Community a invité ses membres à participer à des groupes de travail virtuels (GTV) afin d'étudier plus précisément les questions pertinentes en vue d'élaborer des livres blancs.

La présente publication se base sur des études et des analyses menées par le GTV de l'ENISA intitulé «Comment organiser des programmes de sensibilisation dans les organismes financiers», par le personnel de l'ENISA et grâce à des informations accessibles au public ou fournies à l'ENISA par les organismes concernés.

Organismes financiers: définition

La présente publication est destinée aux organismes financiers, plus particulièrement aux dirigeants et au personnel impliqués dans l'élaboration de programmes de sensibilisation à la sécurité de l'information, afin de leur permettre de protéger leurs données et d'évaluer les risques menaçant celles-ci ainsi que de planifier des initiatives efficaces de formation et de sensibilisation en vue d'éviter les violations et incidents de sécurité de l'information.

Dans le cadre de cette publication, «organismes financiers» est un terme générique englobant les banques de détail et les banques de gros, les entreprises d'investissement, les compagnies d'assurance (vie et générale), les conseillers financiers, les coopératives de crédit et les prestataires de services de paiement de toutes tailles.

Analyse de l'environnement et des facteurs clés

Introduction

Les incidents de sécurité de l'information et les atteintes aux données dans les organismes financiers ont fait beaucoup parler d'eux l'année dernière. Bien entendu, la plupart d'entre nous aurons surtout axé nos discussions sur les banques, celles-ci étant la plaque tournante du monde des finances. Il convient toutefois de remarquer qu'au vu de l'environnement réglementaire actuel, tous les organismes financiers sont actuellement en train de revoir leur approche en matière de sécurité de l'information et particulièrement en matière d'éducation à la sécurité du personnel à tous niveaux d'ancienneté. Ce phénomène concerne notamment les associations de carte de crédit, les négociants

de l'industrie du détail, les prestataires de services de paiements ainsi que les organismes d'assurance.

Ces acteurs du monde financier sont soumis à différents cadres législatifs et sectoriels réglementant la manière dont ils doivent former leur personnel à la gestion des informations et la manière dont les informations à caractère sensible doivent être protégées. Si certains cadres fixent des lignes directrices claires sur la raison d'être, les modalités et la fréquence des formations en matière de sécurité de l'information, les autres restent vagues sur ce sujet. Les organismes financiers doivent tous envisager les grandes questions suivantes:

- ✓ quels cadres législatifs et sectoriels s'appliquent à mon organisme financier et à notre façon de faire des affaires?
- ✓ notre stratégie actuelle de sécurité de l'information permet-elle à l'organisme d'adopter une approche proactive en matière de sécurité de façon à respecter les exigences de conformité ainsi que les obligations de sécurité sectorielles?
- ✓ nos programmes de sensibilisation à la sécurité de l'information et nos initiatives de formation du personnel sont-ils adaptés aux meilleures pratiques exigées dans le secteur financier?
- ✓ la sensibilisation à la sécurité de l'information est-elle approuvée et entièrement appuyée par les hauts dirigeants?
- ✓ la sensibilisation à la sécurité de l'information a-t-elle été positionnée comme un atout commercial et sinon, mon organisme est-il à même de faire des initiatives de sensibilisation un véritable outil de retour sur investissement et d'amélioration de la productivité et non plus un simple poste de coûts?

Le premier problème qui attend les organismes financiers sera toutefois d'arriver à planifier des activités de sensibilisation à la sécurité de l'information et de les mettre en œuvre. Cela s'explique par la nature de leurs activités: le personnel de ces organismes est constamment occupé à garantir à tout moment les flux de données car les temps d'arrêt ne sont pas envisageables. L'exemple de la Bourse de Londres, qui a récemment connu une panne d'une durée sans précédent, démontre précisément la façon dont une panne des systèmes informatiques peut affecter les opérations quotidiennes. Une solution envisageable pour parer à ce problème est d'intégrer aux programmes généraux d'introduction et de formation actuels des activités de sensibilisation à la sécurité de l'information. Celles-ci doivent toutefois s'inscrire dans le cadre d'un processus permanent de sécurité et de conformité commençant par l'éducation, avant de passer à la correction et, le cas échéant, à l'agrément officiel/conformité et, enfin, au maintien de l'agrément par le biais d'initiatives permanentes de sensibilisation à la sécurité de l'information. Le maintien de ce processus itératif est très important pour les marchés financiers, qui sont essentiels pour les infrastructures critiques (IC) du monde et sont donc surveillés de près par les consommateurs, les entreprises et les gouvernements.

Le secteur financier est habituellement régi par deux types d'obligations: les obligations

légales et les cadres sectoriels. S'il existe un certain degré de convergence entre ces deux éléments, qui fait que le respect des orientations sectorielles peut devenir une obligation légale, la plupart des cadres législatifs régissant les organismes financiers fonctionnent indépendamment des cadres sectoriels réglementant la conception, l'élaboration et la mise en œuvre des initiatives de sensibilisation à la sécurité de l'information au sein des organismes financiers. Cela étant, il convient cependant de remarquer qu'au cours des cinq dernières années, le secteur a vu émerger clairement des objectifs communs aux cadres législatifs et sectoriels dans le domaine de la sécurité des informations dans les organismes financiers parce que le nombre de vols d'identité a considérablement augmenté et que des violations graves se sont produites, principalement au R-U et aux États-Unis. Ces deux pays étant les grands centres financiers du monde, ils ont par conséquent joué un rôle moteur dans l'élaboration de législations et de règlementations visant à traiter ces problèmes. De plus, l'obligation de signaler les violations de sécurité a été imposée dans de nombreuses juridictions du monde entier et se généralise peu à peu aux quatre coins du globe. Par exemple, le principe de la loi 1386 du Sénat en Californie (SB 1386), qui décrit quand et comment les consommateurs, les autorités et les médias doivent être informés des atteintes aux données, a servi de modèle à une loi fédérale similaire aux États-Unis, où 40 États disposent aujourd'hui d'une loi sur la notification. Un certain nombre de pays de l'UE, dont le R-U et l'Irlande, étudient actuellement des solutions similaires. Il est important de le remarquer car si la notification des violations de sécurité devenait une obligation légale, plus d'efforts seraient probablement entrepris pour éviter que ces violations ne surviennent. Cela signifie également que l'ensemble du personnel des organismes financiers devra être encore plus conscient des menaces de sécurité de l'information et devra recevoir une formation officielle aux risques associés au traitement des données financières.

Analyse des moteurs commerciaux

La principale incitation à observer les obligations légales et sectorielles est la crainte de sanctions et de poursuites judiciaires (au pénal ou au civil) pour non-respect. Si le respect des obligations implique rarement des récompenses financières ou juridiques directes (du type «sphère de sécurité»), il peut néanmoins permettre dans certains cas de réduire ses frais d'assurance.

Fondamentalement, lorsqu'il s'agit des exigences en matière de sensibilisation, les organismes financiers doivent être bien informés des obligations de conformité et de gouvernance ainsi que des cadres de sécurité, afin de pouvoir déterminer lesquels s'appliquent à eux, au niveau national ou international, et lesquels concernent le secteur financier dans sa globalité. Les grands moteurs commerciaux sont la démonstration d'une bonne gouvernance et du respect des normes tout en améliorant la sécurité de l'information, autant pour l'organisme financier lui-même que pour ses clients et fournisseurs. En d'autres termes, l'écosystème des organismes financiers rend tous ses acteurs interdépendants et il existe des liens évidents entre les responsables de la promotion des normes et ceux qui sont chargés de mettre en œuvre ces normes en aval de la chaîne, par exemple en appliquant la norme PCI DSS (Payment Card Industry Data Security Standard, ou norme de sécurité informatique des données de l'industrie des cartes de paiement). En observant les obligations légales et sectorielles, nous nous servons des cadres sectoriels pour protéger les données à caractère sensible et pour assurer la continuité des activités au sein de cet écosystème. D'un point de vue technique, il s'agit de se concentrer sur la réduction de l'exposition juridique, la protection des relations publiques et la réputation de la marque en protégeant les actifs financiers de la clientèle et l'identité de chaque client individuel.
La norme de sécurité informatique des données de l'industrie des cartes de paiement (PCI DSS) est probablement l'une des rares normes de sécurité fixant réellement un objectif de contrôle entièrement dédié à la sensibilisation à la sécurité de l'information (exigence 12.6). Elle comprend notamment des exigences relatives aux programmes de sensibilisation à la sécurité de l'information et s'adresse à différentes couches du secteur des organismes financiers, des associations de carte à d'autres entités telles que les banques acquéreuses, les fournisseurs de services de paiement, les négociants et toutes les parties tierces appartenant à cette chaîne et susceptibles de stocker, de traiter et de transmettre des informations sur les cartes de crédit. Le respect des obligations de la

norme PCI DSS sera donc exigé de la majorité des détaillants appartenant à de grandes chaînes ainsi que de toute boutique capable d'accepter les paiements par carte de crédit. Cette norme s'applique à toutes les entités du monde entier. Elle se compose de 12 exigences de haut niveau, associées chacune à une série de contrôles stratégiques, procéduraux et techniques et d'exigences en matière de transfert de compétences. L'exigence 12.6 dispose qu'une entité «doit mettre en œuvre un programme officiel de sensibilisation à la sécurité et informer ses employés, dès leur embauche et au minimum une fois par année, de l'importance de la sécurité des données des titulaires de cartes». Elle expose également les modalités de contrôle du respect de cette règle par rapport au niveau le plus élevé de la norme PCI DSS (niveau 1), qui exige l'exécution annuelle d'un audit sur le terrain par des évaluateurs indépendants qualifiés (EIQ). Chaque entité «doit pouvoir prouver, par ses registres de formation, que tous les membres du personnel concerné par le champ d'application ont reçu une formation. Il faut également pouvoir produire les supports de sensibilisation à la sécurité et démontrer qu'ils ont été mis régulièrement à jour en fonction de l'évolution de votre environnement de données de titulaires de cartes ainsi que des nouvelles exigences fixées dans le cadre de la norme». D'un point de vue plus holistique, chaque entité est chargée de renforcer les niveaux de sensibilisation des acteurs en aval de la chaîne PCI: les banques acquéreuses sont donc responsables de la promotion de la norme auprès de tous ses négociants, activité qui nécessite elle-même un projet de sensibilisation à la sécurité.

ISO/IEC 27001, la norme internationale pour les systèmes de gestion de la sécurité de l'information issue du BS7799 et complétée par les normes ISI/IEC 27002 et 27005, prend également de plus en plus d'importance et comprend une disposition destinée aux programmes de sensibilisation à la sécurité de l'information. Bien que le cadre de la norme ISO/IEC 27001 puisse être appliqué à n'importe quel organisme, il n'est pas rare de voir des organismes financiers l'utiliser comme référence pour trouver de bonnes pratiques en matière de sécurité de l'information, afin d'observer une large gamme de cadres législatifs et réglementaires, notamment la norme PCI DSS (remarque: lors d'un récent séminaire sur la norme PCI DSS, la Poste britannique a effectué une présentation expliquant la manière dont elle se basait sur la norme ISO/IEC 27001 pour observer la norme PCI DSS, étant donné que la mise en œuvre d'un système de gestion de l'information permet de répondre à un grand nombre d'exigences de la norme PCI DSS).

Plus fondamentalement, alors que certains nouveaux États membres de l'UE sont toujours en train d'affiner leurs régimes de protection et de non-divulgation des données, la plupart des États membres de l'UE ont adopté la directive européenne de 1995 sur la protection des données. Qu'il s'agisse, par exemple, de la loi irlandaise sur la protection des données, de la loi britannique sur la protection des données, de la loi portugaise sur la protection des données, du Datenschutzgesetz allemand ou de la loi française, à savoir la loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés, la plupart des cadres législatifs européens régissant la protection des données incluent des clauses contraignant les organismes à «prendre les mesures de sécurité appropriées pour protéger la réputation de la société, de ses employés, de ses affiliés et de ses clients» et insistant sur la protection des «données clés, y compris toute information financière» dont ils pourraient disposer([3]). Pour atteindre cet objectif, il est conseillé de mettre en œuvre des programmes de sensibilisation à la sécurité.

(*)* Directive 95/46/CE relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, JO L 281 du 23.11.1995. Figure également dans la loi (modifiée) irlandaise de 2003 sur la protection des données, article 2: «a) «données à caractère personnel», toute information concernant une personne physique identifiée ou identifiable («personne concernée par les données»); est réputée identifiable une personne qui peut être identifiée, directement ou indirectement, notamment par référence à un numéro d'identification ou à un ou plusieurs éléments spécifiques, propres à son identité physique, physiologique, psychique, économique, culturelle ou sociale», consultable à l'adresse suivante: http://www.dataprotection.ie/documents/legal/act2003.pdf

En Irlande, cette recommandation a été très bien diffusée par le Bureau du Commissaire en charge de la protection des données. Un certain nombre de banques et d'organismes d'assurance se sont enregistrés auprès du Bureau et ont élaboré des programmes de sensibilisation à la sécurité à l'intention du personnel et même de leur clientèle, c'est-à-dire les consommateurs finals. Certaines banques, telles que l'Ulster Bank, ont mis en place des programmes d'éducation élémentaires destinés à leurs négociants afin de les aider à respecter la norme PCI, tandis que d'autres mobilisent activement leurs employés en vue de renforcer les niveaux de sensibilisation à la sécurité.

Traditionnellement, les institutions financières ont toujours eu une certaine longueur d'avance en matière de programmes de sensibilisation à la sécurité de l'information, de même que certaines institutions gouvernementales, le secteur des technologies de l'information ainsi que l'industrie pharmaceutique. Les initiatives lancées se sont toutefois majoritairement cantonnées à des séminaires de formation ad hoc consacrés à la fraude et au vol d'identité ou à l'ingénierie sociale. Ce type d'effort n'est désormais plus suffisant (si tant est qu'il l'ait jamais été) pour satisfaire aux exigences législatives et sectorielles, ni pour rassurer la clientèle. Celle-ci s'attend à ce que les informations financières soient conservées en toute sécurité et en toute circonstance et à ce que ses actifs financiers soient protégés, même en cas de violation de la sécurité de l'information d'un réseau de la banque. En d'autres termes, si les consommateurs ne sont pas toujours à même de comprendre totalement les ramifications et les exigences liées à la mise en place de stratégies, de contrôles et de garanties de sécurité, ils attendent néanmoins des institutions financières qu'elles protègent l'argent qu'ils leur ont confié. Cela s'appelle la confiance.

Les institutions financières doivent fournir à leurs clients un environnement sûr et sous contrôle. Il existe toutefois des variations régionales et sectorielles perceptibles dans la manière dont les cadres légaux et sectoriels prévoyant des activités de sensibilisation à la sécurité de l'information sont appliqués aux «marchés» cibles d'une institution financière donnée. Il s'agit souvent d'un défi majeur pour les grands organismes financiers internationaux, qui doivent comprendre leurs obligations légales régionales et locales pour pouvoir les intégrer au sein d'une stratégie de sensibilisation à la sécurité de l'information à l'échelle de l'entreprise qui leur permettra d'assurer la conformité aux normes internes de sécurité tout en respectant les dispositions légales nationales et spécifiques au pays.

La meilleure façon d'élaborer une telle stratégie de sensibilisation au sein d'un organisme financier implique généralement plusieurs étapes:

- ✓ Étape n° 1: répartir les activités en groupes de pays/zones soumis à des législations et cadres sectoriels similaires afin de rendre le projet plus facile à gérer;
- ✓ Étape n° 2: identifier les cadres de protection et de non-divulgation des données s'appliquant à chaque catégorie;
- ✓ Étape n° 3: définir pour chaque catégorie une spécification complète pour les obligations en matière de sensibilisation à la sécurité de l'information;
- ✓ Étape n° 4: réaliser une analyse des écarts par rapport aux programmes de sensibilisation actuels et mettre à jour les programmes pour satisfaire aux obligations légales/sectorielles.
- ✓ Étape n° 5: fournir des programmes à jour à toutes les catégories.
- ✓ Étape n° 6: faire des étapes n° 1 à n° 5 un processus permanent soumis à une révision (au minimum) annuelle.

L'élaboration de stratégies et de programmes de ce type suppose qu'une stratégie d'utilisation acceptable pour les outils de communication d'entreprises est en vigueur et qu'un plan de classification des données a également été approuvé par le conseil d'administration, déterminant ce qui constitue une donnée publique, sensible et confidentielle pour l'organisme financier.

La plupart des institutions financières abordent dans leurs programmes les sujets clés suivants: protection des données personnelles, descriptif des techniques de contrôle utilisées par l'organisme (constituant une obligation aux termes de la directive européenne sur la protection des données) et lignes directrices pour le transfert de données (par exemple de l'UE aux États-Unis). L'on peut également s'intéresser aux mécanismes de signalement, aux termes desquels le signalement d'incidents survenant aux États-Unis sera obligatoire tandis que le signalement dans l'UE se fera tout d'abord au sein de l'équipe de sécurité. Celle-ci collaborera ensuite avec les contrôleurs locaux de la protection des données afin de veiller à ce qu'ils procèdent au signalement dès que nécessaire.

Par ailleurs, les organismes financiers sont généralement performants pour mesurer le taux de réussite des programmes de sensibilisation à la sécurité de l'information. Ils utilisent souvent des mesures basées sur une matrice englobant la portée (l'organisme a-t-il atteint tout son personnel partout dans le monde?), la compréhension (le public ciblé a-t-il entièrement compris ce que l'on attendait de lui, pourquoi et comment améliorer la sécurité?) ainsi que la modification des comportements (veiller à ce que les mauvaises habitudes de sécurité soient abandonnées et que le personnel tout entier soit pleinement conscient des questions de sécurité).

Il convient également de remarquer que la plupart des grands organismes financiers sont à même d'adopter une approche holistique dans le domaine de la sensibilisation à la sécurité. Les hauts dirigeants qui doivent être impliqués dans ce processus restent le principal point de contact/la cible des contrôleurs des cadres gouvernementaux et sectoriels et, en tant que tels, devront favoriser une culture de la sécurité de l'information en adoptant la vision à long terme quantifiable de sensibilisation à la sécurité de l'information décrite ci-dessus. Ils devront donc veiller à ce que les programmes soient viables (c'est-à-dire qu'ils soient des programmes à long terme capables d'évoluer à mesure que le modèle commercial de l'organisme financier évolue lui-même et de prendre en considération les nouvelles menaces et les nouvelles obligations légales et sectorielles), cohérents (toujours appliqués de manière équitable à l'ensemble des membres du personnel, quelle que soit leur ancienneté ou leur rang), efficaces (dont l'efficacité est mesurée et qui sont améliorés en permanence) et transparents (communiqués intégralement à l'ensemble du personnel, y compris lorsqu'il s'agit de sanctions pour non-respect des exigences de sécurité de l'information telles qu'elles sont décrites dans le programme de sensibilisation).

Focus sur les États-Unis – Actualité en matière d'exigences de sensibilisation: des «Red Flag Rules» contre le vol d'identité

Cette nouvelle exigence visant les institutions financières américaines entre en vigueur le 1er novembre 2008. Il convient de remarquer qu'elle dispose que les institutions bancaires doivent renforcer, étayer par des documents et mettre en œuvre de nouveaux programmes de sensibilisation destinés aux employés comme aux clients. La formation, y compris celle des membres du conseil d'administration, est essentielle pour satisfaire à cette règle.

La «Red Flags Rule» fait partie de la loi américaine de 2003 sur les opérations de

crédit justes et adéquates (Fair and Accurate Credit Transactions (FACT) Act). Aux termes de cette règle, les institutions financières et les créanciers possédant des comptes couverts doivent avoir mis en place au plus tard pour le 1er novembre 2008 des programmes de protection contre le vol capables d'identifier, de détecter et de réagir à des comportements, pratiques ou activités spécifiques pouvant indiquer un vol d'identité(4).
Les organismes de réglementation bancaire collaborent avec leurs institutions afin d'assurer le respect de cette règle. La Federal Trade Commission, quant à elle, veille à ce que les autres entités couvertes identifiées en tant que créanciers la respectent également.

État des lieux 2008 de la sécurité des informations bancaires en 2008 - Synthèse analytique de l'enquête

Selon la *2008 State of Banking Information Security survey* (état des lieux 2008 de la sécurité des informations bancaires), l'éducation de la clientèle demeure insuffisante([5]). Selon cette enquête, «pour gagner cette confiance, il y a lieu d'entreprendre des efforts proactifs pour informer la clientèle sur la sécurité bancaire en ligne et sur les risques de vol d'identité - y compris le phishing, perpétré via e-mail et à partir de téléphones situés hors des institutions, mais pouvant tout de même entraîner des dommages considérables et miner la confiance de la clientèle».

Cela prouve que l'éducation et la sensibilisation au sein des organismes financiers doivent être assurées tant au niveau interne qu'externe afin de créer une plateforme de confiance et de permettre d'adhérer de manière proactive aux exigences de conformité et de gouvernance.

Préoccupations des organismes financiers

Les recherches et analyses effectuées par l'ENISA ont permis d'identifier quelques-unes des principales préoccupations des entreprises en matière de sécurité des données.

- ✓ confiance du marché: maintenir la confiance dans le système financier([6]);
- ✓ protection et sensibilisation de la clientèle: une perte de données pourrait avoir un impact important sur les particuliers;
- ✓ fuites de données: afin de limiter ces fuites, les organismes pourraient notamment établir des politiques de sécurité de l'information et réglementer l'utilisation des appareils mobiles;
- ✓ données perdues et coûts des activités d'appui: une politique de sécurité de l'information pourrait aider les organismes financiers à récupérer les données en cas de vol ou de perte, événements pouvant survenir même lorsque des mesures de sécurité sont en place, ce qui permettrait de diminuer les coûts de propriété et les coûts des activités

([4]) Voir McGlasson, Linda, *ID Theft Red Flags Rule: How to Help Your Business Customers Comply* [La «Red Flags Rule» contre le vol d'identité: comment aider vos clients à l'observer], BankInfoSecurity.com, 8 septembre 2008
http://www.bankinfosecurity.com/articles.php?art_id=960andrf=090908eb
(5) Voir *State of Banking Information Security 2008 - Survey Executive Overview,* BankInfoSecurity.com, consultable en anglais à l'adresse suivante:
http://www.bankinfosecurity.com/whitepapers.php?wp_id=143 (dernière visite le 20 novembre 2008).
([6]) Autorité britannique des services financiers, *Data Security in Financial Services* [Sécurité des données dans le domaine des services financiers], Royaume-Uni, avril 2008.

d'appui;
- ✓ les défis que représente le respect des normes réglementaires et de sécurité: faire prendre en charge par les entreprises la sécurité des données permettra de mieux observer les trois aspects de la sécurité de l'information (confidentialité, disponibilité et intégrité) ainsi que certaines normes de sécurité et/ou cadres de conformité (telles que les normes ISO/IEC 27001, PCI DDS, etc.);
- ✓ diminution de la criminalité financière.

Risques et menaces

Vu la structure des organismes financiers, les procédures qu'ils doivent observer, le recours fréquent à de tierces parties pour prester des services spécialisés (publipostage, prestations de services informatiques, etc.) et la capacité d'accéder, de stocker et de transmettre rapidement, facilement et efficacement des informations à caractère sensible, le nombre de risques et menaces potentiels est presque infini. Il est néanmoins possible d'en identifier certains:

- ✓ fuites de données([7]): il est impossible d'évaluer les conséquences d'une fuite de données de valeur subie par un organisme, mais ce problème est pourtant de plus en plus répandu.
- ✓ pertes d'informations: la plupart du temps, lorsque des informations à caractère sensible (par exemple des données sur la clientèle et/ou sur les employés) se retrouvent entre de mauvaises mains, elles sont conservées pour être réutilisées à des fins personnelles, même lorsqu'elles sont classées «confidentielles». La responsabilité juridique de l'organisme peut éventuellement être engagée.
- ✓ confidentialité de l'information: lorsque des informations se retrouvent entre de mauvaises mains, l'institution financière subit une perte bien plus conséquente qu'un simple remplacement du coût, par exemple, du périphérique sur lequel les informations étaient stockées.
- ✓ intégrité de l'information: modification du contenu.
- ✓ corruption des données: modification accidentelle des données.
- ✓ sécurité des données: détournement d'informations de l'entreprise. Les données risquent d'être utilisées ou vendues à des fins illicites.
- ✓ préjudice aux activités/à la réputation/à l'image de l'entreprise: en cas de vol de données, la publicité qui en résulte peut considérablement nuire à la réputation de l'entreprise et ainsi porter préjudice à ses activités.

- ✓ perte de position dominante sur le marché.
- ✓ logiciels malveillants: introduction de codes source malveillants dans le réseau, qu'il s'agisse de virus, de vers, de logiciels espions ou de chevaux de Troie.
- ✓ fraude/tromperie:
  - extorsion;
  - vol d'identité: par exemple, au Royaume-Uni, un ordinateur portable contenant des données relatives à quelque 2 000 personnes et à leurs comptes d'épargne a été dérobé à un employé de l'administration fiscale et douanière britannique; cette même administration a ainsi perdu les informations personnelles de 6 500 bénéficiaires de pensions privées; neuf prestataires de services de santé nationaux ont

([7]) Heiser, Jay, *Understanding data leakage,* Gartner, 21 août 2007; *«Data-leak security proves to be too hard to use»* [Les systèmes de sécurité anti-fuite de données se révèlent trop difficiles à utiliser], Infoworld.com, consultable en anglais à l'adresse suivante: http://www.infoworld.com/article/08/03/06/10NF-data-loss-prevention-problem_1.html (dernière visite le 2 juin 2008).

perdu des dossiers de patients conservés sur un CD-ROM([8]).
- détournement de propriété intellectuelle, de secrets d'affaires, d'informations protégées par un droit de propriété.

✓ blanchiment d'argent.
✓ abus de marché.

Segmentation du public: définition

Une grande partie des activités de planification d'une campagne de formation et de sensibilisation au sein d'un organisme vise à garantir que le programme est exécuté de manière efficace et effective et que son contenu est facilement compris. Son format doit pouvoir être appréhendé par tout le monde.

Un programme commun à toute l'entreprise peut se révéler difficile à appliquer dans l'ensemble d'une organisation lorsqu'il peut être nécessaire de modifier le message afin de s'adapter à la culture, aux lois et aux règlements du pays. Les messages d'entreprise nécessitent souvent une personnalisation en fonction de l'endroit où ils sont délivrés, mais le programme doit néanmoins conserver le style propre à l'entreprise afin de garder le même aspect général.

✓ Quelles sont les dispositions déjà mises en place dans toute l'entreprise/au niveau local?
✓ Quelles sont les autres initiatives mises en œuvre (lien avec l'initiative actuelle)?

Fonctions

Les membres du personnel doivent être répartis en groupes cible selon leur fonction. Chaque groupe cible devra observer des exigences différentes en matière de formation et de sensibilisation. Le contenu applicable du programme devra être réparti en modules et dispensé de manière efficace. La disponibilité et le lieu de travail des employés (travailleurs mobiles, à domicile, etc.) doivent être pris en considération au moment de définir le contenu du programme.

Pour pouvoir mettre en œuvre un programme de formation ciblé, il est nécessaire de regrouper les personnes au sein de divers groupes de fonctions/groupes cible et de définir les risques commerciaux liés à chaque groupe cible afin de définir une formation adéquate.

Pour éviter les pertes de temps et l'énervement, il est important que toute initiative de sensibilisation soit ciblée et que seules les formations applicables soient dispensées. En dispensant une formation applicable dans le format adéquat, l'organisme réussira à motiver son personnel en lui faisant passer un message pertinent et évitera de gaspiller inutilement du temps et de l'argent dans des heures de formations inadéquates.

La sécurité de l'information étant une question omniprésente, les différentes catégories d'employés

([8]) ENISA, *Clés USB: priorité à la sécurité*, 2008, consultable à l'adresse suivante: http://www.enisa.europa.eu/doc/pdf/publications/secure_usb_flash_drives_fr.pdf

ont des besoins d'éducation différents. Outre les activités régulières de sensibilisation auprès des employés au sens large, qui devraient notamment aborder les questions relatives à l'utilisation adéquate des ressources de l'organisation, aux procédures d'alerte, aux responsabilités en matière de continuité des activités, à la conformité et à l'éthique, les groupes spécifiques suivants ne sont que quelques exemples des différents types de formation envisageables:

- ✓ Les employés ayant accès aux informations internes sur la clientèle et étant en contact direct ou indirect avec le public (par exemple les employés des centres d'appel et les caissiers) devraient être informés sur certains sujets tels que l'ingénierie sociale et les réglementations sur la protection de la vie privée car ils ont accès aux informations sur la clientèle et pourraient accidentellement les transmettre à des parties non autorisées.
- ✓ Les employés ayant accès aux informations commerciales internes et étant en contact avec le public (par exemple les vendeurs, gestionnaires de comptes, etc.) doivent être informés de la nécessité d'assurer la confidentialité des informations relatives aux processus commerciaux internes, aux partenariats et aux mécanismes de contrôle au sein de l'entreprise pouvant directement ou indirectement affecter la stratégie de l'organisation.
- ✓ Le personnel IT devrait recevoir une formation au sujet notamment des règlementations auxquelles est soumise l'entreprise, des mécanismes de contrôle et d'audit internes en place ainsi que de la stratégie de l'organisme au sujet des meilleures pratiques de gestion de la sécurité informatique et des réseaux.
- ✓ Les membres de la direction (PDG, directeur financier, etc.) gèrent l'organisme et en sont en fin de compte responsables, c'est pourquoi il convient d'élaborer un programme spécifique de formation/de sensibilisation afin de les informer de manière continue sur les règlementations en vigueur et leurs implications (positives ou négatives) pour l'organisme.

Lors de l'élaboration d'un programme de sensibilisation, il est impératif que tous les rôles soient clairement définis et associés aux différentes questions de sécurité de l'information. Les tableaux ci-dessous présentent une liste des rôles, avec leur description, ainsi qu'un échantillon de modèle avec les rôles dans la colonne de gauche et, en haut, les questions de sécurité de l'information qu'ils doivent connaître:

Rôle	Description
Cadres supérieurs	Doivent connaître les questions relatives à la gouvernance de l'information ainsi les cadres légaux, les risques et les responsabilités (y compris les responsabilités personnelles). Ces personnes ont habituellement des plannings très serrés et sont souvent peu enclines à prendre part aux mêmes activités de sensibilisation que le reste du personnel. Des activités de sensibilisation courtes et plus ciblées sont conseillées; elles établiront clairement un lien entre la sécurité de l'information et la protection de la réputation de l'organisme.
Employés administratifs et employés de bureau assurant des fonctions de post-marché et de soutien	Ces employés travaillent souvent selon des créneaux de traitement des transactions stricts et des objectifs très clairs. Il faut donc étudier attentivement l'organisation et la programmation d'activités de formation leur étant destinées. Il est important de s'entretenir avec les directeurs au sujet de la programmation des activités de formation; les séances de formation en groupe ne sont pas forcément la solution la plus appropriée en raison de leur impact important sur les affaires courantes. La plupart des employés de ce secteur ne travaillent pas hors de leur bureau et ne font pas un usage intensif des appareils portables. Les thèmes à aborder en matière de sécurité de l'information sont donc plus restreints, limitant donc la durée de la formation globale.
Personnel des centres d'appel	Comme pour les employés administratifs et les employés de bureau, la programmation des activités de formation sera probablement difficile dans un centre d'appel où la réponse rapide aux appels des clients revêt une importance capitale. Ici encore, il sera important d'être en contact avec la direction du centre. De même, la plupart des membres du personnel ne travaillent pas hors du bureau et ne

Rôle	Description
	font pas un usage intensif des appareils portables. Le champ d'application des activités de formation est donc restreint. Toutefois, la protection et la confidentialité des données, de même que la sensibilisation à l'ingénierie sociale, seront probablement des sujets essentiels.
Personnel chargé de la vente des services financiers dans les agences	Beaucoup d'employés basés dans les succursales ne disposent pas d'une station de travail personnelle et dans certaines agences, les caissiers n'ont même pas accès à l'intranet. L'accès aux formations électroniques se fait souvent via PC partagés ou via les PC des directeurs; il faut donc les planifier soigneusement afin d'assurer le maintien des services à leur niveau habituel tout en réalisant les objectifs de la formation. Dans les agences, il est également courant que des filiales plus éloignées géographiquement aient une bande passante plus restreinte et rencontrent des difficultés pour accéder à l'intranet de l'entreprise; il faut donc réfléchir aux différents moyens d'optimiser la prestation de formations en ligne dans ce type d'environnement.
Commerciaux et travailleurs à distance	Ces employés accèdent généralement à l'intranet de l'entreprise à distance à partir de dispositifs informatiques portables. Ils présentent des besoins particuliers en formation plus pointus que ceux du reste du personnel, notamment en ce qui concerne: ✓ la sécurité de l'information en dehors du bureau (sécurité des dispositifs mobiles, etc.) ✓ les procédures d'accès à distance ✓ la sécurité durant les déplacements.
Banques d'investissement	Les banques d'investissement ont généralement une culture de la performance et sont axées sur les commissions. Dans ce groupe, il est primordial d'exposer la raison d'être de la formation. Il est également important de veiller à raccourcir au maximum la formation, de veiller à ce qu'elle puisse être suivie en portions gérables et de prévoir des signets afin que les personnes suivant la formation puissent revenir là où elles s'étaient arrêtées sans devoir revenir en arrière. Au sein de ce public cible, le soutien des cadres supérieurs de l'entité est souvent essentiel à la réussite des programmes de formation à la sécurité de l'information.
Marketing	Le personnel de la section marketing est responsable des relations publiques ainsi que de l'image de l'institution. Il doit donc connaître les types d'information qu'il est ou non autorisé à utiliser lorsqu'il prépare une campagne ou lorsqu'il communique avec les médias en cas d'incident.
Personnel IT	Le personnel IT doit être informé de la stratégie de sécurité de l'organisme et doit savoir quels types de contrôles sont obligatoires et quels types de preuves doivent être générés afin d'assurer la conformité.

Figure 1: Liste des fonctions et descriptif de celles-ci. À titre illustratif seulement.

Certains des thèmes relatifs à la sécurité de l'information mentionnés ci-dessous peuvent varier, pour chaque fonction, selon les politiques propres à l'organisme financier. Une banque peut par exemple autoriser le télétravail pour certains employés de bureau. La stratégie pourrait dès lors être adaptée pour ce rôle et les besoins de sensibilisation modifiés en conséquence.

En outre, certains thèmes peuvent être divisés en sous-sections («Traitement des données des clients» est une vaste sous-catégorie du traitement des données à caractère sensible et il peut être judicieux d'y consacrer une section à part entière) et certains sujets peuvent en rejoindre d'autres

(la «sécurité du matériel» pourrait par exemple se retrouver dans la sensibilisation au «travail mobile»).

	Cadres supérieurs	Employés administratifs et employés de bureau assurant des fonctions de post-marché et de soutien	Personnel des centres d'appel	Personnel chargé de la vente des services financiers dans les agences	Commerciaux et travailleurs à distance	Banques d'investissement	Marketing	Personnel IT
Sécurité physique	✓	✓	✓				✓	✓
Sécurité du lieu de travail (par exemple le bureau, la filiale, etc.)	✓	✓	✓	✓		✓	✓	✓
Sécurité du matériel	✓				✓	✓	✓	✓
Contrôles internes	✓	✓	✓	✓	✓	✓	✓	✓
Identifier et signaler les violations de sécurité	✓	✓	✓	✓	✓	✓	✓	✓
Vie privée							✓	
Continuité des affaires	✓	✓	✓	✓	✓	✓	✓	✓
Réglementations obligatoires						✓		
Protection des données et de leur caractère privé	✓							
Rétention, stockage et destruction des informations à caractère sensible	✓	✓	✓	✓	✓	✓	✓	✓
Traitement des données des clients		✓	✓	✓	✓	✓	✓	✓
Dispositifs portables	✓				✓	✓	✓	✓
Supports amovibles	✓			✓	✓	✓	✓	✓
Logiciels (licences)	✓	✓		✓	✓	✓	✓	
Mots de passe	✓	✓	✓	✓	✓	✓	✓	✓
Sauvegardes	✓	✓		✓	✓	✓	✓	✓
Codes malveillants	✓	✓			✓	✓	✓	✓

	Cadres supérieurs	Employés administratifs et employés de bureau assurant des fonctions de post-marché et de soutien	Personnel des centres d'appel	Personnel chargé de la vente des services financiers dans les agences	Commerciaux et travailleurs à distance	Banques d'investissement	Marketing	Personnel IT
Travail mobile & à domicile	✓				✓	✓	✓	✓
Utilisation de l'internet et du courrier électronique	✓	✓		✓	✓	✓	✓	✓
Tierces parties (fournisseurs et visiteurs)	✓					✓		
Ingénierie sociale	✓	✓	✓	✓	✓	✓	✓	✓

Figure 2: Association des rôles avec les thèmes de sécurité. À titre illustratif seulement.

Situation géographique

Mettre en œuvre un programme de sensibilisation à la sécurité de l'information destiné à un personnel disséminé en divers endroits du monde est une tâche compliquée à la fois au niveau du contenu et au niveau de l'organisation. Le principal défi est de donner la formation dans toute l'organisation en s'assurant que son format soit reconnu et accepté de manière uniforme par les différents publics ciblés. Il convient de tenir compte des éléments suivants:

- ✓ Systèmes/méthodes informatiques d'organisation de la sensibilisation: dans les organismes répartis au sein d'une zone géographique étendue où il est impossible d'adopter une approche commune, différentes alternatives de sensibilisation sont envisagées. Certaines régions du monde sont limitées au niveau de l'infrastructure disponible. Lorsque l'apprentissage en ligne ou la formation assistée par ordinateur (FAO) est la méthode privilégiée, il est important d'identifier les limitations existantes avant de prévoir la conception d'une solution centrale ou distribuée. Entreprendre des actions pilotes permet souvent de garantir que le programme puisse satisfaire aux différentes exigences du système et d'éviter les retards dans le processus de mise en œuvre. Des tests clés du système doivent être prévus pour les éléments suivants:
  - bande passante du réseau;
  - limitations du serveur internet;
  - limitations (audio/vidéo, etc.) des systèmes des utilisateurs finals;
  - différents styles d'intranet.
- ✓ Les lois et les réglementations/législations varient dans chaque pays: les lois sur la protection des données/sur la protection du caractère privé des données varient selon les juridictions et il convient de prendre les dispositions suivantes avant d'élaborer le contenu d'un programme de sensibilisation:
  - s'assurer que le contenu est conforme aux lois et réglementations locales;
  - faire appel à des partenaires et spécialistes locaux pour l'élaboration du contenu en cas de manque de connaissances internes;
  - personnaliser certaines parties du programme afin d'observer les lois, réglementations et législations locales.
- ✓ Structure organisationnelle
  - Chaînes de communication compliquées: chaque partie de l'organisme peut présenter des chaînes de communication différentes ou confuses. C'est pourquoi le

soutien des cadres supérieurs est primordial pour chaque mise en œuvre d'une initiative de sensibilisation à la sécurité de l'information. Le projet doit prendre en considération à cet égard les éléments suivants:

- avec qui nouer le dialogue;
- soutien de la direction;
- financement;
- planification;
- élaboration/personnalisation;
- prestation/déploiement;
- évaluation.

✓ Le siège social lance la campagne de sensibilisation: la plupart des mises en œuvre de programmes de sensibilisation ont été lancées par le siège social de l'organisation, avec différents degrés d'acceptation dans le monde. Il est important de faire accepter ces programmes par les cadres supérieurs dans chaque pays/chaque région pour assurer l'adoption réussie du programme dans l'ensemble de l'organisme. Cette approche permettra également de veiller à ce que les exigences locales soient identifiées à un stade précoce et que les programmes soient adaptés en conséquence.

Fusions et acquisitions

Le programme de sensibilisation doit être élaboré de manière à répondre aux défis liés aux fusions et acquisitions. La conception de ce programme sera modulaire afin de ne pas devoir modifier de grosses parties du contenu tout en exploitant les possibilités d'amélioration globale du programme. Il convient de tenir compte des éléments suivants:

✓ divergences des cultures d'entreprises: l'entreprise peut présenter différentes cultures, auquel cas il peut être nécessaire d'adapter légèrement le contenu afin de prendre en considération les nouvelles exigences.

✓ nouvelles entreprises/autres processus/autres risques commerciaux: le profil de risque peut être amené à changer en cas de fusion, rendant ainsi nécessaire la modification de certains éléments du contenu du programme.

✓ profil de l'entreprise: le style de l'intranet et les logos peuvent changer. Le programme de sensibilisation doit être suffisamment flexible pour que son contenu puisse être adapté en fonction du nouveau profil de l'entreprise.

✓ direction: le programme de sensibilisation doit être acceptable pour les nouveaux dirigeants de haut niveau et dirigeants opérationnels. Il est donc important qu'il s'accompagne d'un message émanant du conseil de direction signifiant l'engagement des cadres supérieurs et des actionnaires envers celui-ci.

Environnement multiculturel

La mise en œuvre d'un programme de formation et de sensibilisation à la sécurité de l'information dans un environnement multiculturel représente un défi majeur pour les organismes entre eux, mais aussi au niveau interne, au sein de chaque organisme. Les différences se situent sur plus d'un niveau et il est essentiel de pouvoir les identifier et de les traiter une à une de manière conviviale, tout en assurant le maintien de l'intégrité du programme dans son ensemble.

Les différences culturelles existant au sein d'un organisme doivent également être prises en considération au cours de la phase de planification. Les différentes parties de l'organisme peuvent présenter diverses cultures organisationnelles, surtout lorsque l'organisme a acquis certains processus et systèmes à la suite d'une fusion. Il convient de tenir compte des éléments suivants:

✓ questions culturelles;

- ✓ questions relatives au genre;
- ✓ questions relatives à la religion;
- ✓ questions relatives à la race;
- ✓ attitude face à l'humour (verbal et non verbal).

Canaux de diffusion/Méthode de prestation

Les canaux de diffusion et la méthode de prestation, de même que le message et l'émetteur, doivent être influents et crédibles, sans quoi le groupe cible pourrait être moins enclin à y prêter attention. Pour s'adresser correctement au public, il convient d'utiliser plus d'un canal de communication.

La présente section décrit quelques-uns des principaux canaux de diffusion et méthodes de prestation disponibles pour aider à sensibiliser les utilisateurs dans le cadre d'une initiative sur le thème de la sécurité de l'information. Il est par ailleurs suggéré d'utiliser une combinaison d'approches:

- ✓ formation modulaire ciblée: voir «Segmentation du public» ci-dessus. Il est important de construire le programme de sensibilisation à partir de modules individuels. Cela permettra d'offrir une formation adéquate à différents groupes cibles tout en ayant la possibilité de réutiliser une partie du contenu dans différents programmes.
- ✓ utilisation des ateliers/de l'apprentissage en ligne: les mises en œuvre déjà effectuées ont démontré que la meilleure approche pour favoriser la discussion et, par la suite, l'adoption de la formation dans l'environnement opérationnel, est d'organiser des ateliers départementaux de manière à ce que le contenu du programme de sensibilisation puisse, sous le contrôle des dirigeants opérationnels, s'inscrire dans le cadre d'un plan de travail départemental mis au point durant l'atelier. Les employés auront ainsi la possibilité de discuter, entre eux et avec leur chef opérationnel, des

Banque d'investissement - des formations interactives pour modifier les comportements

Une banque d'investissement nous a expliqué que son principal objectif était de satisfaire aux exigences de conformité au meilleur coût.

Or, ceci n'est pas possible sans l'élaboration de politiques définissant clairement ce que chacun peut faire ou non. Sans cette base, l'application des règles et la discipline deviennent difficiles à mettre en œuvre en cas de problème. Plutôt que de créer de nouvelles politiques et formations, la banque s'est efforcée dans la mesure du possible d'intégrer des points relatifs à la sécurité de l'information dans ses politiques et formations existantes.

Les politiques elles-mêmes ne sont efficaces qu'à partir du moment où le personnel les comprend. L'équipe de sécurité de la banque organise des présentations introductives pour tous les nouveaux arrivants afin de leur expliquer les politiques de sécurité menées par la banque. Ce contact direct permet au personnel de discuter avec l'équipe de sécurité des éventuels problèmes. Les retours d'informations émanant de ces formations démontrent que l'interaction est essentielle pour remettre en question l'attitude des employés et pour les aider à apprendre. Lorsqu'ils posent des questions, un processus de réflexion et d'examen de l'information s'enclenche. Une pièce remplie de personnes silencieuse n'apprend sûrement pas beaucoup. Partager ses anecdotes et ses expériences pertinentes aide le personnel à comprendre comment les menaces de sécurité peuvent l'affecter.

La banque a toutefois remarqué qu'une formation d'introduction n'était pas suffisante. Il est important d'envoyer fréquemment aux employés des rappels renforçant les messages clés d'une manière cohérente. Un élément essentiel à cet égard a été de réussir à convaincre les hauts dirigeants d'inspirer par l'exemple: ce sont eux, et non pas l'équipe de sécurité, qui sont les mieux placés pour promouvoir l'importance de ces messages.

L'équipe de sécurité emploie toute une gamme de techniques pour renforcer en permanence ses messages de sensibilisation. Les quiz et récompenses sont bien accueillis par le personnel: ils favorisent la réflexion et sont bien admis au sein de l'entreprise. Ici encore, l'interaction avec le personnel est cruciale. Par exemple, les affiches, rappels d'ordre passifs qui ne demandent en fin de compte aucune action individuelle sont souvent ignorées dans les faits. Les articles et sites sur l'intranet sont des méthodes efficaces pour promouvoir les messages auprès des personnes qui en font déjà un usage actif. Toutefois, pour ceux qui ne les visitent pas (c'est-à-dire la majorité du personnel), ils ne constituent pas un mécanisme efficace.

risques commerciaux locaux et du contenu du programme de sensibilisation consacré à ce thème et ce, sur leur lieu de travail.
L'utilisation de l'apprentissage en ligne s'est révélée être plus efficace lorsque les membres du personnel sont géographiquement dispersés et lorsque l'apprentissage en ligne est déjà utilisé au sein de l'organisme. La version utilisant l'apprentissage en ligne doit être conforme au programme de sensibilisation par atelier et utiliser le même contenu pour garantir que tous les employés de l'entreprise reçoivent une formation de sensibilisation à la sécurité de la formation d'un niveau homogène. L'apprentissage en ligne s'est également révélé efficace lorsque certains groupes cibles donnés nécessitent une formation spécifique.

- ✓ Utilisation de différents contenus: l'utilisation d'une combinaison d'extraits de films, de scénarios «vrai/faux», de supports d'apprentissage, de jeux et de questions d'autoévaluation s'est révélée utile pour donner une formation de sensibilisation à la sécurité de l'information réussie. La diffusion d'extraits de films représentant des incidents aide les gens à associer les règles aux éléments plus pratiques de leur travail. Lorsqu'une approche et un format plus souples sont proposés, les gens sont plus détendus et n'ont pas besoin de supports d'apprentissage supplémentaires pour comprendre les risques commerciaux, comment réagir en cas d'incident et, surtout, comment prévenir les incidents.
- ✓ Opposition sensibilisation/formation: la sensibilisation est définie comme suit dans la publication spéciale 800-16 du NIST: «La sensibilisation n'équivaut pas à la formation. Le but d'une présentation de sensibilisation est simplement d'attirer l'attention sur la sécurité et de faire comprendre pourquoi celle-ci est importante. Les présentations de sensibilisation visent à permettre aux individus de reconnaître les problèmes de sécurité IT et d'y remédier de manière adéquate. Lors d'activités de sensibilisation, l'apprenant est le destinataire de l'information, tandis qu'il joue un rôle plus actif dans le cadre d'une formation. La sensibilisation cherche à atteindre des publics larges par une présentation attrayante. La formation, elle, est plus formelle; son but est de renforcer les connaissances et les compétences afin de faciliter l'exécution des tâches»([9]).

([9]) NIST, *Information technology security training requirements: A role- and performance-based model* [Exigences de formation en matière de sécurité des technologies de l'information: modèle axé sur les performances et les rôles], NIST — SP 800-16, États-Unis, 1998, consultable à l'adresse suivante: http://csrc.nist.gov/publications/nistpubs/800-16/800-16.pdf (dernière visite le 21 juillet 2008).

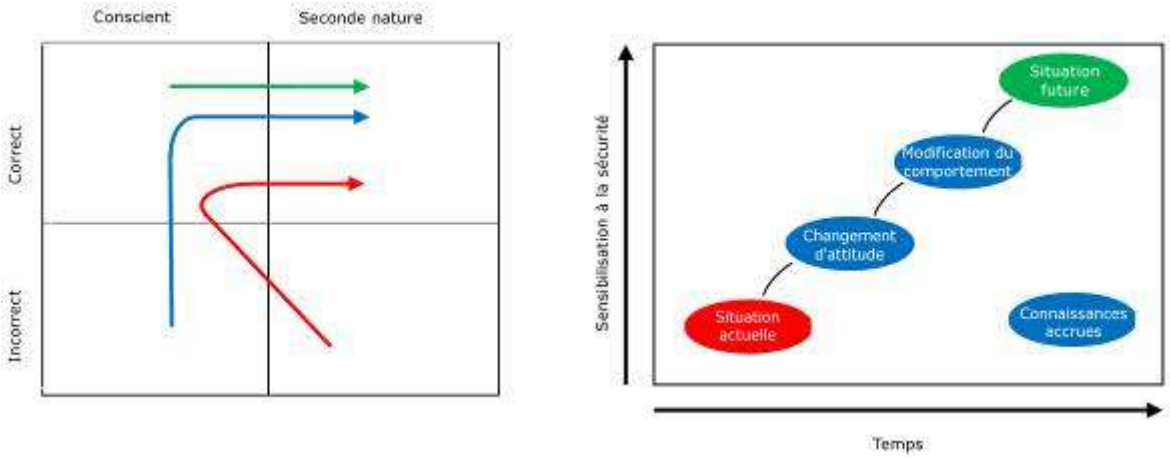

Figure 3: – La sécurité de l'information comme une seconde nature.

La formation est l'une des composantes «Comment» de la mise en œuvre de la sécurité de l'information. Un programme de formation doit être conçu et élaboré en fonction des objectifs d'apprentissage fixés par l'organisme. La formation vise donc à enseigner des compétences permettant d'exécuter une fonction spécifique, tandis que la sensibilisation a pour but d'attirer l'attention sur un ou plusieurs problèmes. Les compétences acquises au cours de la formation sont basées sur les fondations posées durant la phase de sensibilisation et surtout sur les principes de bases de la sécurité de l'information et les supports d'enseignement de base([10]).

Les programmes de sensibilisation commencent par une sensibilisation, passent ensuite à la formation, avant de terminer par l'éducation. Ils doivent être personnalisés en fonction du public spécifique ciblé. Il sera donc très important de pouvoir définir les utilisateurs qui assisteront aux deux programmes. Différentes méthodes peuvent être utilisées pour définir le public cible. L'ENISA a élaboré un instrument simple permettant de mieux identifier un groupe cible et de capter les données le concernant, tel que décrit à la section «Définir le groupe cible» ([11]).

([10]) NIST, *Information technology security training requirements: A role- and performance-based model* [Exigences de formation en matière de sécurité des technologies de l'information: modèle axé sur les performances et les rôles], NIST — SP 800-16, États-Unis, 1998, consultable à l'adresse suivante: http://csrc.nist.gov/publications/nistpubs/800-16/800-16.pdf (dernière visite le 21 juillet 2008).

([11]) Herold, Rebecca, *Information security and privacy awareness program* [Programme de sensibilisation à la sécurité de l'information et au respect de son caractère privé], Auerbach Publications, États-Unis, 2005 (en anglais); NIST, *Building an information technology security awareness program* [Élaborer un programme de sensibilisation à la sécurité des technologies de l'information], NIST — SP800-50, NIST, 2003, consultable en anglais à l'adresse suivante: http://csrc.nist.gov/publications/nistpubs/800-50/NIST-SP800-50.pdf (dernière visite le 17 juillet 2008).

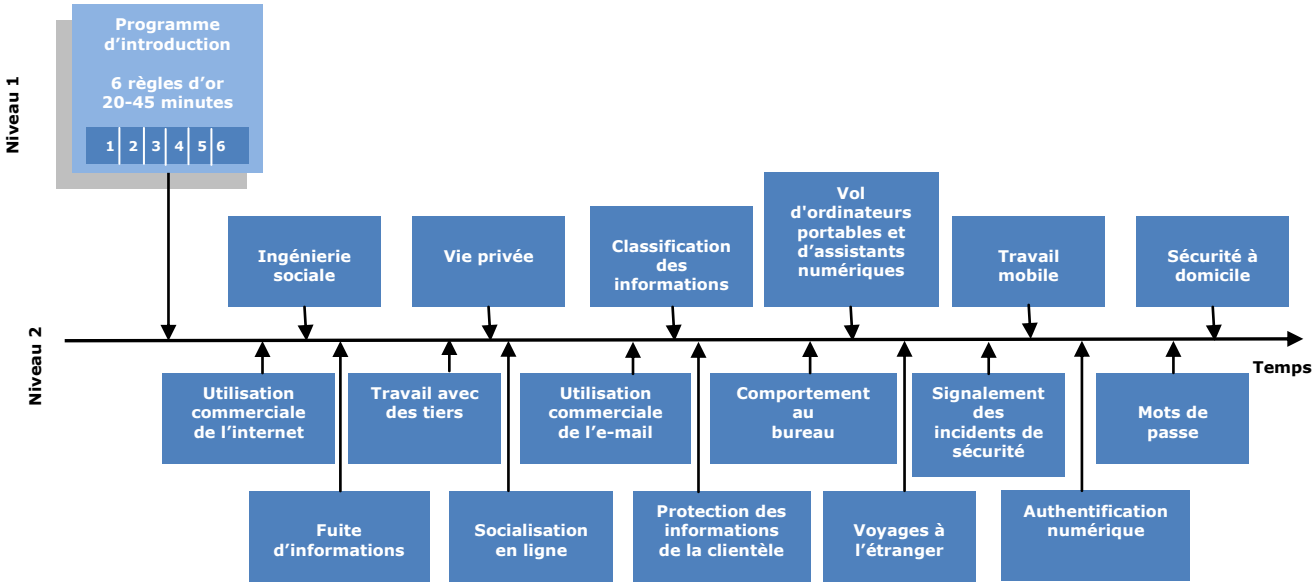

Figure 4: Illustration d'un programme de sensibilisation permanent.

Modularité

La question de la modularité est fondamentale pour parvenir à atteindre un public mondial en pleine croissance. Elle peut encourager davantage l'adoption d'une approche modulaire de la sensibilisation (segmentation du public et du message).

Langues

Faire passer un message aux gens et s'assurer qu'ils le comprennent comporte un autre défi. Le langage commercial formel d'une entreprise n'est pas toujours suffisant et n'est pas toujours compris par tous les employés. L'organisation d'un atelier et l'élaboration du contenu d'un apprentissage en ligne sont donc plus efficaces dans la langue locale. Il est donc très important de tenir compte du fait qu'il puisse exister plusieurs langues au sein d'une même zone géographique. Il convient de tenir compte des éléments suivants:

- ✓ différentes langues dans un même pays
  - un pays – plusieurs langues
- ✓ différentes langues dans différents pays
  - activités internationales
- ✓ langue d'entreprise
- ✓ différentes variantes d'une même langue
  - par exemple, anglais commercial/anglais courant

Assureur international: l'engagement de la direction fait toute la différence

Une compagnie d'assurances nous a expliqué pourquoi la sécurité de l'information était importante pour ses activités. La compagnie collecte, stocke et traite de grandes quantités d'informations financières, médicales et personnelles. Ces informations sont son actif le plus précieux: une violation de la confidentialité pourrait nuire à sa réputation et l'exposer à des poursuites judiciaires dommageables. Malheureusement, les menaces (telles que le vol d'identité et l'escroquerie) sont en pleine expansion, ce qui rend cruciale la sensibilisation du personnel.

Le défi majeur a été de mettre au point une approche adaptée aux quelque 10 000 employés parlant de nombreuses langues différentes. Pour parer à ce problème, la société a engagé un fournisseur externe pour l'aider à concevoir des programmes et supports de formation adaptés. Afin de maximiser leur impact sur le personnel, les supports de formation ont été traduits dans les langues officielles locales des pays concernés.

Un programme permanent vise à ajuster et à promouvoir les messages clés, l'objectif étant d'essayer de modifier les comportements des employés ainsi que leur perception du risque. Les mécanismes d'apprentissage différant selon les personnes, de nombreuses techniques sont utilisées pour atteindre le public.

La plus efficace d'entre elles s'est révélée être le contact direct avec le personnel lors d'ateliers et de séances de formation. Il est plus convivial de pouvoir mettre un visage sur un nom ou une fonction et les employés sont plus réceptifs aux messages lorsqu'ils sont passés de vive voix. La formation est obligatoire. La direction soutient activement les programmes de sensibilisation, en s'assurant que les horaires des séances de formation sont adaptés aux activités et en les promouvant auprès du personnel. Le taux de participation aux séances est satisfaisant car toute absence est signalée au supérieur de l'employé. Ce soutien de la direction dans toute l'entreprise est un facteur déterminant de la réussite du programme de sensibilisation.

D'autres mécanismes non interactifs, tels que des articles sur l'intranet, des e-mails, des affiches et des publications, sont utilisés pour renforcer les messages importants. Il s'est toutefois révélé difficile d'évaluer le nombre de personnes ayant lu ou compris ces messages; par ailleurs, les gens peuvent facilement les ignorer. Ils servent donc plus de complément que de substitut à la formation en classe.

Les principaux instruments de mesure de l'impact de la formation de sensibilisation sont le retour d'informations et les questionnaires remplis lors de la séance ou peu après. Ce retour d'informations permet d'apprécier correctement l'impact de la formation sur l'employé. L'impact a généralement été positif: la grande majorité des employés déclarent en avoir retiré de nouveaux enseignements et s'engagent à essayer de modifier leurs comportements.

D'autres moyens d'évaluation de la sensibilisation ont été envisagés, notamment la vérification de la complexité des mots de passe ou la simulation de situations d'ingénierie sociale afin d'évaluer les réactions. Ces moyens ne sont toutefois pas utilisés en raison des inquiétudes sur leur dépendance à d'autres variables (telles que l'humeur de la personne), sur le respect de la vie privée et sur la possibilité qu'ils donnent lieu à des cas de piégeage.

La compagnie cherche maintenant à garantir que la formation continue à mobiliser les employés; des modules d'apprentissage en ligne sont en cours de développement afin de varier les formats. Un processus continu est également en cours afin d'améliorer la pertinence des supports pour le personnel, pour qu'il puisse constater les bénéfices et mieux comprendre les risques.

PARTIE 2: PROGRAMMES DE SENSIBILISATION

Programmes de sensibilisation

Sensibiliser le public à la sécurité de l'information n'est pas une question qui se règle une fois pour toutes. Un programme de sensibilisation ne peut pas non plus être utilisé éternellement dans un organisme sans faire l'objet de nouvelles mesures ou de modifications. Afin de s'assurer que le programme reste adapté aux objectifs d'un organisme financier et que la sécurité de l'information est intégrée à la culture organisationnelle, la sensibilisation doit être continue ou rappelée en permanence. Il s'agit d'un processus permanent, d'un cycle d'analyse et de changement, tel que nous en trouvons dans bon nombre de systèmes de gestion de la qualité, comme par exemple les normes ISO 9001 ou ISO/IEC 27001. «Il est crucial d'adopter une [telle] approche de gestion du changement pour une initiative de sensibilisation, étant donné que ceci contribue à établir le lien entre un problème particulier et les réactions humaines au besoin de changement, même dans le cas d'un changement culturel»([12]).

La première étape consiste à analyser la sensibilisation et la culture actuelles en matière de sécurité de l'information et d'identifier les principaux facteurs commerciaux. Si la culture ne correspond pas aux objectifs de l'organisme, il faut alors la modifier. Si, au contraire, elle correspond, il conviendra de la renforcer. Les contrôles nécessaires, comme par exemple un programme de formation à la sécurité de l'information ou une campagne de sensibilisation, doivent être déterminés (planification et conception) et réalisés (mise en œuvre). Le succès des mesures choisies doit alors être évalué et les apprentissages doivent être spécifiés (en mesurant l'amélioration et le succès du programme). Ce processus est illustré à la figure 5.

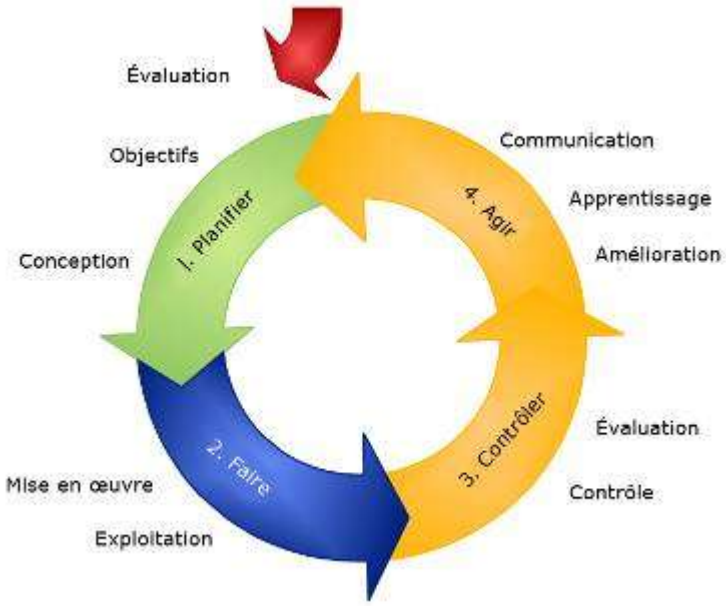

Figure 5: Stratégie globale d'amélioration de la sensibilisation à la sécurité de l'information dans les organismes financiers.

([12]) ENISA, *Un Guide Utilisateur: Comment améliorer la sensibilisation à la sécurité de l'information*, 2008, consultable à l'adresse suivante: http://www.enisa.europa.eu/doc/pdf/deliverables/WGAR/guide_fr.pdf

Évaluation

La nécessité d'une sensibilisation à la sécurité de l'information est largement reconnue. Afin de contribuer d'une manière substantielle au domaine de la sécurité de l'information et de choisir les contrôles adéquats, il est nécessaire de disposer d'une série de méthodes d'analyse. Bien que la sensibilisation et la culture de la sécurité de l'information puissent être mesurées, peu d'organismes financiers ont cherché à quantifier la valeur des programmes de sensibilisation.

Selon Gartner, il existe quatre grandes catégories par rapport auxquelles la sensibilisation à la sécurité de l'information peut être évaluée([13]):

1. Amélioration du processus (élaboration, diffusion et mise en œuvre des lignes directrices recommandées en matière de sécurité de l'information ainsi que formation de sensibilisation),
2. Résistance aux attaques (identification d'un cas d'atteinte à la sécurité de l'information et résistance à une attaque),
3. Compétence et efficacité (compétence et efficacité en cas d'incidents de sécurité de l'information),
4. Protection interne (qualité de la protection d'une personne contre des menaces potentielles).

Dans la pratique, une large gamme d'instruments ciblant ces quatre catégories sont actuellement utilisés pour évaluer la sensibilisation à la sécurité de l'information, mais il n'y a que peu de consensus au sujet des mesures les plus efficaces.

Selon une enquête de l'ENISA, la source d'informations la plus populaire sur les comportements réels est l'audit interne ou externe([14]). Cette enquête indique que bon nombre de participants se servent de leur expérience des incidents de sécurité de l'information comme outil de mesure. Assez peu de participants trouvent utiles les mesures à l'entrée (telles que par exemple le nombre de visiteurs du site intranet ou le nombre de prospectus distribués). Les mesures de ce type les plus utilisées sont le nombre d'employés bénéficiant d'une formation et le retour d'informations qualitatives sur le programme fourni par le personnel. Environ un tiers des participants utilisaient toutes ces mesures.

Au regard de la facilité avec laquelle on peut obtenir des mesures de l'amélioration du processus, peu de participants utilisent ces dernières. Les organismes semblent également éprouver beaucoup de difficultés à mettre en place des instruments de mesure quantitatifs. Par exemple, un tiers des participants seulement incluent des questions sur la sensibilisation à la sécurité de l'information dans les enquêtes qu'ils réalisent auprès de leur personnel. Ils mesurent alors les niveaux de sensibilisation avant et après la mise en œuvre des initiatives. Les participants suivant cette approche quantitative soulignent qu'ils rencontrent des problèmes dus à la complexité de la tâche de collecte et de traitement des données. Avec un questionnaire soigneusement élaboré et testé, une enquête réalisée auprès du personnel sur la sensibilisation à la sécurité de l'information permet de mieux comprendre les facteurs incitant à adopter un comportement prudent, notamment le comportement de la direction, le savoir-faire, l'attitude et la motivation. Certaines études de cas donnent d'excellents résultats sur la base des enquêtes utilisées dans les instituts financiers([15]).

([13]) ENISA, *Information security awareness initiatives: Current practice and the measurement of success, 2007* [Initiatives de sensibilisation à la sécurité de l'information: pratiques actuelles et quantification de leur succès], consultable en anglais à l'adresse suivante: http://www.enisa.europa.eu/doc/pdf/deliverables/enisa_measuring_awareness.pdf

([14]) ENISA, *Information security awareness initiatives: Current practice and the measurement of success, 2007* [Initiatives de sensibilisation à la sécurité de l'information: pratiques actuelles et quantification de leur succès], consultable en anglais à l'adresse suivante: *http://www.enisa.europa.eu/doc/pdf/deliverables/enisa_measuring_awareness.pdf*

([15]) Schlienger, T. and S. Teufel, *Tool supported Management of Information Security Culture: An application to a Private Bank*, [Gestion instrumentalisée de la culture de la sécurité de l'information: application à une banque

Vu la difficulté de prendre en considération toute la palette des comportements humains et des cultures, l'utilisation d'une combinaison d'outils et de méthodes de mesure, tel que le proposent les experts de la culture organisationnelle, semble conseillée. Il serait ainsi possible de vérifier les résultats obtenus par d'autres méthodes. Les organismes financiers pourront ainsi opter pour les méthodes les plus appropriées pour évaluer leur culture de sécurité de l'information.

Un cadre d'analyse rationnel permet à l'organisme financier d'analyser de manière systématique sa culture de sécurité de l'information, d'identifier rapidement d'éventuelles lacunes et les mesures d'amélioration à entreprendre ainsi que de prouver les progrès accomplis lorsqu'il améliore sa culture de sécurité de l'information.

Phases de planification et de conception

Plusieurs facteurs doivent être pris en considération lors de la planification d'un programme de sensibilisation à la sécurité de l'information. Dans la présente section, nous allons examiner les questions les plus importantes, déterminer ce qui fait leur importance et étudier les différentes manières de les aborder.

Approbation du conseil de direction

Le facteur de réussite le plus déterminant dans n'importe quel projet mis en œuvre à l'échelle de l'organisation est la mobilisation de la direction. Il s'agit là de l'un des moteurs les plus puissants dans tout organisme, compte tenu du fait que le soutien de la direction permet non seulement un financement, mais donne également l'exemple à tous les niveaux de l'organisme.

Le conseil de direction doit donc désigner une personne chargée de soutenir officiellement le programme dans tout l'organisme. Ce soutien permettra aux employés de constater que le programme fait partie de la stratégie de l'organisme et garantira également un alignement à tous les niveaux de l'entreprise.

privée], The 20th IFIP International Information Security Conference (SEC 2005) - Security and Privacy in the Age of Ubiquitous Computing [Sécurité et vie privée à l'ère de l'informatique omniprésente], Makuhari Messe, Chiba, JAPON, Kluwer Academic Press, 2007.

Identifier les facteurs

Le but principal de cette activité est de comprendre exactement pourquoi l'organisme financier a besoin d'un programme de sensibilisation. Il est important de citer les raisons qui motivent l'existence d'un programme, de manière à le rendre plus efficace.

Parmi les raisons les plus récentes justifiant le lancement d'un programme de sensibilisation à la sécurité de l'information, citons les contrôles imposés dans ce domaine par certaines réglementations telles que la loi SOX, les normes de Bâle II et d'autres lois nationales sur le respect de la vie privée.

Le programme peut également faire partie de la stratégie propre à l'organisme: plusieurs organismes cherchent actuellement à atteindre des objectifs de certification, tels que la norme ISO/IEC 27001 pour la gestion de la sécurité de l'information ou la norme BS25999 pour la gestion de la continuité des activités, qui supposent un grand engagement de la part de chaque employé.

Certains cadres de contrôles tels que le CobiT soulignent également la nécessité d'une formation et d'une sensibilisation des utilisateurs.

Parmi d'autres raisons potentielles du lancement d'un programme de sensibilisation, citons l'évolution des politiques de l'institution, la mise en œuvre de nouveaux systèmes, le savoir-faire des employés, les valeurs de l'entreprise, les conclusions des audits, les résultats des analyses de risques, etc.

Organisation financière internationale: un programme de sensibilisation à la sécurité de l'information pour tout le personnel

Une organisation financière internationale particulièrement influente à travers l'Europe a décidé de mettre en œuvre un programme de sensibilisation à la sécurité de l'information pour l'ensemble de son personnel. Le but était de l'informer sur les sept principales règles de sécurité à observer.

Afin de prouver la mobilisation de la direction, il a été décidé de réaliser un film mettant en scène le chef de l'organisation. Ce film est un message directement adressé à l'ensemble du personnel pour l'informer des différentes menaces de sécurité et des conséquences potentielles de celles-ci si le personnel n'intègre pas à son quotidien la sécurité de l'information. Dans ce film, le directeur souligne aussi très clairement qu'il suivra lui-même cet atelier et qu'il compte sur ses employés pour faire de leur mieux pour collaborer à cette initiative. Il s'agit là d'un message très fort transmis par la direction à l'ensemble du personnel à tous les niveaux de l'organisation.

L'utilisation de diverses méthodes d'apprentissage a également été jugée essentielle pour la réussite du programme de sensibilisation. On a donc opté pour un programme de sensibilisation comportant des séquences vidéo révélatrices, du matériel d'apprentissage et des questionnaires d'autoévaluation dans le but de rendre le programme plus intéressant et de montrer des exemples concrets de la manière dont peuvent se produire les incidents de sécurité.

Il a été décidé de commencer par mettre en œuvre le programme de sensibilisation dans des ateliers par service, en utilisant une approche directe pour s'adresser aux employés eux-mêmes et pour favoriser la discussion. Le programme de ces ateliers a été agrémenté d'une version en ligne pour les employés ne pouvant pas y participer ainsi que pour tous les nouveaux employés de l'organisation. Le lancement de plans d'action locaux dans le cadre de ces ateliers a servi à inciter le personnel à s'engager à mettre en pratique les principes de sécurité de l'information sur le lieu de travail.

Les résultats des autoévaluations sont enregistrés et un système d'information de gestion est disponible pour indiquer la participation globale et les scores moyens obtenus. Il a été décidé de ne pas évaluer les résultats individuels pour éviter les problèmes concernant la protection de la vie privée dans les différents pays.

Il est important de garder à l'esprit que les différents départements de l'organisme ont des besoins différents. Le responsable du programme doit rencontrer la direction pour déterminer quel type d'informations ses employés doivent recevoir concernant la sécurité de l'information. Par exemple, si les employés ne sont pas au courant de la politique de sécurité de l'information menée par l'organisme, la première mission du programme sera de les en informer.

Les facteurs doivent être intégrés au programme de sorte que les raisons pour lesquelles l'organisme investit des ressources dans ce projet soient généralement bien comprises.

Identifier les exigences et les besoins

Différents types d'exigences, de besoins et de contraintes doivent être identifiés avant de passer à l'élaboration du programme.

Banque privée internationale suisse: évaluation de la culture de la sécurité de l'information et programme de sensibilisation

La sécurité de l'information (SI) est une question importante pour les banques privées. Un certain nombre de mesures, telles que l'information du personnel et des prospectus sur le rangement du bureau, ont été et sont toujours mises en œuvre afin d'assurer et de renforcer la sécurité de l'information. Toutefois, afin de garantir le maintien du niveau de sécurité requis, les formations du personnel sont une partie fondamentale de ce processus.

La direction a demandé qu'on lui suggère des mesures pouvant être adoptées pour mettre en œuvre un programme de sensibilisation à la sécurité et sollicite l'aide de son personnel dans le cadre d'un déploiement du programme à l'échelle de l'entreprise.

La culture de la sécurité de l'information a tout d'abord été évaluée au moyen d'une enquête quantitative auprès du personnel. Différentes sous-cultures ont été identifiées et ce, en raison d'une fusion qui a abouti à la création d'une seule société.
Ensuite, des mesures correctives ont été définies afin de renforcer le niveau de maturité de la sensibilisation à la SI. Ces mesures ont été mises en œuvre dans le cadre d'un programme mondial de sensibilisation.

Ce programme mondial de sensibilisation à la SI comprenait notamment:

- ✓ un film du PDG affirmant l'engagement de la direction envers le programme de SI;
- ✓ la définition de six règles d'or en matière de sécurité;
- ✓ un programme d'apprentissage en ligne comprenant un test;
- ✓ des ateliers de gestion;
- ✓ des supports promotionnels de sensibilisation à la SI, tels que des affiches et des prospectus pour tout le personnel partout dans le monde;
- ✓ une présence renforcée de la sensibilisation à la SI sur l'intranet.

Deux facteurs étaient essentiels à la mise en œuvre réussie de ce programme de sensibilisation à la SI: premièrement, les personnes clés des départements Marketing & Communications et Ressources humaines devaient faire partie de l'équipe de projet; deuxièmement, il fallait un engagement total des membres du conseil d'administration. Ces deux facteurs étaient en effet primordiaux pour la réussite du programme de sensibilisation à la SI. Un autre élément important, par ailleurs, a été l'utilisation d'une enseigne unique pour la sensibilisation à la SI. Une enseigne unique a été créée pour toutes les mesures de communication: programme d'apprentissage en ligne, affiches, prospectus, ateliers de gestion et portail intranet. Cette enseigne prenait la forme d'une photo créée en collaboration active avec les employés. Cette solution a véritablement permis de capter l'attention: elle représentait parfaitement le programme tout en améliorant la sensibilisation au projet. Le programme a ainsi été très bien accueilli par le personnel.

Dans le cadre d'une prochaine étape, la banque prévoit d'évaluer les résultats du programme de sensibilisation à la SI en adoptant une autre approche d'évaluation quantitative. Un processus de gestion de la sensibilisation à la SI va également être mis en œuvre afin d'optimiser en permanence le niveau de sensibilisation à la SI au sein de la banque.

En fonction de la taille de l'institution, les gestionnaires de projet peuvent être amenés à envisager divers détails géographiques et culturels, tels que par exemple, d'une part, les lois et les langues spécifiques à chaque pays et, d'autre part, les valeurs culturelles.

Les exigences et contraintes relatives aux utilisateurs finals doivent être identifiées et interconnectées afin de concevoir un programme de formation plus efficace et conforme aux objectifs de l'institution. Tous ces éléments devront être validés par le département des ressources humaines.

Le budget et les ressources nécessaires doivent également être déterminés; les coûts diffèrent selon les supports et méthodes choisis et l'organisme pourrait souhaiter investir dans différentes ressources pour différentes méthodes de sensibilisation.

Une autre disposition susceptible d'influer sur la planification ou le contenu du programme est celle relative aux exigences des règlementations et des normes. Par exemple, si l'organisme entend obtenir une certification au titre de la norme ISO/IEC 27001, il y a lieu de tenir compte de deux facteurs clés concernant le calendrier et le type de formation choisi. Premièrement, les nouveaux membres du personnel doivent comprendre les politiques et attentes de l'organisme en matière de sécurité de l'information avant d'être autorisés à utiliser les services ou à accéder aux informations de l'organisme; deuxièmement, il est nécessaire d'assurer des programmes de formation continue pour garantir que le personnel se maintienne au courant des contrôles effectués par l'organisme en matière de sécurité de l'information.

Concevoir le programme

Une fois que les facteurs influençant et affectant la conception du programme ont été identifiés, il est temps de passer à la construction du programme proprement dite.

À ce stade, et sur la base des besoins en formation et en éducation qui ont

Groupe de services financiers: réduire le poids des formations pour le personnel

Une grande entreprise de services financiers a expliqué qu'elle accordait une importance particulière à la sensibilisation à la sécurité de l'information. Celle-ci fait partie du programme du conseil d'administration, car elle est jugée importante pour conserver la confiance des clients.

L'un des défis à relever concerne le pourcentage élevé d'employés à temps partiel et de sous-traitants. Un autre concerne le poids actuel des formations obligatoires imposées au personnel (lutte contre le blanchiment d'argent, protection des données, lutte contre la fraude, etc.) Il s'est donc révélé essentiel de pouvoir associer la formation de sensibilisation à la sécurité de l'information à d'autres activités de formation pratique. L'entreprise vient de restructurer son département de sécurité afin de rassembler la sécurité physique, la sécurité de l'information et la prévention de la fraude. Les grandes questions de sensibilisation détachées de chacun de ces aspects sont combinées et traitées au sein d'une seule série de messages de formation.

Le personnel fait preuve d'une bonne compréhension de certaines questions de sécurité, comme par exemple celles relatives à l'e-mail et aux appareils mobiles (téléphones, ordinateurs portables, etc.). Faire passer des messages dans d'autres domaines (tels que les menaces liées à l'internet et la messagerie instantanée) s'est toutefois révélé plus difficile. La formation de sensibilisation décrit clairement les responsabilités personnelles de chaque employé en matière de sécurité de l'information. Des orientations sont ensuite proposées au sujet des bonnes pratiques à adopter pour assumer ses responsabilités.

Les activités de l'entreprise exigent que les formations soient disponibles conformément aux besoins et de manière rentable. Pour ce faire, on cherche à mettre en œuvre des activités de sensibilisation à la sécurité par le biais de systèmes en ligne et d'autoformations. Il est désormais obligatoire de suivre une formation assistée par ordinateur (FAO). Les quiz proposés dans cette formation fournissent des statistiques mesurant le degré de sensibilisation et la FAO elle-même enregistre les progrès de la formation du personnel. La rapidité, la facilité d'utilisation et la cohérence du programme de formation en ligne sont considérées comme des avantages majeurs. Si sa mise en œuvre a nécessité un certain investissement, la rentabilité de la formation dispensée a permis de maximiser le retour sur investissement.

D'autres mesures qui se sont révélées utiles pour évaluer la sensibilisation du personnel sont le nombre d'appareils mobiles égarés et le nombre de problèmes et d'incidents de sécurité signalés.

Le contenu de la FAO est révisé en permanence de manière à prendre en considération les risques émergents et le personnel continue à en tirer des bénéfices. La prochaine étape consistera à cibler les groupes à haut risque afin de leur dispenser une formation directe de sensibilisation à la sécurité.

été identifiés, il y a lieu de déterminer les éléments suivants:

- ✓ les groupes cibles et leurs membres; citons par exemple le conseil d'administration, la direction, la/les équipe(s) de gestion des risques opérationnels, les équipes IT, les employés par rôle, etc.;
- ✓ les mécanismes efficaces pour dispenser la formation: par exemple la formation assistée par ordinateur, la formation en classe, les supports via l'intranet, les affiches, etc.;
- ✓ les horaires; si le projet comprend différentes phases, il est très important de prévoir exactement quand chacune d'entre elles commence et combien de temps elles vont durer, de manière à éviter que les employés ne subissent une surcharge d'informations et à maintenir l'impact du programme.
- ✓ les évaluations des performances des séances et le benchmarking; afin d'évaluer l'efficacité du programme, il conviendra de définir à ce stade une mesure permettant de contrôler l'efficacité de la formation et d'établir un rapport à ce sujet. Une méthode pour y parvenir est de réaliser une enquête avant et après les séances de formation.
- ✓ Mesures d'évaluation du contenu, de la qualité, de l'efficacité, du coût et de la valeur de la formation. Ces mesures permettront de définir les prochains programmes de formation.

Contrôler la conception

Une fois terminée l'élaboration du programme de sensibilisation à la sécurité de l'information, il est temps de le soumettre au conseil d'administration et à la direction pour qu'ils le contrôlent et l'approuvent définitivement.

Il convient à ce stade de veiller spécifiquement à ce que les objectifs du programme soient directement associés aux objectifs de l'organisation et à les soutenir de manière explicite.

Phase de mise en œuvre

La présente section s'attache à décrire comment mettre en œuvre une campagne de sensibilisation réussie et envisage les aspects suivants:

- ✓ développement d'une plateforme de prestation;
- ✓ allocation des ressources du projet;
- ✓ planification et exécution de la mise en œuvre.

Développement d'une plateforme de prestation

L'un des défis majeurs que présente tout projet de formation sur la sécurité de l'information est le déploiement, l'administration et la gestion des différentes solutions d'apprentissage qui constitueront finalement le programme de sensibilisation dans son ensemble.

La plupart des organismes désireux de déployer des solutions de sensibilisation complètes et permanentes optent pour un système de gestion de l'apprentissage (SGA). Ces systèmes permettent

- ✓ de contrôler l'utilisation l'apprentissage en ligne par les employés en enregistrant leurs progrès, leurs taux d'achèvement et d'autres données sur les performances telles que les résultats des tests.
- ✓ d'élaborer une série de rapports de gestion accessibles aux administrateurs et aux directeurs au niveau central et régional.
- ✓ d'importer et d'exporter les données de et vers les autres applications (par exemple le système des RH);
- ✓ de permettre d'établir le profil de l'utilisateur pour que différents contenus puissent être attribués aux utilisateurs en fonction de caractéristiques prédéfinies (telles que par exemple la fonction et/ou la langue préférée).
- ✓ de gérer le déploiement de solutions d'apprentissage dans toute l'entreprise afin de minimiser leur impact sur les ressources commerciales et de réseau.

Un système de gestion de l'apprentissage permet à l'organisme de proposer toute une gamme de solutions de sensibilisation à une variété de publics cibles tout en permettant à l'administrateur du système de contrôler les taux d'utilisation et d'achèvement et d'attribuer un contenu à chacun sur la base, par exemple, de sa fonction ou de son département. Ces systèmes sont conçus spécifiquement dans ce but et sont particulièrement efficaces pour la mise en œuvre d'initiatives de sensibilisation vastes, complexes et permanentes.

Bien que les personnes puissent participer de leur propre gré à la plupart des SGA, le système donne ses meilleurs résultats lorsque la base de données est remplie à l'avance avec les données adéquates des participants. Le remplissage à l'avance de la base de données permet notamment à l'administrateur de contrôler l'attribution de supports d'apprentissages aux groupes prédéfinis d'étudiants et de gérer ainsi soigneusement la mise en œuvre des programmes. De plus, grâce au remplissage à l'avance de la base de données, le suivi et l'établissement de rapports (surtout sur les étudiants qui se sont vu attribuer un programme, mais qui ne l'ont pas suivi jusqu'au bout) sont bien plus faciles.

Allocation des ressources du projet

Une répartition correcte des ressources aux vastes initiatives de sensibilisation à la sécurité de l'information est essentielle pour leur réussite. Le tableau ci-dessous décrit quelques-uns des principaux rôles et responsabilités habituellement requis pour l'achèvement d'un projet de cette nature.

Rôle	Tâches	Engagement
Gestionnaire de projet	✓ Contrôle l'évolution par rapport au plan. ✓ Coordonne les ressources internes. ✓ Gère la relation avec les fournisseurs.	Impliqué d'un bout à l'autre du projet - participe aux réunions régulières sur l'avancement.
Expert thématique	✓ Valide l'approche globale du contenu du programme de sensibilisation. ✓ Approuve le contenu.	Participe dès le début du programme à la définition des attentes et à l'examen du contenu. Ensuite, contacte occasionnellement les concepteurs et développeurs de la formation pour entretenir le lien et identifier tout développement futur requis.
Administrateur du SGA	✓ Gère le SGA. ✓ Génère des informations et des rapports de gestion.	Le temps consacré par l'administrateur du SGA à ces tâches dépend de la fréquence à laquelle des changements doivent être apportés à la configuration du système et quelles sont les exigences en matière de Gi et de déclaration.
Service d'assistance IT	✓ Fournit une assistance aux utilisateurs après le déploiement du programme.	Le service d'assistance doit assurer le soutien des utilisateurs pendant le déroulement du SGA et de tout programme d'apprentissage en ligne dans le cadre de ses tâches habituelles.

		Il peut être utile de proposer au personnel du service d'assistance une courte séance de formation pendant la mise en œuvre.
Corporate Communications	✓ Fournit soutien et conseils sur les questions relatives au marketing interne, à la marque, etc.	Impliqué dans les premières phases de chaque produit pour en approuver l'identité visuelle, les styles, etc. Peut aider à planifier et à mettre en œuvre les campagnes de marketing internes visant à sensibiliser à l'initiative de formation.
Représentants des secteurs d'activités	✓ Assurent la liaison avec les grands secteurs d'activité.	Impliqués dans le soutien et la promotion de la campagne de communication interne et dans la stratégie de déploiement. Peuvent également être impliqués dans les tests et expérimentations de l'acceptation par l'utilisateur des outils d'apprentissage afin de s'assurer de la participation d'activités spécifiques.
Représentant IT et/ou RH	✓ Sert d'interface avec les systèmes RH pour le remplissage à l'avance de la base de données du SGA.	Impliqué dans la création initiale et le remplissage préalable de la base de données du SGA ainsi que dans les mises à jour ultérieures du système pour les personnes qui le rejoignent, qui le quittent ou qui changent d'orientation.

Figure 6: Rôles et responsabilités clés. À titre illustratif seulement.

Planification et exécution du déploiement

Il convient de prendre en considération plusieurs facteurs clés lors de la planification du déploiement d'un programme complet de sensibilisation:

- ✓ Le plan de déploiement doit inclure une expérimentation de tous les supports avant le lancement du programme. Les programmes pilotes doivent tester l'efficacité du contenu des outils d'apprentissage d'un point de vue formatif. Lors de la mise en place d'une formation assistée par ordinateur, il est important de penser à la tester du point de vue technique afin de s'assurer qu'elle fonctionne correctement dans tous les environnements commerciaux proposés.
- ✓ Lorsqu'un système de gestion de l'apprentissage est utilisé pour gérer tout ou une partie du déploiement, il convient de prévoir suffisamment de temps pour s'assurer que toutes les données des étudiants y sont incluses et que des e-mails d'invitation et de rappel ont été rédigés, testés et approuvés. Les risques d'échec du déploiement sont importants lorsque les étudiants rencontrent des difficultés pour accéder au contenu via le SGA ou lorsque les invitations par e-mail ne sont pas assez claires ou pas assez informatives.
- ✓ Un déploiement progressif (sauf en cas d'urgence) est généralement préférable à une approche du «big bang» car:
  - il minimise l'impact de la formation assistée par ordinateur sur les ressources du réseau;
  - il minimise l'impact sur les activités courantes de l'organisme;

- il permet d'identifier et de traiter les problèmes de manière continue, afin d'assurer qu'ils ne soient pas rencontrés par une large part de la population ciblée;

✓ Le déploiement doit accorder la priorité aux domaines d'activité considérés comme «à haut risque» du point de vue de la sécurité de l'information.

✓ Dans les organismes internationaux, il convient de prendre en considération la nécessité de prévoir différentes versions linguistiques d'un même contenu de formation. Idéalement, la stratégie de déploiement permettrait de réaliser entièrement et d'expérimenter une version linguistique «de base» (généralement la principale langue de travail de l'organisme) avant l'élaboration d'autres versions linguistiques. Cette approche garantit l'harmonisation et la cohérence des différentes versions linguistiques et minimise les coûts de gestion, les coûts administratifs et les coûts financiers qu'entraînerait un maintien de plusieurs versions linguistiques au cours de la phase de développement.

✓ Le déploiement doit être planifié en tenant compte des autres évènements connus au sein de l'entreprise (par exemple les grandes initiatives de formation, les lancements de produits, la fin de l'exercice financier, etc.) de manière à minimiser la concurrence entre eux pour attirer l'attention des publics ciblés. Consulter les départements Apprentissage & Développement, Ressources humaines et Communication interne permet souvent d'obtenir des informations très utiles sur d'autres initiatives.

- L'adhésion visible des directeurs des entités aux buts et objectifs du programme de sensibilisation est un facteur de réussite primordial. Toute initiative de sensibilisation doit donc commencer par des évènements (présentations, briefings, etc.) visant à mobiliser l'attention et à s'assurer du soutien actif des cadres supérieurs. La plupart des grands organismes adoptent une approche en cascade en ce qui concerne les communications de la direction et fournissent aux membres de celle-ci des kits de présentation («meetings in a box») pour qu'ils puissent faire passer le message le long des différents échelons de la ligne hiérarchique.

Banque universelle: développer une formation de sécurité et une campagne de sensibilisation à l'échelle de l'entreprise couvrant à la fois les utilisateurs généraux et les spécialistes techniques

Ce projet, pour une institution financière internationale, a été conçu afin d'opérer un changement radical dans la formation à la sécurité de l'information et dans la sensibilisation au niveau de l'entreprise toute entière. Avec 50 000 employés dans plus d'une douzaine de pays, il fallait arriver à atteindre l'ensemble du personnel et à dispenser une formation personnalisée répondant aux spécificités des différentes fonctions et responsabilités.

Après une phase de consultance intensive, une solution en trois étapes a été recommandée. Celle-ci comprenait une formation générale à la sécurité de l'information à l'intention du personnel non technique, avec une formation parallèle destinée aux directeurs et aux cadres. Cette solution a été proposée dans plusieurs langues par le biais d'un système de gestion de l'apprentissage et s'accompagnait d'outils d'évaluation et d'un programme de remise à niveau.

Par ailleurs, une série détaillée d'ateliers et de supports a été élaborée pour les employés techniques et de sécurité. Cette série comprend un programme de base couvrant le développement sécurisé d'applications, les contrôles de l'accès et la gestion des intrusions pour les développeurs, les architectes techniques et les gestionnaires de systèmes. Ces activités ont été mises en œuvre dans plusieurs régions du monde mais en utilisant des supports spécifiques selon les fonctions et les responsabilités. Ces initiatives de formation ont été associées à une campagne globale de marketing interne. Parmi les produits élaborés, citons une campagne détaillée de communication avec slogans, lettres d'information, présentations «en kit», briefings analytiques ainsi qu'un portail rénové sur la sécurité de l'information pour l'entreprise.

Résultat...
Moins de vulnérabilité et plus de sensibilisation sur les questions essentielles en matière de sécurité et sur les responsabilités dans l'entreprise.

- Il arrive souvent que des outils d'apprentissage de grande qualité n'aient que peu d'impact sur les organismes faute d'actions de marketing interne et de relations publiques. La sécurité de l'information n'est pas un sujet ayant intrinsèquement de l'importance pour de nombreux employés. Pourtant, leur adhésion aux messages clés d'une campagne de sensibilisation est essentielle pour obtenir un changement significatif des comportements et établir une culture de la sécurité. Il convient d'obtenir le soutien actif du département des communications internes, qui «vendra» la sécurité de l'information et la sensibilisation à la sécurité au public cible. Cela passe généralement par une variété d'outils et de canaux de communication interne permettant de mettre sur pied une «campagne de lancement» et une communication permanente destinée à favoriser le maintien des niveaux de sensibilisation.
- Si le programme prévu inclut des vendeurs et fournisseurs externes, il est important de s'assurer qu'ils
  - disposent de procédures internes et de capacités de gestion de projets solides afin d'assurer la fourniture de solutions en temps voulu, conformément au budget et selon les critères de qualité fixés.
  - disposent d'une combinaison adéquate d'expertises d'apprentissage et de développement ainsi que d'une expertise sur le thème afin de fournir des solutions d'apprentissage efficaces.
  - il convient de fournir un retour d'informations aux responsables ainsi qu'à tout le public ciblé sur la réussite et l'impact de la campagne de formation de manière à ce que les employés prennent conscience des résultats de leurs activités d'apprentissage et soient incités à considérer le temps consacré à ces activités comme un investissement rentable.

Mesurer les réussites et améliorer le programme

Quantifier la réussite du programme fournit de précieuses informations sur l'efficacité et la pertinence des contrôles mis en œuvre. Cela facilite l'évaluation des contrôles adoptés, la détermination des activités de suivi nécessaires ainsi que la légitimation de l'investissement dans la sensibilisation à la sécurité de l'information, un point particulièrement important pour solliciter un nouveau budget de l'année suivante. L'évaluation d'une campagne ou d'un programme de formation est essentielle pour en comprendre l'efficacité ainsi que pour que les données puissent servir d'orientation pour ajuster l'initiative et la rendre plus fructueuse.

Pour mettre en exergue les changements obtenus dans une culture, il convient d'utiliser les mêmes instruments de mesure que ceux utilisés pendant l'évaluation. Ils peuvent être complétés par une évaluation spécifique des contrôles adoptés afin d'indiquer leur efficacité. Si par exemple, un programme de formation de sensibilisation est mis en œuvre, un test des compétences peut permettre d'évaluer les objectifs d'apprentissage atteints.

Banque commerciale internationale: l'évaluation est essentielle pour cibler les efforts

Une grande banque commerciale possède une fonction centrale de sécurité de l'information. Cette équipe est chargée de dispenser des formations de sensibilisation dans le monde entier. Son but est de faire passer des messages fondamentaux à un public nombreux et géographiquement dispersé. Il lui faut également faire passer des messages spécifiques à des groupes plus restreints d'employés assurant des fonctions clés dans les systèmes ou dans la sécurité.

L'un des défis majeurs rencontrés par la banque a consisté à déterminer comment mesurer les niveaux de sensibilisation et l'efficacité de son programme de sensibilisation. Idéalement, la banque aimerait pouvoir évaluer la modification des comportements des employés, un paramètre difficilement quantifiable. Toutefois, l'évaluation est primordiale pour pouvoir orienter la formation sur les points faibles, c'est pourquoi la banque a investi dans l'identification de mesures pratiques et d'indicateurs clés de performance.

Une technique qui s'est révélée particulièrement fructueuse a été l'utilisation de formations assistées par ordinateur (FAO). Une bibliothèque centralisée des FAO comprend notamment des formations et enregistre les résultats des autoévaluations du personnel. Chaque nouvel employé est tenu de suivre cette formation à son arrivée. Elle est régulièrement mise à jour et l'ensemble du personnel doit la suivre à chaque mise à jour. Des rapports indiquent la progression de la FAO ainsi que les résultats des tests. L'équipe centrale contrôle ces données et prend des mesures lorsqu'elle remarque des tendances significatives.

L'étude des mots de passe fournit une mesure quantitative directe et utile sur l'attitude et le comportement du personnel. La banque utilise périodiquement un logiciel qui scanne les fichiers de mots de passe des systèmes clés et analyse le degré d'inviolabilité des mots de passe individuels. Le nombre d'employés utilisant des mots de passe faciles à deviner est un indicateur clé de la sensibilisation à la sécurité.

D'autres techniques qui se sont révélées efficaces incluent notamment la simulation d'e-mails de phishing et les concours. Ces techniques ont amené le personnel ciblé à réfléchir attentivement à la raison pour laquelle on lui demandait d'être vigilant. Elles ont également fourni des statistiques utiles à l'analyse des tendances.

La banque envisage d'introduire une nouvelle enquête visant à évaluer le niveau de sensibilisation à la sécurité et les comportements au sein de la banque. Une tierce partie indépendante collectera les réponses auprès d'un échantillon aléatoire (et non pas auto-sélectionné) d'employés. La banque pourra ainsi se servir des résultats de l'enquête pour tirer des conclusions statistiquement valables pour l'ensemble de l'entreprise.

Au départ, la banque contrôlait les incidents en vue d'évaluer la sensibilisation à la sécurité, mais l'analyse des principales causes a démontré l'existence de nombreux facteurs derrière chaque incident. Le nombre d'incidents ne donne donc pas une image juste de la sensibilisation à la sécurité. Par ailleurs, la fréquence des incidents est tellement faible qu'une analyse des tendances n'est guère significative. C'est pourquoi les statistiques sur les incidents ne sont plus utilisées pour évaluer la sensibilisation.

Lors de la quantification du succès, des instruments qualitatifs et quantitatifs peuvent être mis en place. Quel que soit l'instrument de mesure utilisé, il est important que l'organisme aborde les questions suivantes([16]):

([16]) ENISA, *Information security awareness initiatives: Current practice and the measurement of success* [Initiatives de sensibilisation à la sécurité de l'information: pratiques actuelles et quantification de leur succès], 2007, consultable en anglais à l'adresse suivante: *http://www.enisa.europa.eu/doc/pdf/deliverables/enisa_measuring_awareness.pdf*

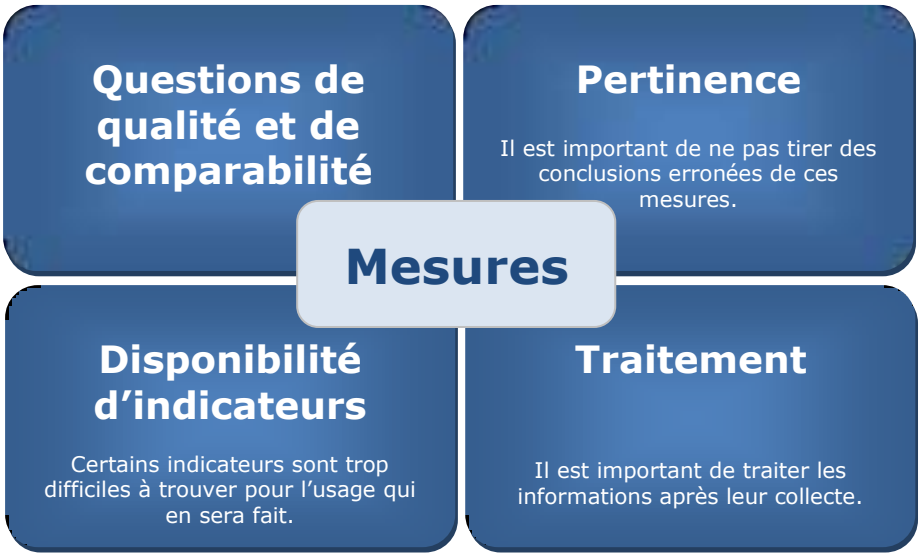

Figure 7: Mesure de l'efficacité des programmes de sensibilisation.

L'évaluation peut apporter la preuve des changements et des améliorations apportés à une culture de sécurité de l'information tout en renforçant l'apprentissage organisationnel, ce qui encourage l'amélioration permanente et favorise une solide culture de la sécurité de l'information.

PARTIE 3: LIGNES DIRECTRICES DE BONNES PRATIQUES

Lignes directrices de bonnes pratiques

Sur la base des informations collectées et de leur analyse, la présente section présente des lignes directrices de bonnes pratiques susceptibles d'aider le lecteur et son organisme dans l'examen de la sécurité des données et la planification d'activités efficaces de formation et de sensibilisation.

Recommandations

	#	Recommandations
Politiques et procédures de sécurité de l'information	**1**	• Définir des politiques et procédures écrites en matière de sécurité de l'information afin de garantir la sécurité des données. Déterminer qui a accès à quels types de documents. Spécifier le format dans lequel les documents peuvent être consultés: électronique ou sur papier. • Éviter d'accorder à l'ensemble du personnel l'accès à toutes les informations personnelles et financières, notamment les coordonnées de comptes bancaires et de cartes de crédit ou les enregistrements de conversations téléphoniques. Les centres d'appel financiers enregistrent très souvent les conversations téléphoniques contenant des données à caractère sensible. Il faut donc y faire particulièrement attention. • Prévoir un mécanisme de contrôle de l'accès aux données personnelles et financières. • Prévoir un mécanisme de rapport en cas de perte de données, indiquant notamment quand et comment prévenir les clients concernés. Préciser les rôles et responsabilités des employés des organismes financiers. • Ne fournir des organisateurs portables et des appareils mobiles (par exemple assistants numériques) qu'aux membres de la direction et aux collaborateurs qui travaillent souvent hors des bureaux. • N'accorder l'accès à l'internet et à l'e-mail qu'aux membres du personnel qui en ont besoin pour des raisons professionnelles. • Encourager l'utilisation de mots de passe difficiles à intercepter.
Sécurité physique	**2**	• Réglementer l'accès aux locaux de l'entreprise, notamment l'accès des visiteurs. • Mettre en œuvre une politique en matière de rangement du bureau. • Ranger les registres personnels et financiers dans un meuble fermé à clé au moment de quitter le bureau. • Prévoir des déchiqueteuses.
Risques de sécurité des données	**3**	• La sécurité des données personnelles et financières constitue l'une des responsabilités essentielles de tout organisme. Chaque donnée est susceptible de présenter de la valeur pour un escroc, qui peut accéder à différentes sources d'informations et recouper celles-ci.
	4	• Contrôler la qualité de l'évaluation des risques et des processus connexes.
Contrôles IT	**5**	• Définir les droits d'accès au moment du recrutement, lorsque les employés changent de poste ou lorsqu'ils quittent l'entreprise. • Créer des comptes d'utilisateur individuels. • Sauvegarder régulièrement les données. • Crypter les données, si nécessaire. • Établir des procédures de continuité des activités et de récupération en cas de sinistre. • Expliquer aux employés l'importance de la sécurité des données personnelles et financières et les risques associés à l'utilisation d'appareils mobiles, tels qu'ordinateurs portables, assistants numériques,

	#	Recommandations
		clés USB, internet et le courrier électronique.
Contrôles	**6**	• Coordonner divers domaines d'activité tels que les ressources humaines, la sécurité physique et la sécurité de l'information afin d'éviter de se concentrer uniquement sur les contrôles IT. • Appliquer les mêmes types de contrôles sur tous les sites, quel que soit leur emplacement géographique. Cela s'applique également aux activités offshore.
Audits internes et conformité	**7**	• Mener régulièrement des audits internes et des contrôles de la conformité de la sécurité des données.
Recrutement et contrôle du personnel	**8**	• Lors du recrutement, effectuer des contrôles de haut niveau sur l'ensemble du personnel. • Garder à l'esprit que le personnel peu expérimenté ou temporaire ainsi que le personnel des centres d'appel disposent souvent d'un plus grand accès aux données personnelles et financières. • Toujours s'assurer que les contrôles adéquats sont effectués, même lorsque des postes doivent être pourvus très rapidement afin de maintenir un niveau adéquat de service à la clientèle.
Tiers	**9**	• Dans la politique de sécurité de l'information de l'entreprise, déterminer si les tiers, comme les centres d'appel, les sociétés d'archivage et les sociétés de consultance informatique, peuvent accéder aux données personnelles et financières et, si oui, les modalités de cet accès.
Mise sur pied des initiatives de sensibilisation et de formation	**10**	• Le plus important est d'obtenir le soutien et le financement de la direction. Le conseil d'administration doit comprendre la dépendance de l'organisme à l'information, reconnaître sa valeur et son importance et comprendre l'environnement réglementaire et légal dans lequel il évolue.
	11	• La sensibilisation à la sécurité de l'information ne se cantonne jamais à l'aspect purement informatique. Les aspects les plus importants d'un programme de sensibilisation sont la communication, le marketing et la formation. Il est donc vivement recommandé de créer un groupe de projet interdisciplinaire composé de membres du département des communications internes, du département marketing, du département des ressources humaines ainsi que du département de la sécurité physique et de la sécurité de l'information.
	12	• Maintenir un rythme constant durant toute la durée du projet est un important facteur de réussite d'un projet. Il peut être souhaitable, dans certains cas de figure, de prévoir différentes étapes plutôt que de s'engager dans un plan plus complexe et plus long.
	13	• Le programme de sensibilisation doit être personnalisé en fonction des besoins de l'organisme. Les programmes génériques sans lien commercial et sans contenu spécifique sont la plupart du temps voués à l'échec.
	14	• Un programme sur mesure doit contenir des valeurs culturelles précises relatives à la sensibilisation aux risques. Ces valeurs sont définies par une structure de documents comprenant une déclaration de stratégie publiée, des lignes directrices et des normes. Les documents doivent être à jour, approuvés par le conseil d'administration et doivent également refléter la méthode de travail de l'organisme. Dans de nombreux cas, les politiques ne sont pas à jour et ne reflètent pas les procédures

	#	Recommandations
		appliquées. Il est alors conseillé de les revoir.
Personnalisation du programme de sensibilisation	**15**	• Il est essentiel de comprendre les différents niveaux de sensibilisation de l'organisme. Le temps des collaborateurs est très précieux. Les programmes de formation doivent être aussi courts que possible, mais aussi longs que nécessaire. Il est donc judicieux de connaître les points forts et les points faibles de la culture de sécurité de l'information et de mettre au point un programme ciblant les lacunes spécifiques à l'organisme.
	16	• Il est essentiel d'adapter le programme aux besoins spécifiques du groupe cible. Les utilisateurs n'ont pas tous besoin des mêmes informations et ils ne seront pas attentifs au message s'ils reçoivent trop d'informations ou des informations non spécifiques.
	17	• Les groupes cibles qui sont au minimum recommandés pour les organismes financiers sont: ○ la direction; ○ l'ensemble du personnel; ○ le personnel manipulant des données à caractère confidentiel.
	18	• Le programme doit également respecter les diverses cultures des différents pays. Des enquêtes culturelles démontrent que la perception et l'attitude vis-à-vis de la sécurité de l'information sont différentes en Europe, en Amérique latine et en Asie.
Processus de gestion du changement	**19**	• Ne jamais penser qu'un projet ponctuel suffira pour modifier à long terme la sensibilisation à la sécurité de l'information. Celle-ci évolue selon une courbe donnée: au départ, on peut constater une amélioration de la sensibilisation et de la motivation, mais la courbe s'aplatit ensuite et peut même revenir à son point de départ. La sensibilisation vise à modifier les comportements, ce qui peut prendre des années.
	20	• Il est donc recommandé d'adopter un processus de gestion du changement. Une communication et une formation continues en matière de sensibilisation sont de bonnes manières de maintenir une attention élevée sur ce sujet. Il est également très important d'évaluer chaque étape et d'adapter si nécessaire les objectifs et les mesures. Cela implique donc de prendre en considération le retour d'informations du public cible.

Figure 7: Recommandations.

Conclusions

Les récents incidents impliquant des pertes de données ont contraint bon nombre d'organismes à étudier les différents moyens qui leur permettraient d'améliorer la sécurité de leurs données. Protéger ces données personnelles et financières constitue d'ailleurs l'une des responsabilités clés du secteur des services financiers. En raison de la nature de leurs activités, les organismes financiers qui gèrent mal la sécurité de leurs données s'exposent à des risques conséquents. Ils détiennent en effet généralement de gros volumes de données personnelles et financières sur leurs clients, comme leurs noms, adresses, dates de naissance, coordonnées bancaires, historiques des transactions, codes PIN, numéros d'assurance sociale, etc. C'est pourquoi le secteur des services financiers doit soigneusement étudier la manière dont il traite ce type de données.

Les organismes financiers sont de plus en plus conscients du coût potentiel d'une perte de données. Cependant, les politiques, procédures et contrôles prévus par les entreprises pour assurer la sécurité de l'information ne suffisent pas pour éviter les pertes de données dues à un manque de sensibilisation des employés sur les risques liés au traitement de l'information.

Des mécanismes efficaces de formation et de sensibilisation sont essentiels dans ces organismes car les risques auxquels ils s'exposent, tels que notamment le vol d'identité, le blanchiment d'argent, l'abus de marché, peuvent tous entraîner de lourds désagréments et éventuellement des pertes financières pour les victimes, ainsi que des dommages à l'organisme lui-même.

L'ENISA espère que cette publication constituera un outil précieux pour les organismes financiers qui leur permettra de comprendre l'importance d'une perte de données et de préparer et de mettre en œuvre des programmes de formation et de sensibilisation.

Références et sources d'informations supplémentaires

BERR, *2008 Information Security Breaches Survey* [Enquête 2008 sur les violations de la sécurité de l'information], disponible en anglais à l'adresse suivante: http://www.security-survey.gov.uk (dernière visite le 22 juillet 2008).

«*Data-leak security proves to be too hard to use*» [Les systèmes de sécurité anti-fuite de données se révèlent trop difficiles à utiliser], Infoworld.com, consultable en anglais à l'adresse suivante: http://www.infoworld.com/article/08/03/06/10NF-data-loss-prevention-problem_1.html (dernière visite le 2 juin 2008).

Directive 95/46/CE relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, JO L 281 du 23.11.1995.

ENISA, *Un Guide Utilisateur:* Comment améliorer la sensibilisation à la sécurité de l'information, 2008, consultable à l'adresse suivante: http://www.enisa.europa.eu/doc/pdf/deliverables/WGAR/guide_fr.pdf

ENISA, Information security awareness initiatives: Current practice and the measurement of success, 2007 [Initiatives de sensibilisation à la sécurité de l'information: pratiques actuelles et quantification de leur succès], consultable en anglais à l'adresse suivante: http://www.enisa.europa.eu/doc/pdf/deliverables/enisa_measuring_awareness.pdf

ENISA, *Raising Awareness in Information Security – Insight and Guidance for Member States* [Améliorer la sensibilisation à la sécurité de l'information], 2005, consultable en anglais à l'adresse suivante: http://www.enisa.europa.eu/doc/pdf/deliverables/enisa_cd_awareness_raising.pdf

ENISA, *Clés USB: priorité à la sécurité*, 2008, consultable à l'adresse suivante: http://www.enisa.europa.eu/doc/pdf/publications/secure_usb_flash_drives_fr.pdf

Autorité britannique des services financiers, *Data Security in Financial Services* [Sécurité des données dans le domaine des services financiers], Royaume-Uni, avril 2008.

Heiser, Jay, *Understanding data leakage* [Comprendre la perte de données], Gartner, 21 août 2007.

Herold, Rebecca, *Managing an Information Security and Privacy Awareness and Training Programme* [Gérer un programme de formation et de sensibilisation à la protection des données et au respect de la vie privée], Boca Raton: Auerbach, États-Unis, 2005.

Herold, Rebecca, *Information security and privacy awareness program* [Programme de sensibilisation à la sécurité de l'information et à la protection de la vie privée], Auerbach Publications, USA, 2005.

McGlasson, Linda, «ID Theft Red Flags Rule: *How to Help Your Business Customers Comply*» [La «Red Flags Rule» contre le vol d'identité: comment aider vos clients à l'observer], BankInfoSecurity.com, 8 septembre 2008 http://www.bankinfosecurity.com/articles.php?art_id=960andrf=090908eb

NIST, *Building an information technology security awareness program* [Élaborer un programme de sensibilisation à la sécurité des technologies de l'information], NIST — SP800-50, NIST, 2003, consultable en anglais à l'adresse suivante: http://csrc.nist.gov/publications/nistpubs/800-50/NIST-SP800-50.pdf (dernière visite le 17 juillet 2008).

NIST, Information technology security training requirements: A role- and performance-based model [Exigences de formation en matière de sécurité des technologies de l'information: modèle axé sur les

performances et les rôles], NIST — SP 800-16, États-Unis, 1998, consultable à l'adresse suivante: http://csrc.nist.gov/publications/nistpubs/800-16/800-16.pdf (dernière visite le 21 juillet 2008).

Schlienger, T. and S. Teufel, *Tool supported Management of Information Security Culture: An application to a Private Bank*, [Gestion instrumentalisée de la culture de la sécurité de l'information: application aux banques privées], The 20th IFIP International Information Security Conference (SEC 2005) - Security and Privacy in the Age of Ubiquitous Computing [Sécurité et vie privée à l'ère de l'informatique omniprésente], Makuhari Messe, Chiba, JAPON, Kluwer Academic Press, 2007.

«State of Banking Information Security 2008 - Survey Executive Overview» [État des lieux 2008 de la sécurité des informations bancaires – Synthèse analytique de l'enquête], BankInfoSecurity.com, consultable en anglais à l'adresse suivante: http://www.bankinfosecurity.com/whitepapers.php?wp_id=143 (dernière visite le 20 novembre 2008).

Sensibilisation des organismes financiers à la sécurité de l'information

ISBN: 978-92-9204-033-8

Numéro de catalogue: TP-80-08-395-FR-N

Doi : 10.2824/14368

TP-80-08-395-FR-N

enisa
European Network and Information Security Agency

ISBN 978-92-9204-033-8

PO Box 1309, 71001 Heraklion, Greece, Tel: +30 2810 391 280
www.enisa.europa.eu