Dynamique des règles de sécurité et modes de contrôle

Emmanuel DAUVIN
Université de Namur
emmanuel.dauvin@unamur.be

Annick CASTIAUX
Université de Namur
annick.castiaux@unamur.be

Résumé :

Dans cet article, nous nous intéressons aux processus de négociation des règles de sécurité liées à la gestion et à l'utilisation des systèmes d'information. À partir d'une collecte de données qualitatives réalisée dans une entreprise du secteur bancaire où cette sécurité est d'importance stratégique, nous analysons à l'aide de la Théorie de la Régulation Sociale (TRS) la manière dont se créent et se transforment les règles de sécurité. Nous identifions quatre modes de contrôle successifs que nous avons appelés : la sécurité autonome, la sécurité obligatoire, la sécurité négociée et la sécurité contrôlée. Ces modes suivent une dynamique dépendant à la fois d'un système de contrôles que nous mettons en évidence et des enjeux des acteurs de la sécurité qui, en situation, négocient et construisent les pratiques effectives.

Le cas sélectionné nous sert de point d'ancrage et de révélateur des relations sociales qui se développent entre les acteurs. Dans le domaine industriel des banques et des paiements électroniques, la sécurité et le contrôle sont au cœur de l'activité économique, et la sécurisation des systèmes d'information est un souci permanent pour sa pérennité. En effet, de la fabrication des cartes aux paiements dans les points de vente, l'activité de paiement électronique est totalement informatisée ; une défaillance sécuritaire peut avoir des conséquences importantes pour l'ensemble des acteurs de la chaine.

La méthode d'investigation est l'étude de cas et la collecte des données repose sur l'observation participante et non participante, sur l'étude de données secondaires telles que des documents internes, ainsi que sur la conduite d'entretiens semi-directifs. Cette approche qualitative est idéale pour montrer comment les acteurs font d'abord émerger un nouveau concept pour redéfinir les frontières des nouvelles règles du jeu, convenant ensuite des règles de sécurité compatibles, d'une part, avec leurs enjeux d'autonomie et de contrôle, et d'autre part, avec les exigences de la norme de sécurité.

Mots-clés : Sécurité des systèmes d'information, Théorie de la régulation sociale, Recherche qualitative, Étude de cas

Dynamique des règles de sécurité et modes de contrôle

1 Introduction

La sécurité des systèmes d'information[1] se distingue de la sécurité industrielle par la nature de son objet, les systèmes d'information, et surtout par la nature « virtuelle », mais bien réelle, des risques qu'elle entend juguler. En effet, il n'y a pas ici de risque physique, d'accident corporel, d'incendie, ou d'événements dramatiques. Le tangible fait défaut. Cependant, en termes de risques industriels, la frontière entre le virtuel et le physique n'est pas aussi claire et les deux mondes sont de plus en plus imbriqués (Alcaraz, Roman, Najera, & Lopez, 2013; Miller & Rowe, 2012).

Notre expérience de terrain dans la gestion de la sécurité des systèmes d'information nous a amenés à nous interroger autant sur les règles de sécurité elles-mêmes que sur les processus qui participent à leur émergence. La question n'est pas neuve, mais les recherches n'ont pas épuisé la problématique de la sécurité et de la gestion des situations à risque et des crises (de Terssac, 2013; Gilbert, 1998; Laroche & Steyer, 2012; Portal, 2009) dans la société moderne. Elle est d'actualité tout particulièrement dans le contexte des systèmes d'information. En témoignent les incidents médiatisés ces dernières années. Les conséquences financières et non financières peuvent être importantes, surtout en cas de fraudes (Summers, 2009), et les enjeux sécuritaires dépassent les frontières de l'entreprise concernée, se propageant à l'ensemble de la société (Beck, 2008). Cette question de la protection des systèmes d'information est particulièrement pressante dans les secteurs bancaires et d'assurances qui doivent faire face à l'augmentation des cas de fraudes (Ernst & Young, 2009).

Le recours à la normalisation des pratiques, c'est-à-dire ici à conformer les pratiques à un ensemble de prescriptions définies par une instance externe à l'organisation et donnant lieu à une certification de conformité, est un des moyens à la disposition des entreprises pour s'assurer de l'application des règles sur le terrain. Ceci est à la base de la garantie de qualité à laquelle tous les secteurs industriels doivent se conformer depuis de nombreuses années, à des

[1] Nous préférons "sécurité des systèmes d'information" à "sécurité informatique", car il y a pour nous dans cette première appellation, une dimension systémique qui intègre des règles, des machines de traitement, des acteurs et un important volet organisationnel.

degrés et selon des dispositions diverses. Avec le développement croissant des services et produits virtualisés, l'industrie informatique est concernée par l'application de normes et de standards liés à la sécurité et adaptés au contexte d'application. Dans les secteurs financiers et bancaires, la normalisation des pratiques sécuritaires, dont le paiement électronique est une activité particulière, est au cœur de notre cas d'étude.

Notre objectif est de contribuer à enrichir la littérature en gestion des systèmes d'information en procédant à une analyse des processus de régulation des règles de sécurité. Pour cette analyse, nous mobilisons la Théorie de la Régulation Sociale (TRS) qui l'est peu dans ce contexte de la sécurité des systèmes d'information, mais qui l'est remarquablement bien dans celui de la sécurité des systèmes industriels (de Terssac & Mignard, 2011; de Terssac, 2013).

À cette fin, nous avons suivi un projet de normalisation et analysé ses implications. Cette recherche sur le terrain nous sert de point d'ancrage pour comprendre les enjeux des acteurs, les relations qu'ils établissent et entretiennent, mais aussi pour appréhender leurs interprétations des changements introduits par la normalisation, en termes de pratiques et de règles, de relations de pouvoir et de relations sociales.

2 Problématique et question de recherche

Grâce à une étude exploratoire réalisée sur le terrain en 2010, nous avons mis en évidence lors d'observations la présence de plusieurs règles de sécurité des systèmes d'information : la gestion des mots de passe, la gestion des droits d'accès ou encore celles du cycle de vie des identités logiques. Ces règles participent à un ensemble que nous avons appelé la pratique de contrôle des accès. Elles sont répétitives, structurées et partagées par l'ensemble des acteurs de l'organisation. Or les règles qui constituent ces pratiques ne sont pas que les règles écrites et immuables des « *Security Policies* » : les acteurs engagés dans l'action les renégocient, les adaptent, en prennent possession et en inventent de nouvelles. Notre questionnement concerne ces dynamiques et les règles du jeu que les acteurs adoptent pour mettre en place les règles de gestion de la sécurité des systèmes d'information. Quels sont les modes de contrôles et comment structurent-ils la manière dont les acteurs construisent et transforment les règles de sécurité des systèmes d'information ?

Cette question demande de comprendre les logiques d'acteurs et les relations sociales qui structurent les règles de gestion de la sécurité des systèmes d'information. Ces règles du jeu sont pratiquées par les acteurs qui s'organisent à travers une structure pour répondre à un

impératif sécuritaire sous les multiples contraintes, parfois contradictoires, de systèmes sociotechniques aux risques nombreux et difficilement prévisibles (Rasmussen, 1997).

Nous nous intéressons bien plus au « comment » qu'au « quoi » de la dynamique des règles de sécurité. C'est pourquoi nous passons préalablement par une description du cas qui nous sert de « poste d'observation » de la problématique. Le processus de normalisation n'est pas considéré pour lui-même, il est un alibi pour interroger les acteurs. Que mettent-ils en jeu dans ce processus ? Comment reconfigurent-ils les relations de pouvoir dans l'organisation ? Quelles marges de manœuvre ont-ils pour cela ?

3 Approche par la Théorie de la Régulation Sociale

La Théorie de la Régulation Sociale (TRS) offre un cadre théorique pertinent pour ouvrir notre champ d'études à l'acteur social et à sa capacité de construire des règles et d'y consentir (Reynaud, 1991). La dynamique des règles de sécurité à travers le projet de normalisation constitue une rupture, et la base de nouvelles règles sociales qui se traduisent sur le terrain par l'émergence ou la transformation des règles sécuritaires. Deux raisons nous sont importantes dans la justification de cette démarche et nous amènent à faire le choix de ce cadre théorique. D'abord, nous ne nous limitons pas à l'analyse des règles sécurité, mais nous incluons les relations entre les acteurs. Les régulations, c'est-à-dire les « processus de production de règles et d'orientation des conduites des acteurs dans un espace social déterminé » (Reynaud, 1988), sont au centre de notre cadre théorique. Ensuite, les acteurs ne sont pas seulement ceux qui sont impliqués au premier degré dans le projet, mais aussi tous ceux qui participent aux échanges sociaux de négociation de règles, une communauté réunie par les règles (Reynaud, 1991), potentiellement l'ensemble des acteurs et des parties prenantes.

Ajoutons encore que de Terssac (2011; 2013) fait de la TRS un usage central pour l'analyse des relations sociales autour de la dynamique des règles de sécurité industrielle. Son approche qui met en évidence les processus d'appropriation des règles de sécurité par les acteurs dans le domaine industriel n'est pas sans lien avec notre recherche. En effet, que ce soit dans le monde virtuel de l'électronique ou dans celui bien matériel de l'industrie manufacturière, « la sécurité consiste à poser des règles pour garantir la continuité du fonctionnement productif d'un système sociotechnique » (de Terssac, 2013). La TRS propose une grille de lecture des négociations de règles à travers trois régulations de base. La régulation de contrôle nous offre une lecture des logiques des règles que le management met

en place pour contrôler les activités des employés (Reynaud, 1988). Quant à la régulation autonome, elle s'adresse aux règles que les opérateurs construisent pour garantir leur autonomie. Enfin, la régulation conjointe est le résultat de la négociation entre les opérateurs et le management, d'où émergent des règles effectives observables sur le terrain.

Pour Reynaud (1993) les règles sont aussi des conventions en ce sens que, même dans les situations de fortes contraintes, elles demandent un consentement des acteurs. Se soumettre à la règle, c'est aussi l'anticiper et en prévoir la réalisation, comme réponse à un problème coordination et de rationalité pure qui intègrerait la totalité des causes et des conséquences.

D'un point de vue empirique, l'opérationnalisation de ce cadre théorique a pour objectif de rendre compte de la dynamique de la régulation sociale, de caractériser les règles du jeu dans lequel elle prend place. Notre approche consiste à identifier les régulations en concurrences, à analyser les relations de pouvoir spécifiques et à les positionner dans la perspective des acteurs et des objets des régulations. Elle met en évidence les éléments dont les effets combinés contribuent à mettre en place de nouvelles régulations (Reynaud, 1988).

La sécurité est un composant important de la gestion des systèmes d'information de l'entreprise ; elle met en place des dispositifs afin de l'organiser (Baskerville, 1993). Les membres de l'organisation définissent comment sécuriser les informations et avec quels équipements ou procédures, et surtout qui les contrôle et comment ce contrôle est exercé. Faisant référence au cadre théorique que nous avons choisi, plus qu'une liste de tâches, ce sont des interactions sociales par lesquelles les acteurs définissent, transforment et contestent les pratiques. Ce sont les règles du jeu. Elles ont pour objectif de réguler les relations entre les acteurs et de garantir à l'organisation la protection des données et des systèmes d'informations tout en permettant à ces mêmes acteurs de satisfaire à leurs objectifs d'une part d'autonomie dans la manière de remplir cette mission, et d'autre part de production (de Terssac, 2013), c'est-à-dire, dans notre cas, la livraison de services informatisés. Elles constituent un ensemble de normes sociales, qui organisent la sécurité des systèmes d'information dans l'organisation.

4 Terrain de recherche

4.1 Description du cas

Le cas retenu dans notre étude est situé chez un opérateur de paiements électroniques sous licence Visa et MasterCard. La principale activité sur laquelle nous avons concentré notre

étude est le traitement des transactions électroniques de paiement dans les points de vente. Cette activité, appelée *Acquiring*, consiste à collecter les transactions de paiement auprès de commerçants à l'aide d'un terminal dédié installé dans les points de vente ou à l'aide d'un terminal virtuel s'il s'agit de l'intégrer à un site internet marchand. Notre étude a été réalisée dans les départements qui sont directement en contact avec la sécurité opérationnelle de ces activités : les départements informatiques, que nous nommons les départements IT, et le département de sécurité.

Cette activité doit impérativement répondre aux critères de la norme de sécurité PCI-DSS (Payment Card Industry – Data Security Standard) car l'opérateur réalise à l'aide de ses systèmes informatiques le traitement, le stockage et la transmission de données relatives aux cartes de crédit (PCI Security Standards Council, 2010). Cette norme est un référentiel comportant 12 catégories d'exigences issues historiquement de la famille des normes ISO27000 (Rowlingson & Winsborrow, 2006). Il est publié et maintenu par le Security Standards Council fondé par American Express, Discover Financial Services, JCB International, MasterCard Worldwide et Visa. Ces propriétaires de schémas de paiement imposent aux opérateurs de leurs licences d'exploitation de faire certifier leurs systèmes d'informations selon cette norme. La motivation affichée par le Council est la réduction des fraudes exploitant le *skimming*, c'est-à-dire le vol d'informations de cartes de crédit pour réaliser des transactions de paiement frauduleuses. Il s'agit de faire face à un ensemble de techniques de piratage relativement faciles à mettre en œuvre, très répandues, qui permettent la fraude parfois à grande échelle et le vol d'identité (Allison, Schuck, & Lersch, 2005; Paget, 2007; Philippsohn & Thomas, 2003). Nous identifions cette obligation comme un point pivot entre la liberté de l'opérateur d'organiser ses activités de manière optimale et l'intégration de contraintes externes à l'organisation.

D'emblée, les acteurs font face à l'obligation de leur entreprise de se soumettre à la norme. L'interprétation de la norme PCI-DSS (domaine d'application, critères de définition de ce domaine, exigences...) ouvre les discussions et soulève de nombreuses questions. Le cadre laisse une plus ou moins large place à l'interprétation de la part des opérateurs, des managers et des auditeurs, ces premiers chargés d'appliquer ces normes et ces derniers chargés de certifier leur application sur le terrain. Le PCI Council impose les critères de détermination du domaine d'application, mais il délègue aux opérateurs de paiements la responsabilité de définir l'ensemble des systèmes qui doivent répondre aux exigences de PCI-DSS.

Bonner et ses collègues (2011) ont analysé une technique générique pour la mise en œuvre de PCI et soulignent les difficultés que pose l'arrivée de nouvelles règles dans un environnement existant. Même si leurs travaux traitent principalement des aspects techniques de la gestion des systèmes informatiques, ils montrent que cette nouvelle situation force les acteurs à se positionner et à négocier de nouvelles règles de sécurité ou à renégocier des règles existantes. Nous avons également observé que l'entreprise disposait de pratiques de sécurité avant la décision de normalisation, n'ayant pas attendu de devoir se conformer à une norme externe pour développer la sécurité interne. Cela se traduit dans les procédures des opérateurs et des ingénieurs, et dans les dispositifs matériels utilisés pour sécuriser les infrastructures. Cette préexistence des pratiques est particulièrement intéressante pour envisager la recherche dans une perspective longitudinale. Cette analyse de terrain nous permet donc d'explorer la dynamique des règles et des relations sociales des acteurs, puisque ceux-ci, par l'introduction de la nouvelle norme, sont en situation de négociation des règles de sécurité nouvelles ou existantes. Ce terrain est donc particulièrement adapté à notre objectif de recherche.

4.2 La dimension organisationnelle

L'entreprise cible a pour mission de vendre des services des paiements électroniques de manière sécurisée avec en vue externe deux pôles importants : la fiabilité des paiements sous laquelle on retrouve la confidentialité et l'intégrité des données des transactions, et la disponibilité du service 24 heures sur 24 et 7 jours sur 7. Bien qu'il s'agisse d'une mission pour toute l'entreprise, deux types de départements sont en première ligne.

Les premiers sont les départements IT qui ont en charge toutes les étapes de conceptualisation et d'opérationnalisation des technologies, sur l'ensemble de la chaîne de valeur : design des infrastructures de services aux clients, développement des programmes informatiques, production et opération des technologies, des réseaux, des matériels, des données et des programmes. La division du travail est forte sur le plan horizontal mais faible sur le plan vertical. Les départements IT sont spécialisés pour piloter des infrastructures hautement complexes. Chacun d'eux est responsable d'une « tranche » de l'infrastructure : un département est en charge des équipements électroniques, un autre, des bases de données, un autre encore, des systèmes d'exploitation, et ainsi de suite. Leurs responsabilités couvrent toutes les étapes du design à la production. Ils jouissent de compétences et de budgets qui leur offrent une certaine autonomie et leur permettent de décider des projets d'infrastructure, des achats d'équipements, de l'organisation des activités de production, notamment pour

garantir la haute disponibilité des infrastructures. Cette autonomie leur permet d'atteindre leurs buts essentiellement internes, tournés vers la réalisation de performances techniques dans lesquelles ils excellent. Il est peu, ou rarement, fait référence à des buts externes en relation directe ou indirecte avec les services offerts aux clients de l'entreprise.

Le second type de département en première ligne pour la mission de sécurité est le département de Sécurité (SCY). Il rédige les politiques de sécurité au niveau de l'entreprise, et est par là le producteur d'une certaine norme. Il se présente comme un organe de contrôle dont il définit lui-même les modalités. On pourrait donc l'assimiler à un département interne d'audit. Il exerce aussi un rôle prescriptif des règles en éditant des politiques de sécurité, ou *Security Policies*, et en rédigeant des recommandations (contraignantes ou non) dans le cadre des projets ou dans les rapports d'incidents. Il a enfin un rôle préventif : il communique aux collaborateurs et managers les bonnes pratiques à adopter et les points qui doivent faire l'objet d'une attention accrue.

Les collaborateurs du département de Sécurité sont très qualifiés, la plupart possédant une thèse de doctorat en électronique, mathématique ou informatique, tandis que d'autres ont acquis leur spécialisation au fil des ans et sont très expérimentés. La présence de ces collaborateurs expérimentés assure la transmission des connaissances et compétences, ce qui maintient un haut niveau d'expertise collective et individuelle. On observe également une forte standardisation des qualifications, notamment par les formations spécialisées des collaborateurs. Nous faisons le même constat d'autonomie que pour les départements IT.

Utilisant le vocabulaire de la systémique des organisations (Mintzberg, 1998, 2003; Nizet & Huybrechts, 1998; Pichault & Nizet, 2000), l'entreprise cible s'apparente à une organisation professionnelle, mais le grand nombre de procédures internes fait apparaître des caractéristiques d'une bureaucratie.

5 Méthodologie

5.1 Étude de cas

Afin de répondre à notre question de recherche formulée en Comment, nous mettons en place une démarche par étude de cas (Yin, 2009) auprès des différents acteurs de l'entreprise cible impliqués dans les décisions, la gestion opérationnelle et l'utilisation des systèmes d'information. L'approche qualitative, justifiée notamment par la visée exploratoire de notre travail, nous permet de saisir le sens, socialement construit, des actions des acteurs en

interaction avec leur environnement, et comme réalité multiple (Merriam, 2002). Cette démarche est orientée vers la compréhension des éléments qui constituent les conduites des acteurs dans leur situation. Une caractéristique des analyses qualitatives est la richesse et le caractère englobant avec un potentiel fort de décryptage de la réalité (Miles & Huberman, 1999).

Pour Cusin (2008, 2009), les recherches qualitatives en management étudiant des sujets sensibles comme la sécurité, font face, plus que les autres, à des difficultés méthodologiques qui peuvent porter atteinte aux qualités de fiabilité, de validité et de vraisemblance des résultats, au sens de Guba et Lincoln (1985). La libre parole des interviewés, ainsi que l'accès aux informations et au terrain peuvent être très limités en raison du caractère sensible du sujet étudié. Toutefois, notre recherche bénéficie d'un accès privilégié au terrain grâce à notre présence importante au sein de l'entreprise cible et à la volonté de celle-ci de s'impliquer dans la recherche. Cet accès offre la possibilité de cibler des groupes d'utilisateurs pertinents et de les observer, particulièrement en ce qui concerne leurs pratiques quotidiennes. Nous avons aussi la possibilité de participer à certaines réunions. À la demande de l'entreprise cible, les documents, les informations contenues dans les rapports d'interviews sont traités en toute confidentialité. Le processus peut s'avérer complexe au premier abord, mais des mesures simples de protection peuvent prévenir les principaux risques (Thietart, 2007, p. 260) de non-respect de la confidentialité du matériel de recherche.

Cusin recommande de privilégier l'analyse en profondeur d'un nombre limité de cas choisis et de multiplier les entretiens pour atteindre la saturation sémantique. Il recommande aussi de faire preuve d'opportunisme méthodologique en n'hésitant pas à ajouter à son échantillon des cas qui n'étaient pas envisagés au départ mais qui se révèlent riches et intéressants (Cusin, 2009). Cette approche est cohérente avec la méthode des cas préstructurés présentée par Miles et Huberman (1999) pour aborder les situations contraignantes en temps et en complexité. Ces auteurs recommandent de circonscrire le champ d'étude du cas préalablement à la collecte des données et de procéder à plusieurs itérations de collectes de données si cela s'avère nécessaire.

L'étude de cas présentée dans cette recherche met en œuvre les techniques en trois étapes : préparation, collecte et analyse (Quivy & Van Campenhoudt, 2006). Dans un premier temps dédié à l'approche du terrain et à la préparation, une étude exploratoire permit un repérage large des problématiques propres aux pratiques des règles dans le cadre général de la sécurité

des systèmes d'information. Le projet de normalisation, ou projet PCI, a émergé comme pivot dans la négociation de règles. Nous avons vérifié à cette occasion la faisabilité d'une étude dans ce cadre et obtenu les autorisations nécessaires. C'est à cette étape de préparation que nous avons réalisé les premières interviews de managers et de collaborateurs. Celles-ci avaient pour objectif de prendre contact avec le terrain et de développer un climat de confiance tout en initiant les observations, notamment du contexte organisationnel.

Le deuxième temps a pour objectif d'alimenter l'étude en données qualitatives. Il a commencé par une volumineuse collecte de données secondaires composées de plus d'un millier de documents : courriers électroniques, rapports de réunions, rapports techniques et documents variés traitant de sécurité. Nous avons réalisé des observations plus spécifiques et plus ciblées pour approfondir les concepts utilisés par les acteurs afin de bien en comprendre le sens. Nous avons utilisé un questionnaire semi-directif. Il s'agit d'un guide assez général dont les questions sont ouvertes et les principaux thèmes sont abordés largement mais néanmoins cadrés dans le sujet de notre recherche. L'utilisation de ces trois techniques, 1/ les observations participantes ou non, 2/ le recueil de données secondaires, notamment les documents et les e-mails, et 3/ les entretiens, permet de croiser les résultats, de faire converger et de consolider les discours des acteurs (Creswell & Miller, 2000).

La principale collecte d'information est constituée par vingt interviews réalisées entre avril et août 2013, et d'une durée de 30 à 60 minutes. L'expression des interviewés est libre mais orientée autour de quatre thèmes : 1/ la perception des acteurs sur les pratiques de sécurité et sur le projet de certification, 2/ leur autonomie d'action face aux règles de sécurité, et 3/ leur rôle et celui des autres, et 4/ le compromis de sécurité.

Les personnes interviewées sont issues principalement du département de sécurité SCY et des départements IT de l'entreprise cible, ce sont des directeurs, des cadres, des ingénieurs et des opérateurs impliqués à leur niveau dans la sécurité et dans la normalisation des pratiques débouchant sur la certification. À la fin de chaque entretien, toujours sous enregistrement, la personne était invitée à parler librement d'un aspect qu'elle n'avait pas encore abordé. Par la suite, hors enregistrement, la discussion se prolongeait parfois, des notes étant prises pour garder trace de ces propos. Grâce ces 20 interviews, l'ensemble du personnel fortement impliqué dans la problématique de sécurité a été rencontré. Une seule personne parmi les 20 a refusé l'enregistrement.

L'étude s'appuie sur des observations participantes et non participantes réalisées lors de réunions, ainsi que sur la collecte de données secondaires, c'est à dire des documents produits dans le cadre du projet ou, plus généralement, relatifs à la gestion de la sécurité. Le corpus constitué est caractérisé par une grande hétérogénéité de forme rendant l'analyse automatique difficile. En effet, la langue, le format et la structure des documents varient fortement. Les langues à l'usage dans l'entreprise sont l'anglais, le français et le néerlandais. Les formats sont l'e-mail, le document MS-Word, MS-PowerPoint, MS-Excel, MS-Visio et PDF. Quant à la structure, les documents MS-Word et PDF sont les plus structurés et les plus aisés à traiter ; les e-mails sont les moins structurés parce qu'ils contiennent souvent des « conversations » écrites, témoignages d'échanges entre les acteurs. Il reste néanmoins que l'ensemble de ce corpus constitue une véritable richesse pour le chercheur.

Le troisième temps est dédié à l'analyse et à l'interprétation. Nous avons opté dans un premier temps pour une stratégie inductive pour mettre en évidence les jeux dans lesquels les régulations prennent place et les règles du jeu qui sont ainsi (re)définies. Dans un second temps, une stratégie déductive à partir d'une grille de lecture renvoyant à la Théorie de la Régulation Sociale (Reynaud, 1988, 1991) nous permet de cadrer les actions des acteurs dans les régulations de contrôle, autonomes et conjointes. Il ne s'agit pas ici de tester des hypothèses, mais d'utiliser le langage de la théorie. Dans la pratique, nous procédons à l'analyse par des allées et venues entre ces deux stratégies afin de les enrichir mutuellement.

5.2 Dimension temporelle et dimension spatiale

La dimension temporelle du cas que nous étudions chez cet opérateur de paiements électroniques est centrée sur un projet d'entreprise dont l'objectif est l'obtention de la certification PCI-DSS. L'enjeu du projet est porté au niveau de toute l'entreprise, car ce certificat qui atteste de la conformité à la norme est indispensable à la poursuite des activités sous licence Visa et MasterCard, propriétaires des schémas de paiements. Nous identifions d'emblée trois phases successives du projet. La première correspond à la période avant la décision du management d'obtenir le certificat. Nous soulignons de nouveau que les pratiques de sécurité préexistaient à cette décision. La deuxième phase est celle pendant laquelle le projet de normalisation est piloté. La fin de cette période est marquée par l'obtention de la certification et la clôture du projet un peu plus tard. La troisième phase est post projet, elle est en prolongement du projet car la certification obtenue doit être renouvelée

annuellement. Le remplacement du dispositif de projet par un dispositif opérationnel en est la principale caractéristique. Il y a donc bien un avant et un après.

Dans sa dimension spatiale, le cas étudié couvre un premier cercle composé des départements IT et le département de Sécurité de Sécurité. En raison de l'omniprésence des systèmes automatisés pour le traitement des informations sur les paiements électroniques et sur les détenteurs de cartes, la dimension spatiale s'étend ensuite à l'ensemble de l'entreprise. Elle peut même dans certains cas particuliers inclure des parties prenantes externes, comme les clients. L'entité tierce qui délivre la certification est appelée dans le jargon de PCI le Qualified Security Assessor (QSA). Son rôle est de vérifier les pratiques effectives, d'émettre des recommandations et des conseils d'amélioration, et de finaliser la délivrance du certificat.

6 Analyse des résultats

L'analyse des interviews et des données secondaires nous a permis d'identifier quatre temps distincts qui caractérisent la dynamique dans laquelle les acteurs sont engagés et font évoluer les règles de sécurité. L'analyse nous montre aussi que ces quatre temps correspondent à des phases successives dans un processus d'élaboration de nouvelles pratiques de sécurité.

6.1 La sécurité autonome

L'analyse exploratoire nous a montré que les règles de sécurité préexistaient la décision de la direction, ce que les interviews confirment. Ce premier temps des règles de sécurité correspond à une période antérieure à la décision de la direction. À cette époque, la sécurité est située chez les ingénieurs des systèmes d'informations, membres des départements IT. Ceux-ci sont en contact direct avec les événements et ils disposent de l'autonomie d'action et de l'expertise technique pour garantir la sécurité des systèmes d'information pour toute l'entreprise.

> *Il y avait principalement dans notre entreprise, une philosophie de travail, une adéquation entre les services d'audit interne, ... et les contrôles, des autocontrôles. C'est-à-dire qu'on fait attention par nous-mêmes à la sécurité parce qu'on a eu des événements extérieurs. […] Nous avions une culture de sécurité. […] À l'époque chaque personne avait une certaine autonomie dans ses produits (note : le produit dont parle ce responsable est un service de paiement électronique) par rapport à un budget défini en début d'année et un budget qui était, nous on dirait, en coopération. C'est à dire qu'à la limite on ne savait pas qui était le client der-*

rière, mais le produit on le faisait. Et de ce fait-là on avait une autonomie pour gérer. (un responsable des départements IT)

C'est le temps de la sécurité des experts, de la sécurité de métier. Le savoir-faire fait partie de l'identité des ingénieurs, c'est eux qui « font » la sécurité.

Il était prévu que ce soient des pilotes (note : les opérateurs de jour et de nuit) qui durant les nuits probablement du dimanche au lundi, installeraient tout ce qui est patches sécuritaires. Donc ça, c'était positif en ce qui me concerne parce que ça permettait de rehausser un petit peu les compétences de ces pilotes et de leur donner justement plus d'autonomie. En remontant leur niveau de compétence. (un manager des départements IT)

De son côté, le département de sécurité reconnaît qu'il ne dispose pas de cette expertise de terrain. Son rôle consiste essentiellement à prescrire des recommandations mais sans possibilité réelle de les faire appliquer.

Nous ne sommes pas les gens qui ont défini tout ce qu'il faut faire, là on s'est reposé sur l'expertise des gens qui le font d'habitude. Nous, on n'est pas des experts réseau. C'est aux experts réseau de se débrouiller pour proposer quelque chose de viable. Parce que, nous, on peut proposer tout plein de choses, mais on ne sait jamais si ça va marcher, si c'est opérationnellement gérable. On sait si ça va marcher, mais ça c'est au moment où on le met en marche. (un directeur du département de sécurité)

La sécurité autonome est le reflet de l'autonomie des ingénieurs des départements IT. Les règles de sécurité ont à cette époque un ancrage fort dans leur métier grâce à leurs connaissances d'experts et aux moyens financiers dont ils disposent. Cette autonomie est leur capacité à faire mettre en œuvre leur conception d'un « produit » sécurisé.

6.2 La sécurité obligatoire

Dans ce deuxième temps, la certification PCI devient une fin, un objectif impérieux à atteindre. Qu'elles soient des départements IT, du département de sécurité ou de la direction, les personnes interviewées reconnaissent que l'obtention du certificat PCI est un impératif pour les activités de leur entreprise, même si nous avons constaté des degrés d'adhésion très variables d'une personne à l'autre. Un membre de la direction et un employé expliquent leurs points de vue.

PCI n'est pas une contrainte mais plus comme une partie inhérente aux produits et services qui constituent une partie de notre core business. (un membre de la direction)

PCI ? Je n'en pense rien de particulier, rien de spécifique, c'est une obligation qui est venue de la direction et aussi de Visa. Ils ont dû suivre ce qu'ils disaient (Visa) sinon il n'y aurait plus de boulot. C'est comme les autres certifications, il faut les suivre et appliquer les règles. (un employé)

Les activités concernées reposent fortement sur l'informatique ; une technologie très complexe contrôlée depuis sa création par les ingénieurs des départements IT. La direction n'a pas beaucoup de contrôle sur ces activités hautement qualifiées et craint ne pas obtenir la certification PCI indispensable pour la poursuite des activités commerciales. Elle prend un certain nombre de décisions et initie des actions en impliquant le département SCY pour maitriser le risque de non-conformité à la norme PCI et donc de non-certification. Il s'agit, selon nous, de l'initiation d'une régulation de contrôle dont les premiers concernés sont les départements IT. Nous observons à cette occasion la mise en place de plusieurs dispositifs.

6.2.1 Un dispositif de projet

Le premier dispositif est constitué autour de l'organisation du projet de normalisation et notamment par la distribution des rôles. Le département de sécurité reçoit de la direction de l'entreprise la responsabilité des relations avec l'auditeur externe. Dans ce cadre, sa mission est de défendre le dossier de certification auprès des instances externes dont Visa et Mastercard, mais surtout de formaliser des politiques de sécurité qui ne sont pas en deçà des exigences de la norme et de promouvoir, voire d'imposer, le développement de pratiques conformes et normalisées. C'est aussi un rôle d'agent de liaison dans une relation triangulaire avec les départements IT. Lors de l'évaluation par l'auditeur externe, les explications et les preuves de conformités sont apportées par les départements IT, mais leur défense auprès de cet auditeur est pilotée par le département de sécurité. Ce dernier peut donc jouer sur cette relation pour tenter d'imposer son point de vue et invoquer la mission reçue par la direction pour l'appuyer.

On essaie d'imposer. En fait non on ne peut pas imposer, on ne peut pas dire « c'est comme ça sinon je vais aller voir le chef (note : le CEO) » et c'est très rare que je doive aller voir le chef. Parce que d'habitude on arrive à quelque chose de

raisonnable, mais si c'est nécessaire, c'est nécessaire. (un directeur du département de sécurité)

6.2.2 Un dispositif de communication

Le second est un dispositif de communications d'entreprise qui nous montre que la distribution des rôles dépasse la structure organisationnelle du projet. En effet, par la communication sur le sujet vis-à-vis du personnel, tous les membres de l'entreprise sont impliqués. Il leur est demandé de respecter les politiques de sécurité et les instructions du département de sécurité afin d'obtenir la certification. Les moyens de communication sont importants : e-mails, distributions de tracts et de goodies, mais surtout la « certification interne ». Celle-ci consiste à inviter tous les membres de l'entreprise à répondre à un questionnaire-test de sécurité constitué de 25 questions sélectionnées aléatoirement. Les questions sont formulées dans la langue de l'utilisateur (le français ou le néerlandais). Un score supérieur à 75% donne lieu à un certificat personnel envoyé par email à l'employé et à son supérieur hiérarchique.

[La certification interne] vérifie chaque année […] que les gens sont bien conscients de ce que c'est PCI. (le chef de projet PCI)

Il s'agit ici d'impliquer un maximum d'acteurs et de généraliser l'objectif à toute l'entreprise. La sécurité n'est plus seulement l'affaire du département de sécurité et des départements IT, tous les travailleurs sont concernés ; du CEO aux opérateurs, personne n'y échappe. Cela a pour conséquence que le dialogue ne se fait pas uniquement à l'intérieur des départements IT et entre les spécialistes : les néophytes en sécurité sont invités à prendre un rôle actif dans la sécurité et ainsi participer à l'effort vers la certification PCI. Cette initiative a pour effet d'élargir l'espace de dialogue à toute l'entreprise. D'une certaine manière, les experts le deviennent un peu moins, et il s'installe une concurrence sur ce domaine réputé comme particulièrement confiné. Cette situation donne lieu à la possibilité de controverses sociotechniques et à leur résolution (Callon, Lascoumes, & Barthe, 2001). L'utilisation obligatoire d'une technologie de réseau privé sécurisé[2] pour accéder aux applications de paiement offre un exemple de controverses dans laquelle l'expertise des utilisateurs néophytes en sécurité est mise en concurrence avec celle des ingénieurs.

[2] Le réseau privé sécurisé, ou VPN, est une technologie qui peut s'avérer contraingnante pour les tâches quotidiennes des utilisateurs.

Ce que nous appelons la sécurité obligatoire est une régulation de contrôle dont le fonctionnement est piloté par la direction grâce à une structure de gestion par projet et par l'élargissement du champ d'application de la règle à toute l'entreprise. Cet élargissement est l'élément permettant l'ouverture vers la sécurité négociée.

6.3 La sécurité négociée

Le troisième temps de la sécurité est marqué par l'implication de nombreux acteurs et par un certain nombre d'innovations techniques comme la « Zone PCI », l'usage du VPN étendu à tous les utilisateurs, le « Vulnerability Management » (un processus répétitif d'installation des correctifs de sécurité). Pour réussir, le processus d'innovation ne doit pas rester confiné à la technique des experts des départements IT, il cherche une légitimité auprès du département de sécurité, et doit se faire accepter par les utilisateurs et recevoir l'approbation de l'auditeur externe. La sécurité négociée n'est pas forcément celle de la norme PCI, mais elle s'en revendique. Les acteurs font naitre un certain nombre de règles de sécurité qui sont le résultat de compromis.

> *Il y a pas mal de discussions avec les gens de la sécurité qui ont permis de définir des solutions intéressantes. À côté de ça il y a des cas où j'ai dû beaucoup résister pour ne pas me laisser embarquer dans des solutions où je prenais pour moi des choses qui manifestement ne doivent pas être faites chez moi. (un manager des départements IT)*

Pour le département de sécurité, cette négociation présente des opportunités pour demander plus de sécurité et étendre son contrôle.

> *Moi, j'en ai profité pour sécuriser un peu mieux, un peu plus structurellement l'entreprise. Ces deux objectifs sont congruents. (un directeur du département de sécurité)*

Mais les départements IT sont vigilants et dénoncent les tentatives de propagation des contrôles de sécurité au delà de l'étendue initiale du projet PCI.

> *[…] j'ai eu comme ça quelques conflits avec la sécurité ; « désolé je ne prends pas ça dans mon programme parce que c'est pour moi, pas lié à PCI ». (un chef de projet)*

La négociation inclut aussi les relations avec l'auditeur externe que les acteurs tentent de contrôler. Le chef de projet note dans son rapport de clôture que « *même si tout est en ordre, il y a toujours des zones grises sur lesquelles l'auditeur peut discuter* » et il note un peu plus

loin que « *certaines entreprises gardent toujours une partie pas tout à fait conforme, mais solutionnable. De cette manière l'auditeur passe son temps sur cet éventuel problème et n'a pas le temps de regarder les autres problèmes* »..

Si la sécurité négociée est caractérisée par un processus d'échanges et d'innovation, elle est surtout l'espace que les acteurs se donnent et dans lequel ils mettent en place des dispositifs de contrôle pour les uns et des dispositifs d'autonomie pour les autres.

6.4 La sécurité contrôlée

La certification est octroyée pour une période d'un an et elle doit être renouvelée tous les 12 mois. Notons que le renouvellement de la certification est aussi l'expiration de la certification en cours. Le mouvement de négociation s'amplifie à l'approche du renouvellement de la certification et il se fige dès que celle-ci est obtenue. Les actions en vue du renouvellement commencent systématiquement dans l'urgence, quelques semaines seulement avant l'échéance. Une situation tendue que les départements IT tentent d'utiliser pour demander plus de ressources humaines et matérielles. Le chef de projet raconte comment il formule cette demande à la direction.

> *[J'allais voir la direction pour] leur demander « bon voilà j'ai besoin de cette organisation-là si vous voulez ce scope-là ». (un chef de projet)*

Mais la direction et le département de sécurité ont leur réponse.

> *On n'a pas mis en place des processus de contrôle, on a mis en place des processus qui sont des passages obligatoires sinon ça ne se fait pas, c'est différent d'un contrôle. (un directeur du département de sécurité)*

Cet espace de négociation est pour nous celui d'une régulation conjointe. Elle apparaît plus ouverte dans les circonstances du renouvellement et de nouvelles formes de contrôle peuvent y prendre place. Nous en avons identifié deux : la pénurie de ressources et l'externalisation du contrôle d'audit. Par contre, nous n'avons pas identifié de nouvelles formes d'autonomie pour les départements IT, tout au plus leurs autonomies existantes ne sont pas frontalement remises en question et ils peuvent jouer avec le sentiment d'urgence créé à l'approche du renouvellement pour tenter de peser sur les négociations, notamment en ce qui concerne les ressources et les moyens financiers.

6.4.1 La pénurie des ressources

Pour les membres des départements IT, les nouvelles règles introduites par la norme PCI ne sont pas accompagnées de l'augmentation des ressources humaines nécessaires, voire

indispensables, pourtant l'entreprise n'est pas en difficulté. Cette situation crée chez les ingénieurs IT un sentiment de démotivation et une perception accrue des risques d'incidents et surtout du risque de ne pas atteindre le niveau d'exigence requis pour garder la certification. Le manager d'un des départements IT exprime bien la situation :

> *Pour moi, c'est que c'est extrêmement difficile de motiver les gens sur des projets pareils. Tout le monde considère ça comme une corvée et donc dans le cadre d'un projet considéré comme une corvée, toi, tu dois essayer malgré tout d'obtenir des résultats pour passer l'audit. Donc, ça veut dire que cette période d'audit est toujours une période de stress épouvantable … chaque fois convaincu que tu vas te planter et que chaque fois tu as vraiment l'impression que c'est un miracle que tu as réussi quand l'auditeur est parti et qu'il n'a rien sorti. Parce qu'effectivement c'est toujours au strict minimum et c'est aussi uniquement dans le but d'avoir le papier pour le moins d'argent possible. Mais on ne s'améliore pas. (un manager des départements IT)*

Le manque systématique de ressources est donc très contraignant pour les ingénieurs. Leur marge de manœuvre est faible et ils sont obligés de faire avec les ressources dont ils disposent, de faire les choix qui réduisent leur perception des risques et garantissent au mieux la certification et son renouvellement.

> *Disons que tu as quand même le document qui décrit ce qu'il faut faire pour être PCI compliant, donc les résultats à atteindre qui sont quand même déjà très contraignants en eux-mêmes parce que, je vais dire, il y a certains endroits [où] ils ne te laissent même pas le choix dans la manière où il faut implémenter. C'est très directif. Et puis, bon, c'est clair qu'au dessus de ça il y a [la sécurité] qui parfois en rajoute encore une couche en manière de directivité. (un manager des départements IT)*

Aucun des acteurs n'a indiqué que le manque de ressources est lié à une situation économique difficile pour l'entreprise. La cause serait donc, selon eux, d'origine interne, c'est-à-dire liée à des décisions de gestion. La pénurie de ressources oblige à rendre des comptes, à justifier l'usage des budgets, à quémander des moyens supplémentaires pour terminer les projets. Elle a pour conséquence qu'on ne peut plus faire « comme avant » : maintenant les ingénieurs doivent faire plus avec des ressources identiques voire moindres, dans un contexte local où il devient de plus en plus compliqué de compresser les tâches. Faire plus devient donc faire

autre chose, c'est-à-dire se focaliser sur la sécurité pour la certification. Celle-ci s'impose donc au détriment de la sécurité « de métier ».

6.4.2 L'audit externe comme externalisation du contrôle

Du point de vue de la gouvernance de l'entreprise, la normalisation participe à l'exercice du pouvoir c'est-à-dire au « système de relations qui s'entrelacent dans le fonctionnement des institutions et établissent le rôle des acteurs » (Gomez, 1996). À ce titre, elle met en place un système externe de sanctions matérialisé par un organisme d'audit externe qui est « chargé de sanctionner l'exactitude des engagements » (Gomez, 1996). Pour l'ensemble des acteurs, dès lors qu'un d'un processus de certification est engagé, il faut tenir compte des enjeux et des exigences d'un organisme tiers à qui on demande d'attester de la conformité des règles à la norme (Grenard, 1996). Les acteurs perçoivent bien ce rôle dans l'organisation et se montrent très critiques.

> *[…] L'audit [externe] n'acceptait pas, parce qu'ils n'étaient pas au même niveau et l'audit avait une dent contre [eux]. Et donc, ce n'était pas sain. Quand un auditeur est en même temps partie prenante […], il n'y a pas fiabilité de l'auditeur externe. (un responsable des départements IT)*

Par ailleurs, le système interne de sanctions est faible et peu coercitif. Les acteurs des départements IT et du département de sécurité, ne perçoivent pas une augmentation ni du contrôle interne ni de la surveillance. Certains d'entre eux le regrettent et sont même en attente de plus « d'autorité interne ».

> *Pour moi il n'y a pas plus de contrôles pour PCI. On ne va faire que 60% des contrôles, et pourtant on refait l'examen. (un responsable des départements IT).*
>
> *Je dirais que c'est à peu près au même niveau [de contrôle] (un directeur du département de sécurité)*
>
> *À mon avis, le seul moyen c'est avoir une autorité au dessus, suffisamment forte que pour imposer les choses. Donc et avoir des mesures, d'avoir le risque de mesures de rétorsion. Faut avoir un département de sécurité qui ait des pouvoirs liés la sécurité évidemment, mais qui sont très forts. (un manager des départements IT)*

L'auditeur externe chargé de vérifier la conformité des pratiques de sécurité dans les départements IT est l'élément central du deuxième dispositif de contrôle. Ils lui reconnaissent peu de légitimité : ils doutent de ses compétences pour juger leurs pratiques de sécurité et ils

se méfient de son impartialité car c'est un tiers, externe à l'entreprise, choisi et rémunéré par la direction et le département de sécurité. Cette nouvelle situation change la règle du jeu qui voulait que les experts soient les principaux acteurs qui décident des options technologiques et sécuritaires.

7 Conclusion

Dans notre question de recherche (« Quels sont les modes de contrôles et comment structurent-ils la manière dont les acteurs construisent et transforment les règles de sécurité des systèmes d'information ? »), nous avons questionné la transformation des règles du jeu dans le cadre d'un processus de normalisation et de la certification qui l'accompagne. Les observations, l'analyse des documents et les interviews nous ont permis d'identifier les quatre modes de contrôle, ou quatre temps de la sécurité, passant d'une sécurité autonome à une sécurité contrôlée.

Utilisant le vocabulaire inspiré de la Théorie de la Régulation Sociale, le projet de normalisation est le déclencheur d'une régulation de contrôle de la part la direction et pilotée par le département de sécurité. En réponse, les ingénieurs des départements IT défendent leur indépendance d'experts tout en reconnaissant que la normalisation est indispensable pour avoir le certificat qui permet à l'entreprise de poursuivre ses activités. Les acteurs font émerger ensemble des concepts sociotechniques qui leur permettent de stabiliser leur situation et de nouvelles règles peuvent être construites en y faisant référence. La zone PCI nous en a fourni un exemple. Quant au dispositif de contrôle, il est peu, voire pas du tout coercitif. Cependant, le poids de l'obligation est bien présent. La sécurité contrôlée est marquée par de nouvelles contraintes de contrôle et de surveillance : celle d'obtenir des résultats avec des ressources réduites et celle de se soumettre à l'examen de l'auditeur externe. Pour le département de sécurité, le projet PCI n'a pas pour seul but d'obtenir la certification, mais présente la possibilité de (re)prendre le contrôle de la sécurité laissée précédemment aux ingénieurs. . Dans le tableau ci-dessous, nous mettons en regard les informations collectées à travers les interviews, les observations et les données secondaires avec les quatre modes de sécurité identifiés dans notre analyse.

Tableau 1

Informations collectées sur le terrain	Analyse
(1) La sécurité de terrain est majoritairement réalisée par des actions techniques. Les départements IT disposent de l'autonomie de décision et des ressources nécessaires à la mise en œuvre. Le département de sécurité a principalement un rôle de conseiller, les règles prescrites (*Security Policies*) sont faiblement ancrées dans les pratiques des ingénieurs IT.	1. Les acteurs disposent des marges de manœuvre qui leur permettent d'être autonomes dans leur zone de responsabilité. Sécurité autonome correspond à une situation équilibrée entre les actions des départements IT et le département de sécurité. C'est la sécurité des experts, des métiers.
(2) L'entreprise doit être certifiée pour continuer ses activités. La direction et le département de sécurité se font le relai de cette obligation vers toute l'entreprise et particulièrement vers les départements IT.	2. La sécurité obligatoire correspond à une régulation de contrôle initiée par la direction et pilotée par le département de sécurité. La sécurité des experts est remise en question.
(3) Les technologies de sécurité des départements IT ne sont plus le principal centre de la sécurité, des controverses naissent et des nouvelles solutions sont trouvées. Les utilisateurs deviennent des parties prenantes dont il faut de plus en plus tenir compte. Les acteurs sont sous les contraintes d'obtenir la certification et de garantir la sécurité effective.	3. La sécurité négociée correspond à une régulation conjointe où les acteurs sont à la recherche d'un nouvel équilibre : ils doivent créer et intégrer de nouvelles règles de sécurité. L'engagement des acteurs dans la recherche de solutions communes, de nouvelles règles du jeu, est qualifié de fort.
(4) La certification doit être maintenue d'année en année, elle n'est jamais définitivement acquise et les solutions peuvent être remises en cause par l'auditeur externe. Les départements IT perçoivent une diminution de leurs possibilités d'actions. La situation est peu coercitive mais le manque de ressources financières et humaines, et les contrôles sur leurs utilisations sont qualifiés de forts à très forts.	4. La sécurité contrôlée est l'installation durable de dispositifs de contrôle : contrôle sur les ressources et contrôle par l'auditeur externe. Les nouvelles règles du jeu sont intégrées par l'ensemble des acteurs.

Les règles du jeu ne sont pas données, elles sont négociées, et les acteurs ne sont pas sans moyens pour faire pression (Reynaud, 1993). Notre étude montre que les règles de sécurité formalisées et normées sont présentées comme indispensables à la certification, car elles garantissent la solidité et la prévisibilité des systèmes (Wildavsky, 1988), qu'elles sont au centre de négociations et de controverses, et qu'elles sont traversées par de fortes tensions.

Finalement, notre analyse pose une nouvelle question : l'évolution des règles de sécurité d'une sécurité autonome vers une sécurité contrôlée mène-t-elle à une meilleure sécurité des systèmes d'information ou s'accompagne-t-elle d'une augmentation des risques étant donné les stratégies adoptées par les acteurs ?

8 Références

Alcaraz, C., Roman, R., Najera, P., & Lopez, J. (2013). Security of industrial sensor network-based remote substations in the context of the Internet of Things. Ad Hoc Networks, 11(3), 1091-1104.

Allison, S. F. H., Schuck, A. M., & Lersch, K. M. (2005). Exploring the crime of identity theft: Prevalence, clearance rates, and victim/offender characteristics. Journal of Criminal Justice, 33(1), 19-29.

Baskerville, R. (1993). Information systems security design methods: implications for information systems development. ACM Comput. Surv., 25(4), 375–414.

Beck, U. (2008). La société du risque: sur la voie d'une autre modernité. Flammarion.

Bonner, E., ORaw, J., & Curran, K. (2011). Implementing the Payment Card Industry (PCI) Data Security Standard (DSS). Journal of Electrical Engineering, 9(2), 365-376.

Callon, M., Lascoumes, P., & Barthe, Y. (2001). Agir dans un monde incertain: essai sur la démocratie technique. Paris: Éditions du Seuil.

Creswell, J. W., & Miller, D. L. (2000). Determining Validity in Qualitative Inquiry. Theory Into Practice, 39(3), 124.

Cusin, J. (2008). Survie en milieu hostile: l'étude qualitative de sujets sensibles en management. XVIIème Conférence Internationale de Management Stratégique.

Cusin, J. (2009). L'élaboration d'un design de recherche. Revue internationale de Psychosociologie, XV(1), 117.

De Terssac, G. (2013). De la sécurité affichée à la sécurité effective: l'invention de règles d'usage. Gérer et comprendre, (1), 25–35.

De Terssac, G., & Mignard, J. (2011). Les paradoxes de la sécurité: le cas d'AZF. Paris: Presses universitaires de France.

Ernst & Young. (2009). European fraud survey 2009: Is integrity a casualty of the downturn?

- Ernst & Young - United Kingdom.

Gilbert, C. (1998). Des objets à géométrie très variable. Entretien avec Claude Gilbert. Politix, 11(44), 29-38.

Gomez, P.-Y. (1996). Normalisation et gestion de la firme : une approche conventionnaliste. Revue d'économie industrielle, 75(1), 113-131.

Grenard, A. (1996). Normalisation, certification : quelques éléments de définition. Revue d'économie industrielle, 75(1), 45-60.

Laroche, H., & Steyer, V. (2012). L'apport des théories du sensemaking à la compréhension des risques et des crises. Les cahiers de la sécurité industrielle, 44.

Lincoln, Y. S., & Guba, E. G. (1985). Naturalistic inquiry. SAGE.

Merriam, S. B. (2002). Qualitative research in practice: examples for discussion and analysis. Jossey-Bass.

Miles, M. B., & Huberman, A. M. (1999). Qualitative data analysis. SAGE.

Miller, B., & Rowe, D. (2012). A Survey SCADA of and Critical Infrastructure Incidents. In Proceedings of the 1st Annual Conference on Research in Information Technology (p. 51–56). New York, NY, USA: ACM.

Mintzberg. (1998). Structure et dynamique des organisations. Éditions d'Organisation.

Mintzberg, H. (2003). Le pouvoir dans les organisations (Nouvelle.). Éditions d'Organisation.

Nizet, J., & Huybrechts, C. (1998). Interventions systémiques dans les organisations: Intégration des apports de Mintzberg et de Palo Alto. De Boeck Supérieur.

Paget, F. (2007). Identity theft. McAfee Avert Labs technical white paper, 1. Consulté à l'adresse http://www.pubblicaamministrazione.net/file/whitepaper/000042.pdf le 14/01/2014

PCI Security Standards Council. (2010, octobre). PCI-DSS version 2.0 - Requirements and Security Assessment Procedures Document. Consulté à l'adresse https://www.pcisecuritystandards.org/security_standards/documents.php?document=pci_dss_v2-0#pci_dss_v2-0 le 14/01/2014

Philippsohn, S., & Thomas, S. (2003). E-Fraud — What Companies Face Today. Computer Fraud & Security, 2003(1), 7-9.

Pichault, F., & Nizet, J. (2000). Les pratiques de gestion des ressources humaines: approches contingente et politique. Seuil.

Portal, T. (2009). Crises et facteur humain: Les nouvelles frontières mentales des crises. Groupe de Boeck.

Quivy, R., & Van Campenhoudt, L. (2006). Manuel de recherche en sciences sociales, PAris : Dunod.

Rasmussen, J. (1997). Risk management in a dynamic society: a modelling problem. Safety Science, 27(2-3), 183-213.

Reynaud, J.-D. (1988). Les régulations dans les organisations: Régulation de contrôle et régulation autonome. Revue française de sociologie, 29(1), 5-18.

Reynaud, J.-D. (1991). Pour une sociologie de la régulation sociale. Sociologie et sociétés, 23(2), 13-26.

Reynaud, J.-D. (1993). Les règles du jeu: l'action collective et la régulation sociale. A. Colin.

Rowlingson, R., & Winsborrow, R. (2006). A comparison of the Payment Card Industry data security standard with ISO17799. Computer Fraud & Security, 2006(3), 16-19.

Summers, B. J. (2009). Fraud Containment. SSRN eLibrary. Consulté à l'adresse http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1341158 le 14/01/2014

Thietart, R.-A. (2007). Méthodes de recherche en management (3ème édition.). Paris: Dunod.

Wildavsky, A. B. (1988). Searching for Safety. Transaction Publishers.

Yin, R. K. (2009). Case study research: design and methods. Sage Publications.