Revue Française de Gestion Industrielle
Vol. 28, N° 1

GESTION DES RISQUES ET CULTURE DE SURETE : LE CAS DU VECTEUR BADGE, VERITABLE « PASSEPORT POUR L'ENTREPRISE DE DEMAIN »

Sophie GAULTIER-GAILLARD*, Pierre PECH*, Bernard GALEA**

Résumé. - La sûreté devient un nouvel enjeu de compétitivité, elle est désormais partie intégrante de toute politique de gestion des risques pour les entreprises. Il s'agit aujourd'hui de mettre en place un ensemble de mesures et de moyens au sein de l'organisation en vue de garantir la sécurité des personnels, la protection des biens et du patrimoine sensible, l'intégrité de l'image de la société et le crédit de ses dirigeants. Dans un contexte de mondialisation et de libéralisation des échanges, ces mesures conditionnent le développement de l'entreprise vis-à-vis de ses concurrents. Il en résulte que l'un des véritables enjeux stratégiques dans le domaine du contrôle d'accès physique, en termes de recherche et de développement, consiste aujourd'hui à tenter d'unifier les modes d'accès sur les différents sites d'un même Groupe, notamment lorsque ceux-ci sont répartis dans plusieurs pays et faire ainsi du badge d'accès un véritable passeport d'entreprise. On peut alors s'interroger sur les moyens à mettre à la disposition de l'entreprise pour lui permettre de concilier sûreté et performance économique tout au long de sa supply chain. Le vecteur badge semble être une solution plébiscitée par les résultats de notre enquête par questionnaire, et pourrait devenir un véritable passeport pour l'entreprise de demain. Nous démontrerons l'intérêt de son usage et son importance dans le développement stratégique de l'entreprise, en étudiant notamment l'impact de la biométrie sur le contrôle d'accès physique.

Mots-clés : Gestion des risques, Culture d'entreprise, Sûreté, Supply chain, Contrôle d'accès.

* Université Paris 1 Panthéon-Sorbonne, Laboratoire de Géographie Physique UMR CNRS 8591 et Laboratoire PRISM_ISO.
** Directeur Sûreté Groupe, FM Logistic.

1. Introduction

La compétitivité et la sûreté économique nationale s'articulent essentiellement autour de la sécurité au quotidien de nos entreprises. La mondialisation et la libéralisation des échanges, l'émergence de la concurrence exacerbée qui en résulte, entretiennent un véritable climat d'insécurité autour des entreprises françaises et menacent parfois leur existence. Cette insécurité proprement économique est accentuée par la croissance des actes malveillants allant du pillage de données à l'intrusion physique ou à la contrefaçon [Le Gentil A. et al, 2005].

Depuis les années 90 [Reason, 1998], la nécessité d'une culture de sûreté partagée par tous au sein des entreprises n'est plus contestable. Cette notion intègre désormais, en théorie, les aspects techniques, humains et organisationnels dans les démarches de prévention des risques industriels [Chevreau, 2006]. L'entreprise est considérée comme une entité à part entière, constituée de ressources variées. Elle se doit alors de mettre en place une politique de gestion des risques qui lui permette d'atteindre les objectifs stratégiques assignés en gérant ses ressources disponibles [Gaultier-Gaillard, Louisot, 2005].

Dans ce cadre d'étude, la sécurité de l'entreprise pourrait se définir comme étant un ensemble de mesures et de moyens à mettre en œuvre au sein de l'organisation afin de garantir : la sécurité des personnels, la protection des biens et du patrimoine sensible, l'intégrité de l'image de la société et le crédit de ses dirigeants. La sûreté est quant à elle la protection contre des actes de malveillance, c'est-à-dire l'éloignement de tout péril. Si dans le monde du nucléaire, la sûreté atteint son paroxysme, cette discipline doit s'appliquer également à l'ensemble des établissements tertiaires et industriels. Cependant les enjeux ne seront pas les mêmes dès lors qu'il s'agit de protéger l'information (contrôle d'accès logique) ou les biens matériels (contrôle d'accès physique). Nous limiterons donc volontairement l'étude aux biens matériels.

Afin d'adopter une approche globale de gestion des risques, l'entreprise sera considérée comme un système défini par cinq grandes classes de ressources sur lesquelles s'appuie son organisation pour atteindre ses objectifs. Il s'agit des ressources humaines, techniques, informationnelles, financières, les partenaires économiques amont (sous- traitants et fournisseurs) et aval (circuits de distribution « networks » et clients).

Dès lors, afin de réduire les vulnérabilités susceptibles de peser sur l'organisation, notamment en termes d'événements dommageables (périls endogènes ou exogènes), de ressources qui peuvent être atteintes (vol, destruction, vandalisme...), de pertes financières induites lors de la réalisation de ces périls, l'entreprise est amenée à se protéger en gérant le risque et en mettant en œuvre, toute proportion gardée, le concept du principe de précaution. Par conséquent, indépendamment de leurs tailles, de leurs activités, de leurs localisations, la

problématique du contrôle d'accès physique reste un enjeu majeur concourant à la protection de leur patrimoine, tant sur les plans physiques qu'informationnels. Pour certaines sociétés, le choix du type de contrôle d'accès s'inscrit dans une démarche stratégique et la décision de s'engager sur tel ou tel système est prise à un niveau central, voire en conseil d'administration. Cela s'explique en partie par la réflexion qui aura conduit à l'option technologique retenue et par les engagements financiers qui en seront induits.

Il en résulte que l'un des véritables enjeux stratégiques dans le domaine du contrôle d'accès physique, en termes de recherche et de développement, consiste aujourd'hui à tenter d'unifier les modes d'accès sur les différents sites d'un même groupe. En particulier, lorsque ceux-ci sont répartis dans plusieurs pays et faire ainsi du badge d'accès un véritable passeport d'entreprise. L'objet de cet article est de démontrer que le défi à relever pour équiper les grandes entreprises spécialisées de demain ne peut s'effectuer que par une mise en place d'une politique de gestion des risques qui intègre la culture de sûreté et les concepts de l'intelligence économique. Ce constat suppose que l'entreprise soit capable de gérer simultanément sûreté et performance économique (2), qu'elle ait identifié ses intérêts stratégiques (3) et qu'elle puisse mettre en œuvre les moyens pour les sécuriser (4).

2. Entre sûreté et performance économique : comment une entreprise peut-elle organiser la défense de ses intérêts stratégiques ?

Nous porterons une attention particulière aux vulnérabilités d'une organisation face à une agression sur son patrimoine informationnel ou à un acte de malveillance sur ses biens matériels. Ce type d'analyse a été systématisé par les praticiens des cindyniques [Kerven, 1991, 1995]. Le postulat de départ (vérifié lors de nombreuses analyses de crises réelles) est que les crises arrivent lorsqu'un certain nombre de déficits générateurs de dangers sont présents. Un déficit peut par exemple être un sentiment de supériorité face à la concurrence. Un second peut être l'absence d'un système de retour d'expérience. Ainsi, une entreprise qui cumulerait ces deux déficits, même si elle était informée par exemple d'actions de renseignements de ses concurrents et des conséquences graves de ces actions, nierait probablement l'évidence et ne prendrait aucune mesure de protection. Dans cette analyse, on étudie de manière systématique des déficits de l'organisation, qui génèrent du danger. Ces déficits sont regroupés en trois grandes familles : les déficits culturels, organisationnels et managériaux. La systémique nous aide à poser les problèmes mais n'a pas vocation de fournir directement des solutions. C'est un savoir méthodologique, « une paire de lunettes » qui nous permet de mieux déchiffrer la réalité complexe et d'agir sur elle avec plus de pertinence [Morin et al, 2000].

Ainsi pourrions-nous constater que certaines passerelles, voire imbrications, peuvent exister entre l'Intelligence Economique (IE) et la gestion des risques. En effet, la cindynique enseigne qu'une crise a toujours pour origine une lacune dans le système d'information « on ne savait pas que… », « on avait omis de reporter que… » or le but de l'I.E. n'est-il pas d'apporter la bonne information au bon moment et à la bonne personne ? Mettre en place et optimiser un système d'intelligence économique dans l'entreprise n'est pas une mode ou une révolution mais davantage une adaptation obligée de l'entreprise à l'économie de la connaissance de l'information. Ethique et déontologique, l'intelligence collective de l'entreprise est une aide à la décision, un facteur d'influence et de performance, un outil d'innovation, de détection des opportunités. Cette discipline offensive et défensive a également pour finalité de détecter les menaces, les actes de malveillances et de prévenir les risques. De nombreux ouvrages [Mongin, Tognini, 2006] tendent à démontrer que seule la mise en place d'un système d'intelligence économique permet la création d'une véritable intelligence des risques nécessaire pour prévenir les crises. Le système d'intelligence économique de l'entreprise, voué par ailleurs à l'intelligence des opportunités, se transforme également en intelligence des risques. Il assurera la sensibilisation, la prévention, le calcul et la hiérarchisation des risques (gravité et probabilité d'occurrence) et leur réduction par la mise en place d'une véritable mission de protection de l'entreprise [Besson et al., 2006]. Ainsi, une entreprise mieux informée est une entreprise mieux défendue : « connaître son ignorance est la meilleure part de la connaissance[1] ».

Partant du principe que les bonnes pratiques de sûreté ne doivent surtout pas gêner les performances, chaque individu doit pouvoir trouver un intérêt personnel et immédiat dans la politique de sûreté mise en place, sachant que la sûreté est faite pour l'Homme et non l'inverse. Aussi, en s'appuyant sur les travaux réalisés par Yves Maquet [Maquet, 1991], il est possible d'optimiser la sûreté stratégique d'une entreprise en tirant parti des facultés d'organisation des équipes internes et de leur créativité en se focalisant davantage sur le risk management des fonctions. Ainsi, l'identification des missions et des objectifs reste prioritaire.

Cette démarche de gestion par la création de ressources est souvent utilisée par des cabinets d'audit et de conseils de référence, spécialisés dans la gestion externalisée des risques dans le domaine du supply chain management [Carbone & Meunier, 2006], en particulier lors de la rédaction de cahier des charges pour des systèmes de contrôle d'accès[2].

Comme nous pouvons le constater, il n'existe pas à proprement parler de méthode unique permettant de répondre à l'ensemble de la problématique de sûreté des entreprises, en revanche il est nécessaire d'aborder la sûreté par une approche globale quitte à la décliner ensuite par

1 Proverbe chinois.

2 Société ACCIS (Audit Conseil Concept Ingénierie Sécurité), prescriptions pour système multi-postes de gestion des accès, 28p.

tronçon en appliquant les méthodes les plus adaptées. Ceci est naturellement recommandé au niveau du management des systèmes de contrôle d'accès [Kovacich & Halibozek, 2003, 2005]. L'instauration d'une culture de la sûreté est donc une étape d'une politique de gestion des risques en entreprise et s'intègre parfaitement dans une démarche fondée sur l'intelligence économique.

3. Identification des intérêts stratégiques à sécuriser

3.1 Méthodologie

Des rencontres avec des experts et des chercheurs travaillant sur les évolutions technologiques, juridiques et éthiques concernant la problématique du contrôle d'accès ont été organisées. Des entretiens avec les professionnels des secteurs industriels, fabricants, fournisseurs et utilisateurs[3], se sont déroulés afin de déterminer les possibilités exactes pour répondre à la problématique posée consistant à faire du vecteur badge un véritable « passeport d'entreprise ».

Comme le souligne Alain Bauer : « *Désormais, il faut être conscient que l'entreprise a rencontré le monde du crime. Elle est un acteur de la vie économique mais elle est également un enjeu majeur comme outil : vols, racket, enlèvements, espionnage industriel, sont aujourd'hui présents. Le seul élément qui permet d'intégrer la problématique de la sûreté, reste l'anticipation* » [Bauer, 2007], le contrôle d'accès physique est donc devenu un enjeu stratégique pour un Groupe. Ainsi, la première étape de mise en œuvre d'une démarche sûreté au sein d'un établissement consiste à analyser les risques sûreté et les différentes catégories de menaces. Bien que l'imagination des criminels soit débordante, il est néanmoins possible d'établir une typologie de la malveillance. Qu'ils soient d'origine interne ou externe à l'établissement, les actes de malveillance, pour la supply chain, peuvent être regroupés selon 5 catégories :

- la criminalité courante : vols ou démarques inconnues, vandalisme, revente de marchandises diverses sur des marchés parallèles si l'on est confronté à un réseau lié au banditisme ;
- l'espionnage industriel visant à dérober des informations confidentielles ;
- les troubles sociaux qui peuvent résulter d'un conflit social dans l'entreprise mais également à l'extérieur de l'établissement (conflit de voisinage, mouvements

[3] Dont participation au Salon Cartes et Identification 2007 (13-15/11/07- Paris).

défenseurs de la nature) présentant un danger pour l'exploitation d'un site ou lui interdisant son accès par effets collatéraux ;

- les actes de sabotage qui consistent à détruire l'outil de production pour en perturber le bon fonctionnement ;

- le terrorisme qui correspond à l'ensemble des actes de violence commis par une organisation ou un individu isolé, pour créer un climat d'insécurité et de terreur.

Pour analyser les risques qui pèsent sur un établissement, une approche qualitative par la méthode des centres de risques complétée par un retour d'expériences du secteur sera adoptée. Au travers des entretiens auprès des propriétaires des processus critiques ou des directions Métiers de l'entreprise, les cinq catégories de vulnérabilité sont examinées. Une fois le questionnaire administré, il est possible de quantifier chaque catégorie de risques, en additionnant les réponses obtenues et en pondérant les questions qui apparaissent être les plus importantes pour l'établissement étudié.

Deux questionnaires ont été préparés à cet effet et adressés à 30 experts du domaine de la sûreté. L'un destiné aux chercheurs tant du domaine universitaire (laboratoires de recherches) que des secteurs industriels (département contrôle d'accès et sûreté des systèmes d'information), l'autre aux opérationnels de la gestion quotidienne de sites (directeurs de plateformes, responsables sécurités). L'étude a été réalisée entre le mois de novembre 2006 et le mois de novembre 2007, soit une durée d'un an. Chaque questionnaire visait à recueillir l'expertise des hommes de l'art aussi bien sur les outils les plus couramment utilisés que ceux en cours de développement, tout en essayant de mettre systématiquement en parallèle les vulnérabilités de l'entreprise auxquelles ces moyens devraient répondre.

3.2 Résultats

Les principaux résultats tendent à prouver que si des solutions industrielles à la problématique posée existent sur le marché, elles sont encore excessivement complexes à mettre en œuvre et le coût en reste élevé.

Pour autant, comme il est expliqué au début de cet article, il s'agira d'un choix stratégique pour l'entreprise. Si celle-ci s'engage sur cette voie, il lui sera possible à moyen terme d'unifier ses systèmes de contrôle d'accès et de faire de son vecteur badge un véritable passeport d'entreprise. Cependant, l'exercice restera délicat s'il doit être mené sur l'ensemble des sites d'un même Groupe implanté sur différents continents. Pour cela, un état des lieux sécuritaire et organisationnel, véritable audit du site, à la lumière de l'analyse des risques, pourra alors être réalisé. La documentation ISO 17 799, bien que destinée principalement à la protection du

patrimoine informatique, pourra être utilement employée en la déclinant comme un référentiel de base de référence pour un audit contrôle d'accès physique ou pour des prestataires extérieurs évoluant dans ce domaine d'activité. Après traitement des questionnaires, il s'avère que les moyens de protection sûreté d'un site s'articulent essentiellement autour des points suivants :

- entrave de la visibilité et dissuasion : clôture et retard à l'effraction, éclairage, végétation…
- contrôle d'accès : identification, authentification et vérification des flux piétons et voitures, entrées et sorties ;
- détection et alerte : vidéosurveillance, télésurveillance… ;
- intervention et gestion de crise : chiens de garde, intervention des forces de l'ordre, équipe de sûreté…

Les moyens de protection mis en œuvre devront être proportionnels à la nature des biens à protéger. D'ailleurs selon le préfet Rémy Pautrat[4] : « *Préserver le secret dans un monde de transparence impose donc de savoir établir le périmètre du cœur stratégique de l'entreprise* ». Il apparaît clairement que les moyens de protection les plus adaptés seront ceux dédiés au contrôle d'accès physique, conjugués naturellement aux autres systèmes mentionnés supra. Ainsi, après avoir clairement défini ce que l'on désire protéger, la réflexion stratégique conduira l'entreprise à prendre deux décisions. La première portera sur le choix du vecteur (avec quoi) : carte, clé, badge, biométrie,… La seconde consistera à en définir la technologie désirée (comment).

En effet, les technologies occupent aujourd'hui une place essentielle dans les domaines de la sûreté et notamment celle de la lutte contre la malveillance. Utilisées dans le cadre de la prévention (analyse), du traitement des crises (planification, gestion de l'information, communication opérationnelle) ou de leurs conséquences, elles accroissent considérablement les capacités d'analyse et d'action des structures qui les utilisent et sont susceptibles d'influer sur la prise de décision [Gérard, 2006].

[4] Discours d'ouverture de la 10ème promotion de l'IERSE par le préfet Rémy Pautrat: « les défis pour l'entreprise au XXI siècle », septembre 2006.

4. Moyens à mettre en œuvre pour sécuriser ses intérêts stratégiques

4.1 Le vecteur contrôle d'accès

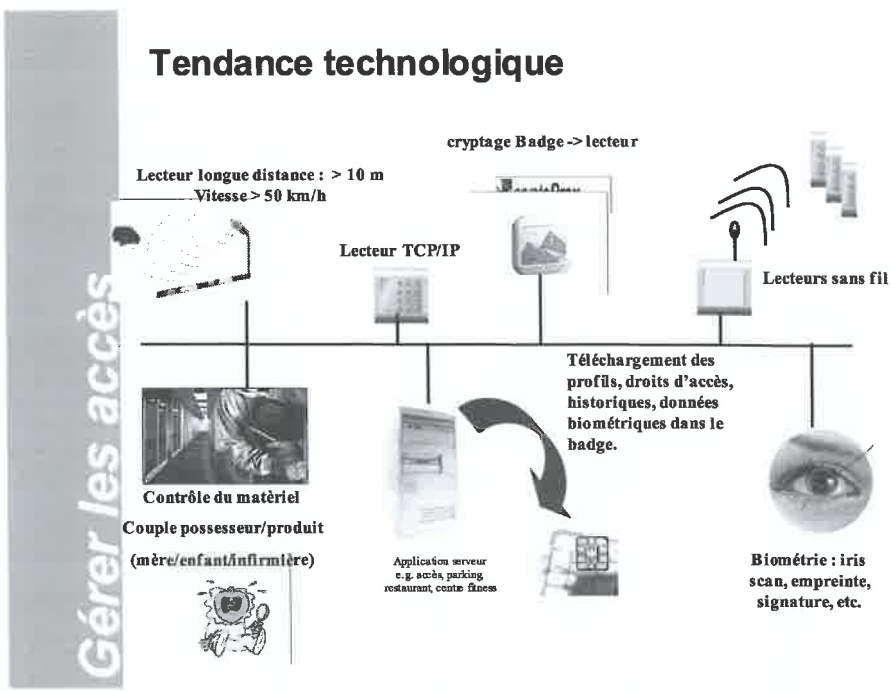
Le vecteur contrôle d'accès est donc le niveau le plus critique en termes de protection patrimoniale : « l'entreprise est un joyau, protégeons-la » et représente la première image que donne l'entreprise tant à ses employés qu'à ses clients, sous-traitants et visiteurs : « montre-moi ton contrôle d'accès, je te dirai comment je te perçois ». On peut légitimement évoquer ici le fait que les systèmes de contrôle d'accès qui participent à la gestion des risques humains, contribuent, de manière paradoxale, à la communication de l'entreprise quant à la gestion des risques liés à la réputation. A titre d'exemple, nous pouvons comparer l'image que donne à ses salariés et à ses visiteurs une entreprise utilisant un système de contrôle d'accès physique fondé sur des badges à piste magnétique (technologie de première génération) avec celle employant un système de contrôle biométrique de dernière génération. L'image en sera certainement différente. Nous voyons dès lors apparaître une certaine singularité pour une pratique qui se veut initialement une application de type sûreté, protection patrimoniale, et qui participe in fine, à une certaine forme de communication de l'entreprise. Le choix doit donc en être particulièrement adapté et représente un enjeu stratégique important.

Aujourd'hui, l'un des véritables défis, qui débouche sur des questions liées à des enjeux de recherche et développement consiste à essayer d'unifier les modes d'accès sur les différents sites d'un même Groupe. L'idée d'un seul système pour entrer sur tous les sites, sans pour autant être en situation de non concurrence vis-à-vis d'un seul fournisseur d'accès, est séduisante mais encore difficile à mettre en œuvre d'autant que cette problématique n'est jamais réellement achevée puisque, d'une part les technologies évoluent et, d'autre part, dans le cadre des fusions/acquisitions, la société acheteuse rachète l'existant, y compris en termes de contrôle d'accès.

4.2 Les technologies disponibles

Les recherches réalisées tendent à démontrer que les badges à lecture/écriture accompagnent l'évolution du contrôle d'accès vers plus de sécurisation de l'identification et vers les technologies de biométrie (cf. figure 1). Ils permettent, en plus, la cohabitation de plusieurs applications sur le même support allant vers un outil d'identifications multiples. En effet, à la base le badge sans contact à lecture simple sur 125 kHz renferme une antenne et une puce de mémoire qui est codée lors de la fabrication du vecteur. Concrètement, il s'agit d'un badge à écriture unique et à lecture multiple. La plupart des badges sont passifs, ils ne sont pas alimentés. L'antenne génère un courant induit quand elle est plongée dans un champ magnétique à proximité du lecteur le champ doit être suffisamment puissant. Ce courant

alimente une puce de mémoire qui transmet les informations contenues via l'antenne du badge qui devient émettrice. Cette émission est reconnue par l'électronique du lecteur comme signature du badge. L'autre grande famille des badges est celle sans contact passif à lecture-écriture sur 13,56 MHz fonctionnant de manière identique aux précédents. Cependant, ici le courant induit alimente une puce mémoire où des opérations d'écriture et de lecture peuvent être réalisées. Avec ce système, la mémoire est nettement supérieure et le client peut alors imposer ses propres clés de chiffrement au fournisseur.



Source M.Carlier, 2007.

Figure 1 : Les tendances technologiques liées à la gestion des accès.

Au niveau de la sécurité, la technologie à 13,56 MHz a pour avantage par rapport au 125 kHz, un fonctionnement plus sécurisé, de plus courtes distances de lecture, un cryptage des données non imposé par les normes et des algorithmes à clés symétriques pour l'authentification. L'utilisation de lecteurs pirates à haute énergie pour les badges, placés dans les poches de leurs porteurs à leur insu,, bien connue des spécialistes en 125 kHz, est techniquement possible en 13,6 MHz. Toutefois, les protocoles transactionnels limitent *a priori* l'accès à l'identifiant en empêchant l'accès aux données de la mémoire sans connaissance et mise en œuvre de sa structure. L'utilisation de badges falsifiés est également difficilement envisageable. Les niveaux de sécurisation sont beaucoup plus élevés et l'utilisation de clés est

une barrière importante. Pour ce qui est de l'adaptabilité à l'existant ou la substitution, les systèmes de contrôle d'accès physique les plus répandus sont ceux utilisant des badges de proximité en 125 kHz, très lourds et coûteux à remplacer.

Afin de s'intégrer harmonieusement avec ceux-ci lors d'une évolution de structure, certains fabricants proposent désormais des badges à double technologie 125 kHz et 13,56 MHz. Ils permettent ainsi l'identification sur les lecteurs existants en 125 kHz mais également l'ouverture à des services tels que le porte-monnaie électronique à l'intérieur de l'entreprise (très apprécié des comités d'entreprises gestionnaires des cantines par exemple).

Par ailleurs, les coûts des solutions de contrôle d'accès utilisant les badges de proximité, représentant la quasi-totalité du marché des nouveaux systèmes, ont sensiblement diminué ces dernières années. Parmi ces solutions de proximité, celles utilisant les badges de lecture/écriture montent fortement en puissance, étant beaucoup plus abordables que par le passé, surtout en regard des services apportés. Elles ne se substituent pas totalement aux badges classiques. Le 125 kHz est bien loin d'être remplacé. Les coûts des solutions en 125 kHz et en 13,56 MHz ont tendance à se rejoindre selon certains fournisseurs. Comparé au 13,56 MHz, le 125 kHz possède encore la plus forte croissance en volume. Le 13,56 MHz a une plus forte croissance en pourcentage, mais en partant de volumes beaucoup plus réduits. La sécurité du 125 kHz suffit ainsi dans un grand nombre de cas. Il s'agit d'une technologie très mature, simple et économique. De plus, cette technologie possède une plus grande tolérance aux légers défauts de qualité des antennes de certains badges, alors que les technologies en 13,56 MHz sont très peu tolérantes et un plus grand confort de lecture avec des distances supérieures.

La détermination de la technologie du vecteur badge reste un choix crucial pour l'entreprise car elle impactera fortement son coût. Le marché du badge de proximité connaît aujourd'hui un développement considérable dû principalement à l'avènement des nouvelles technologies. HID[5], MIFARE[6], WIEGAND[7], RFID[8]. Pour répondre au défi de demain en faisant du vecteur badge un véritable passeport, il est impératif que l'entreprise s'oriente vers une technologie dite « ouverte ». Il s'agit d'une technologie de badge du futur qui permettra une

---

5 HID : Human Interface Device.

6 La technologie MIFARE (MIkron FARE-collection System) a été développée par Mikron puis acquise par Philips en 1998.

7 Wiegand. Le terme Wiegand est une marque de la société *Sensor Engineering Company*. Il est utilisé pour désigner une technologie permettant de réaliser des « badges à effet Wiegand » et les lecteurs de badges correspondants. Techniquement, les badges à effet Wiegand présentent par rapport aux cartes magnétiques l'avantage d'une très grande robustesse. Commercialement, les badges à effet Wiegand sont en perte de vitesse depuis la montée en puissance de la technologie des badges de proximité. D'autre part, la *Security Industry Association* utilise le terme Wiegand pour désigner plusieurs normes d'interfaces, dites interfaces Wiegand, principalement utilisées pour les lecteurs de badge.

8 Radio Frequency Identification.

rationalisation des coûts sur le long terme en pouvant, sans modifier ses systèmes de contrôle d'accès, évoluer vers des applications voire y insérer, pour certains sites ou zones de stockage, des éléments d'identification biométrique tout en respectant, pour ce qui est du territoire national, les recommandations de la CNIL.

Toutefois, au-delà du vecteur badge, qui représente le premier niveau de sûreté de l'entreprise, voire le plus critique, il conviendra d'intégrer dans le prix de revient relatif de l'uniformisation du contrôle d'accès sur l'ensemble des sites d'un Groupe, le coût des interfaces des têtes de lecture. Actuellement, la technologie MIFARE domine assez largement le marché, il s'agit de la technologie de carte à puce sans contact la plus répandue dans le monde ; avec 500 millions de cartes et 5 millions de modules de lecture/encodage, elle répond par ailleurs au standard ISO 14443.

S'agissant des normes, il existe 3 standards : ISO 14443 A 1-4, ISO 14443 B 1-4 et ISO 15693. Aussi est-il impératif de bien différencier les compatibilités partielles et complètes. En effet, tout lecteur intégralement compatible ISO 14443 A -4 peut lire et écrire sur toutes les marques de cartes complètement compatibles ISO 14443 A -4, de même pour ISO 14443 B -4. Une compatibilité partielle à ces normes entraîne une incompatibilité totale avec d'autres badges. Tout lecteur A-3 ou B-3 n'est ainsi compatible qu'avec lui-même, donc complètement propriétaire. Lors d'un projet de contrôle d'accès, il convient de vérifier l'étendue de la compatibilité d'un système avec toutes les parties 1, 2, 3, et 4 des normes. Par ailleurs, tous les supports à mémoire, dont les badges, voient leur capacité augmenter. Le marché évolue vers des cartes plus puissantes à microprocesseurs, aux niveaux de sécurisation compatibles avec les parties 4 des normes A et B. Afin d'assurer une compatibilité totale présente et future, certains nouveaux lecteurs satisfont simultanément et pleinement aux 3 normes. Ils permettent ainsi la lecture et l'écriture de toutes les cartes respectant parfaitement les normes et sont d'ores et déjà compatibles avec ce qui va sortir. Pour quelques fabricants, la « rétro compatibilité » est possible et ne doit pas seulement être technologique mais aussi respecter les usages, comme le confort d'une grande distance de lecture et une vaste gamme de lecteurs pouvant comporter un clavier. Une compatibilité totale aux normes permet de s'adapter à tous les développements d'applications.

La sécurité est une préoccupation de plus en plus importante au sein des entreprises, qui commence par l'accès à l'information. Pour se prémunir des éventuelles indélicatesses, une nouvelle technique de contrôle d'accès a fait son apparition et ne cesse de croître depuis une décennie : il s'agit de la reconnaissance physique des personnes par des systèmes biométriques. Ces systèmes sont utilisés aussi bien pour des contrôles d'accès physique que pour des contrôles d'accès logiques. Depuis 6 ans environ, cette technologie a connu un développement important notamment suite aux attentats du 11 septembre 2001. Les techniques de contrôle d'accès sont

fondées sur les critères suivants : ce que l'on sait, un mot de passe ; ce que l'on possède, une carte, un badge, un document ; ce que l'on est, c'est la biométrie.

Prise au sens large, la biométrie recouvre l'ensemble des procédés tendant à identifier un individu à partir de la « mesure » de l'une ou de plusieurs de ses caractéristiques physiques, physiologiques ou comportementales. Le mot « biométrie » utilisé dans le domaine de la sécurité est une traduction de l'anglais « biometrics » correspondant à notre mot anthropométrie. Le mot français biométrie définit « l'étude mathématique des variations biologiques à l'intérieur d'un groupe déterminé ». Dans la suite de l'article, pour plus de clarté, nous utiliserons la définition « franglaise » qui est passée dans le langage « sécurité » courant : biométrie. Le principe de fonctionnement des technologies biométriques est identique quel que soit le vecteur utilisé. Il s'agit de comparer une image biométrique préalablement saisie d'un utilisateur avec une image biométrique de même nature d'un utilisateur X. L'application détermine la similitude ou son absence entre les deux images. Seule la similitude permet l'accès à un site ou à l'utilisation d'un appareil informatique par exemple. Trois phases constituent le principe de fonctionnement du système : la capture de l'information biométrique, le traitement de l'information avec la création d'un fichier signature de référence enfin la vérification ou phase de comparaison des images des deux fichiers afin de déterminer « un taux de similitude » permettant la prise de décision. Ainsi peut-on définir les systèmes biométriques comme des applications permettant l'identification automatique ou l'éligibilité d'une personne à se voir reconnaître. Ces droits sont fondés sur la reconnaissance des particularités physiques : empreintes digitales, iris de l'œil, contour de la main, etc., Il est rappelé que l'identité d'un individu est l'ensemble des données de fait et de droit qui permettent de l'individualiser. Ainsi, la vérification de l'identité conduit à l'identification, la preuve de l'identité conduit à l'authentification. La biométrie est donc l'identification d'une personne fondée sur ses caractéristiques physiologiques ou biologiques, automatiquement reconnaissables et vérifiables.

Pour le contrôle d'accès physique, l'empreinte digitale continue à être la principale technologie biométrique en parts de marché, près de 50% du chiffre d'affaires total. La reconnaissance du visage, avec 12% du marché, dépasse la reconnaissance de la main, qui avait jusqu'à présent la deuxième place en termes de source de revenus après les empreintes digitales. Les autres technologies sont encore émergentes, comme la reconnaissance de l'iris et de la rétine.

Par ailleurs, dans le souci d'améliorer l'authentification de l'utilisateur, les organismes ont tendance à cumuler différents procédés : la reconnaissance du visage et des empreintes vocales ou bien, sur un clavier d'ordinateur, la frappe d'un mot de passe, l'empreinte digitale et une carte à puce. Dans ce dernier cas, on trouve un triple niveau d'authentification : par ce que l'on

sait, par ce que l'on possède et par ce que l'on est. C'est ce que l'on appelle la biométrie multimodale [Dorizzi et al., 2007].

Evidemment, la combinaison technique biométrique et mot de passe demeure la moins onéreuse. C'est l'association de la carte à puce et de la technologie biométrique qui présenterait incontestablement les plus grands avantages pratiques et économiques. Les avantages d'une telle association sont considérables en termes de protection des données personnelles et des libertés individuelles. Effectivement, il n'est plus nécessaire d'avoir une base de données biométriques, l'empreinte biométrique demeurant sur soi, au cœur de la carte à puce. A titre d'exemple, différentes solutions de carte à puce, fondées sur les empreintes digitales, sont en cours d'études. Il s'agit des procédés suivants :

- Match off Card : les références biométriques sont stockées dans la carte à puce. L'authentification se fait à travers un terminal externe. La décision est prise par ce terminal externe ayant accès aux références biométriques, ce qui les expose au monde extérieur.

- Match On Card : l'identification utilise toujours un terminal externe pour acquérir l'empreinte digitale. Mais dans ce cas, la carte à puce comparerera les données et prendra la décision. Les références biométriques ne sortent donc pas de la puce et ne sont pas exposées au monde extérieur.

- Partial Match On Card : les cartes à puce ayant de faibles capacités de calcul, la solution de ce procédé devient difficilement utilisable avec des paramètres biométriques de grande taille qui offrent une sécurité accrue. Le partial Match On Card permet de laisser le terminal externe réaliser les calculs lourds et complexes, tout en laissant la décision à la carte à puce.

- System On Card : la carte contient le capteur d'empreintes. Elle est donc autonome, la décision n'est pas communiquée au monde extérieur[9].

L'intérêt de mener une étude approfondie sur la recherche fondamentale et appliquée de cette matière a conduit la CNIL à entreprendre, avec les professionnels concernés, une étude d'ensemble sous l'éclairage de la protection des données personnelles et de la vie privée. Il convient cependant de constater que la CNIL a autorisé en 2005 l'installation de 34 dispositifs de

[9] Recherches fondamentales menées par le Groupe Gemalto qui regroupe depuis 2000 les sociétés Gemplus et Axalto. Gemalto est l'un des leaders de la carte à puce.

contrôle d'accès par système biométriqu et en a refusé 5 (en 2006, 299 ont été acceptés et 9 refusés)[10].

Les résultats obtenus au cours de cette enquête tendent à indiquer que l'uniformisation des systèmes de contrôle d'accès pour une même entreprise, sur l'ensemble de ses sites dans le monde, est aujourd'hui envisageable. Pour cela, deux décisions stratégiques devront être arrêtées à un niveau central. Il s'agira de choisir le vecteur d'accès (badge et/ou biométrie) et la technologie retenue pour ce système. Nous avons constaté précédemment que cette technologie doit être « ouverte » et répondre aux protocoles ISO. Il conviendra de mettre en place une politique de gestion des clés de chiffrement et d'imposer celles-ci aux fournisseurs.

Pour autant, les sites les plus anciens ne supporteront certainement pas les nouvelles technologies répondant aux critères supra, il s'agira de prendre en compte l'impact financier du remplacement des interfaces « têtes de lecture ». Outre l'aspect budgétaire (détermination du coût et de qui paye : niveau central ou chaque site/pays), il faudra intégrer l'inertie de la mise en œuvre.

Ces réflexions conduisent à mener obligatoirement en amont un audit interne sur l'ensemble des sites afin de réaliser un état de l'existant (version des systèmes, normes ISO..) et de dresser la liste des fournisseurs utilisés et potentiels. Le vecteur badge, qu'il intègre ou non des données biométriques, véritable passeport de l'entreprise, reste, sans aucun doute, un défi pour demain.

5. Discussion

Bien plus qu'une simple ouverture sécurisée de porte, un système de contrôle d'accès doit assurer la sécurité d'accès aux locaux de l'entreprise ainsi que la protection des biens, du personnel et des visiteurs. Aujourd'hui, les entreprises ont besoin de flexibilité et d'une forte adaptabilité en horaires, notamment dans le domaine de la logistique. Les systèmes de contrôle d'accès sont paramétrables pour répondre aux spécificités de chaque société. Ces systèmes peuvent disposer des fonctionnalités suivantes (non exhaustives compte tenu des évolutions technologiques en cours comme nous l'avons vu ci-dessus) :

- définition hiérarchisée du contrôle d'accès (accès personnalisé individuellement en fonction de groupes de salariés, clients, visiteurs, sous-traitants…) ;
- définition des droits attribués (visualisation, modification, création) ;

[10] Rapport d'activité 2006 de la CNIL.

- adaptabilité des horaires d'accès en fonction des horaires du planning ;
- définition des périodes de zones ouvertes (ex : journées portes ouvertes) ;
- vision globale des accès autorisés grâce à la planification des accès ;
- comparaison entre les « badgeages » de gestion des accès et de gestion des temps ;
- anti pass-back (pour éviter que deux personnes puissent utiliser le même badge pour entrer sur un même site), unicité du passage ;
- mémorisation des anomalies ;
- historique des accès permettant l'analyse des flux ;
- contrôle total des flux (entrées / sorties) ;
- identification des personnes (gestion des accès et surveillance des visiteurs, traçabilité) ;
- couplage possible avec des portillons d'accès ;
- sécurisation renforcée des zones à risques ;
- reconnaissance biométrique intégrée ;
- mise en place d'un « badgeage » spécial en gestion de crise (gestion des habilitations).

Cependant les systèmes de contrôle d'accès génèrent leurs propres risques. En effet, il est inutile de déployer un tel système en l'absence d'un tourniquet ou de tripode pour réguler et contrôler les flux, dès qu'une porte est ouverte par un collaborateur, tous ses collègues non habilités peuvent s'y engouffrer. La possibilité d'échanger ou de se passer les badges entre collaborateurs pour accéder à un site protégé existe. Cela est quelquefois le cas avec des personnels intérimaires, employés régulièrement dans la logistique, à qui l'on remet un badge actif mais non nominatif et sans photo pour la durée de leur mission. Très souvent, ces badges ne sont pas déposés le soir au poste de sécurité et une autre personne peut donc le réutiliser sans vérification de l'identité de la personne (d'où l'intérêt aussi des reconnaissances biométriques intégrées).

Une autre grande difficulté consiste à activer l'anti-pass back sur des sites importants de l'ordre de 700 à 2000 personnes et il faut une grande discipline des collaborateurs qui, si pour

une raison ou pour une autre ne « badgent » pas en sortie (sortie par exemple en passager dans un véhicule de direction...), ne peuvent plus entrer et imputent la faute au système. De fait, l'anti pass-back génère beaucoup d'incidents. Naturellement des solutions existent, par exemple en rajoutant un gardien au poste de sécurité pour faire ouvrir électroniquement la barrière par celui-ci une fois que l'ensemble des passagers a badgé, mais cela induit des coûts supplémentaires...De plus, lorsqu'il y a une centralisation intersites du système et que toutes les portes de sorties ne sont pas équipées de tourniquet (les sièges par exemple), les collaborateurs peuvent sortir en groupe avec un même badge et ne plus pouvoir entrer sur les autres sites car ils ne sont pas officiellement sortis du précédent. Enfin, et cela n'a aucun caractère d'exhaustivité, il faut bien sûr que dès qu'un badge est perdu, le détenteur avertisse immédiatement le service de sécurité concerné afin qu'il soit désactivé.

Concernant « les bons produits » pour le contrôle d'accès, on peut dire que les équipements des grandes enseignes actuellement sur le marché se valent à peu près tous. La différence tient dans le service après vente et dans la capacité notamment à intervenir rapidement pour des coûts abordables (proximité de l'équipe d'intervention technique). Pour une grande société installée dans plusieurs pays qui recherche la standardisation et la simplification maximale (centralisation du contrôle d'accès avec badge unique pour tous les sites, par exemple), le problème est de faire appel à un fabricant international avec un maximum de représentations ou fournisseurs locaux. Aujourd'hui cela n'est pas encore le cas pour de nombreux groupes de la supply chain et souvent les entreprises ont scindé en régions voire en sous régions leurs systèmes de contrôle d'accès. Toutefois, avec l'évolution des technologies d'une part et la prise de conscience par les fabricants de cet enjeu stratégique d'autre part, notamment en termes de parts de marchés, des solutions commencent à se faire jour.

Nous avons également constaté que les systèmes de contrôle d'accès physique peuvent contribuer au renforcement de l'image de l'entreprise et participer à son système d'intelligence économique, notamment pour la protection de son information [Besson et al., 2006].

L'information a une valeur marchande [Milon, 1999], c'est une véritable richesse pour l'entreprise qui se doit de la protéger. Cette protection est essentielle pour l'entreprise car la veille existe aussi chez les concurrents. Rien ne sert de faire de la veille si on ne maîtrise pas les fuites d'informations sensibles. A l'ère de l'informatique et des réseaux, il ne faut pas pour autant obérer les intrusions physiques. Aussi, ne pas définir une politique de sûreté, c'est s'exposer à des risques financiers importants, voire à la faillite de l'entreprise. Se protéger efficacement revient à mettre en œuvre un ensemble de bonnes pratiques que l'on appelle une « politique de sûreté », indispensable pour réduire ces risques. Cette politique n'est valable dans le temps que si elle est évaluée régulièrement contre les nouvelles menaces (dans le domaine du contrôle d'accès, ces nouvelles menaces peuvent être liées à l'évolution de la technologie et aux

procédures dites de contournement : copie de badge d'accès à distance ou « skiming » par exemple) et les changements de l'organisation (fusions/acquisitions). Dès lors, il devient nécessaire, voire impératif pour une entreprise de mettre en place un système de contrôle des entrées et des sorties de l'ensemble des personnes entrant sur un site. L'entreprise doit assumer le risque après l'avoir identifié, analysé et évalué en termes de probabilité et de conséquences prévisibles. C'est ce qu'on peut appeler la sagesse. Celle-ci repose sur les notions de seuil d'acceptabilité du risque et d'éthique du risque. La prise de risque accompagne toute forme d'action. Elle doit déboucher sur une gestion intelligente et réaliste qui éclaire la responsabilité de chacun. Le risque, à travers les notions de « responsabilité civile et/ou pénale » et de mise en danger d'autrui introduite par le nouveau code pénal de 1994, est devenu aussi juridique. Cette dimension a par ailleurs tendance à s'amplifier quotidiennement jusqu'à en devenir presque paralysante !

Face à une actualité tragique encore récente, la directive européenne n°96/82/CE du 9 septembre 1996, dite SEVESO, a complété le champ juridique du risque industriel. Cette directive communautaire a été transposée dans le droit national par un arrêté du 10 mai 2000 dit « SEVESO II », publié au journal Officiel du 20 juin 2000. Ainsi, dans ce nouveau cadre, l'entreprise doit définir une véritable politique de prévention des accidents majeurs et informer le voisinage des risques encourus, mais également se prémunir des actes de malveillances susceptibles d'être l'élément déclencheur de ces accidents. Les systèmes de contrôle d'accès physique prennent ici toute leur importance. Par ailleurs, les normes internationales ou européennes qui encadrent la mission de protection des entreprises seront obligées dans les années à venir de tenir compte de l'effet du 11 septembre 2001. Les attentats de New York et de Washington, ceux qui ont suivi en plusieurs endroits de la planète, ont introduit le risque terroriste dans le concept de protection. Chaque établissement, site ou partie de site classé SEVESO est désormais une bombe en puissance. Les populations avoisinantes sont prises en otage par des groupes terroristes internationaux. Aux Etats-Unis et au Japon, la communauté de la gestion du risque réexamine l'ensemble du concept. Les pouvoirs publics seront, ici comme ailleurs, de plus en plus partie prenante de la mission de protection de l'entreprise. Cet aspect du terrorisme, sans paranoïa excessive, peut parfois remettre en cause l'équilibre économique de toute entreprise en cas d'accident.

Aussi pour être ou pour rester efficace dans le temps, la gestion des risques doit faire l'objet de procédures d'audit qui garantissent la qualité du diagnostic des vulnérabilités et la pertinence du programme de traitement des risques mis en œuvre. Il faut prévoir régulièrement des audits de conformité à la politique et aux normes. L'analyse des performances doit dégager des pistes d'amélioration. Les entreprises opèrent dans des environnements eux-mêmes en constante évolution. Il convient donc de mettre en place des mécanismes pour faciliter l'indentification de ces évolutions internes et externes de façon à pouvoir adapter le programme

de gestion des risques à ces changements. Les procédures d'audit doivent garantir la présence de contrôles appropriés aux activités de l'entreprise et ces procédures doivent être comprises et respectées par tous. Elles doivent permettre de déterminer notamment si les mesures adoptées ont donné les résultats escomptés, si les procédures adoptées et les informations recueillies pour dresser le diagnostic des vulnérabilités et l'évaluation sont appropriées aux objectifs poursuivis, si une meilleure connaissance aurait permis de prendre de meilleures décisions et d'améliorer la qualité du diagnostic des vulnérabilités dans le futur.

Au-delà du simple aspect technique, il ressort de la précédente étude que les systèmes de contrôle d'accès physique participent pleinement au développement stratégique de l'entreprise. Ils font partie intégrante de la gestion des risques de sûreté au sein de l'organisation, ces derniers se répartissant en quatre groupes : les atteintes aux personnes (agressions d'ordre moral ou physique concernant tous les personnels et partenaires de l'entreprise et les membres de leurs famille), aux biens matériels (dégradation, atteintes à l'intégrité des systèmes d'information et de communication ou des centres vitaux de l'entreprise...), au capital immatériel (infiltration mafieuse ou sectaire, acte d'espionnage, rumeurs...) et celles liées à des déficits de management du risque sécuritaire global (niveau de formation insuffisant ou inadapté en matière juridique et jurisprudentielle, de protection de la vie privée, de vision stratégique de la mission protection...). Ainsi, compte tenu de l'importance que représentent les systèmes de contrôle d'accès physique, niveau le plus critique en termes de protection, leurs choix doivent être particulièrement adaptés. Les recherches technologiques en cours sur les vecteurs badges sans contact à 125 Khz et/ou 13,56 MHz, démontrent si besoin les enjeux stratégiques et financiers de ces systèmes. Dans ce domaine, deux grands chantiers sont en cours : celui de l'évolution du contrôle d'accès vers plus de sécurisation de l'identification par l'intégration de techniques de biométrie et les recherches et développements pour faire du vecteur badge un véritable passeport d'entreprise pour les grands groupes disposant de plusieurs sites répartis dans divers pays. Il semblerait donc que l'uniformisation des normes dans ces domaines pourrait être l'un des enjeux de demain.

6. Bibliographie

BESSON B., POSSIN J.C., 2006. L'intelligence des risques. Ifie, 450 p.

CARBONE V., MEUNIER C., 2006. Supply Chain Management : portée et limites – l'apport de la théorie des réseaux, AIMS 2006, Annecy, 17p.

CHEVREAU F.R., 2007. Les processus de maîtrise des risques à l'épreuve de la culture de sécurité : nouvelle approche de la culture de sécurité, nouvelles perspectives, AIMS 2006, Annecy, 28 p.

DORIZZI B., GARCIA C., 2007. Biométrie multimodale. Anales des télécommunications, Vol 62 N°1-2, 272p.

FINKENZELLER K.,2003. Fundamentals and applications in contacless smart card and indetification. Seconde edition, John Wiley & Son, 501 p.

GAULTIER-GAILLARD S. et LOUISOT J-P., 2005. Diagnostic des risques, AFNOR 200p.

GERARD E., 2006. Sécurité aérienne l'Europe en Tête ? Les carnets du CAP p 27-35.

KERVEN G-Y et RUBISE P., 1991. L'archipel du danger, introduction aux cindyniques, CPE Economia, 444p.

KOVACICH, G. L., & HALIBOZEK, E. P., 2005. Security Metrics Management. Boston, MA, Butterworth-Heinemann, 352 p.

KOVACICH, G. L., & HALIBOZEK, E. P., 2003. The manager's handbook for corporate security establishing and managing a successful assets protection program. Boston, MA, Butterworth-Heinemann, 463 p.

MAQUET Y., 1991.Des primes d'assurances au financement des risques : éléments fondamentaux de Risk Management. Brylant Bruxelles, 253p.

MAQUET Y., 2007. Mag-Sécurs n°17. Le besoin de sécurité et le goût du risque, 3p.

MILON A., 1999. La valeur de l'information : entre dette et don. PUF, coll. Sociologie d'aujourd'hui, 232p.

MONGIN P. et TOGNINI F., 2006. Petit manuel d'intelligence économique au quotidien. Dunod, 182p.

REASON J..1998. Achieving a Safe Culture: Theory and Practice, Work & stress, 12, 293-306.