LE RÔLE DES RELATIONS DE POUVOIR DANS L'ÉLABORATION DES POLITIQUES DE SÉCURITÉ DES SYSTÈMES D'INFORMATION

Annick CASTIAUX
Université de Namur, Belgique
Annick.castiaux@unamur.be

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

RESUME

Les règles de sécurité des systèmes d'information reposent en partie sur un processus de négociation et d'appropriation lors duquel les acteurs vont interpréter les normes de sécurité et remettre en question leurs modèles d'actions, tant dans leurs aspects techniques que dans les modalités organisationnelles. Dans cet article, nous questionnons le rôle des relations de pouvoir dans ce processus.

Notre démarche explore deux études de cas aux relations de pouvoir contrastées qui se jouent entre les managers de la ligne hiérarchique et les ingénieurs du département informatique. Toutes deux sont situées dans des organisations qui sont amenées à élaborer des règles de sécurité informatiques conformes à une norme externe qui leur est imposée.

Les résultats de notre analyse tentent à soutenir les conclusions de Nizet et Pichault (2011) selon qui la nature des règles produites à l'issue d'un travail de négociation et d'interprétation plus ou moins intense d'une norme externe est étroitement liée aux relations de pouvoir à l'œuvre dans ces situations.

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

LE RÔLE DES RELATIONS DE POUVOIR DANS L'ÉLABORATION DES POLITIQUES DE SÉCURITÉ DES SYSTÈMES D'INFORMATION

INTRODUCTION

La pensée organisationnelle moderniste voit dans les organisations des entités objectives dont les actions et les décisions sont dirigées par des normes de rationalité, d'efficience et d'efficacité (Hatch & Cunliffe, 2009). La plupart des modèles de gestion des systèmes d'information sont dans la droite ligne de cette vision du monde : ils cherchent à établir des méthodes et des techniques pour organiser et contrôler la gestion en structures rationnelles. Le modèle COBIT, « *Control Objectives for Information and Related Technology* » (ISACA, 2015; Wikipedia, 2015), est certainement l'exemple le plus emblématique de cette pensée techniciste. La présentation rationnelle de ce modèle, ou des modèles proches, a séduit depuis plus d'une décennie les managers responsables de la gestion des systèmes d'information. La sécurité de ces systèmes, c'est-à-dire la protection du capital informationnel de l'organisation, est une des responsabilités majeures de ces managers, en particulier lorsqu'il s'agit d'informations sensibles, comme les informations financières (Hardy, 2006; IT Governance Institute, 2006; Simonsson, Johnson, & Wijkström, 2007; Tuttle & Vandervelde, 2007). En sécurité des systèmes d'information, les principales normes sont ISO27001[1] et PCI-DSS[2]. La première est généraliste : elle apporte un cadre aux situations les plus courantes dans différents secteurs d'activité. La seconde est spécifique au secteur bancaire : elle vise à la protection des données de comptes bancaires.

[1] Le texte de la norme ISO/IEC 27001 est soumis à licence d'utilisation, il est disponible sur le site de l'International Organization for Standardization (http://www.iso.org/iso/iso27001, consulté le 09/07/2016).

[2] Le texte de la norme PCI-DSS est libre d'accès. Il est accessible au format PDF sur le site du PCI Security Standards Council (https://fr.pcisecuritystandards.org/minisite/en/pci-dss-v3-0.php, consulté le 09/07/2016).

Ces normes sont des modèles normatifs externes à l'organisation, présentés comme des ensembles cohérents et exhaustifs d'exigences, de spécifications et de bonnes pratiques qu'il faut idéalement suivre en adoptant des règles internes conformes. Leur respect strict est présenté comme la condition nécessaire et suffisante qui assure aux organisations une gestion performante de leurs systèmes d'information. L'exigence de leur respect amène à recourir périodiquement à des auditeurs externes qui vérifient que les règles en vigueur dans l'organisation respectent bien la norme et ils délivrent, le cas échéant, un certificat attestant de cette conformité.

Sans remettre en question ces modèles eux-mêmes, nous constatons qu'ils dominent le champ du management des systèmes d'information et s'y imposent comme des références évidentes, sans que soit questionnée leur interaction avec les relations de pouvoir dans ces organisations. Le respect de la norme, avec ou sans audit de certification, devient un enjeu et donne lieu à un processus de changement qui passe par l'élaboration de nouvelles règles ou par l'adaptation de celles qui sont déjà en place.

Cependant, bien que les règles de sécurité aient été pensées et mises en place rationnellement selon les normes, les modèles de gestion des systèmes d'information considèrent qu'il reste toujours une possibilité qu'un incident se produise. Ce que l'actualité des incidents de sécurité informatique nous confirme régulièrement. Selon Perrow (1984), le risque zéro n'existe pas, car on parle de systèmes sociotechniques complexes soumis au phénomène de « l'accident normal ». Le respect strict des normes et des règles de sécurité présente donc des espaces d'incertitudes dans lesquels les incidents de sécurité peuvent malgré tout se produire. Pour de Terssac et Mignard (2011) qui ont développé ce paradoxe, la sécurité contient des contradictions qui tiennent d'une part à la cohabitation des mesures de sécurité et des efforts pour combattre les risques, et d'autre part aux limitations des décisions pour rendre celles-ci rationnelles.

D'autres recherches dans ce domaine ont montré l'existence d'alternatives au courant de pensée dominant. Elles contredisent les finalités d'efficience et d'efficacité rationnelles des normes et réintègrent la multiplicité de sens que peuvent leur associer les différents acteurs (managers, ingénieurs, utilisateurs, etc.) et leur caractère structurant (Orlikowski, 2000; Orlikowski & Robey, 1991). Elles montrent que la sécurité n'est pas déconnectée des enjeux des acteurs et que les règles de sécurité ne sont pas figées, qu'elles ne sont pas écrites une fois pour tout.

Concernant cette évolution dynamique des règles, la littérature de la contingence stratégique, notamment à travers les travaux de Crozier et Friedberg (1977) et de Pfeffer (1981), a montré que les acteurs sont capables d'agir pour changer les règles et qu'ils le font en mobilisant des ressources qu'ils utilisent comme leviers de pouvoir. Qui plus est, selon ces travaux, les acteurs sont dans une démarche politique, ils développent et utilisent des sources de pouvoir pour obtenir les résultats qu'ils privilégient pour défendre leurs intérêts.

Notre objectif est de comprendre ce que sont les règles de sécurité des systèmes d'information, qui sont le résultat (jamais définitif) de négociations et de stratégies d'acteurs, en explorant l'articulation entre les relations de pouvoir existantes entre les managers de la ligne hiérarchique et les ingénieurs informaticiens, et le travail d'interprétation d'une norme de sécurité. Pour ce faire, notre article propose d'explorer la dynamique sociale des acteurs engagés dans l'élaboration de règles de sécurité à partir de deux études de cas issues de nos recherches en gestion de la sécurité des systèmes d'information.

Dans un premier temps, prenant appui sur la Théorie de la régulation sociale de Jean-Daniel Reynaud (1997, 1999), nous présentons les concepts spécifiques utilisés dans ce champ du management des systèmes d'information. Nous complétons le cadre théorique en y introduisant le rôle des relations de pouvoir. Ensuite nous présentons plus en détail les deux études de cas issues de départements informatiques confrontés à la mise en œuvre d'une sécurité de leurs systèmes d'information. L'une provient du domaine bancaire, l'autre, de celui de l'énergie. Avant de conclure, nous développons et discutons l'interaction entre les règles de sécurité produites et les relations de pouvoir à l'œuvre, en mettant en évidence plus particulièrement l'impact de cette interaction sur le caractère plus ou moins structurant de ces règles.

1 LA SECURITE INFORMATIQUE A LA LUMIERE DE LA THEORIE DE LA REGULATION SOCIALE

La Théorie de la Régulation Sociale (TRS) constitue un cadre pertinent pour étudier les mécanismes d'élaboration des règles collectives et leurs dynamiques dans les organisations (Reynaud, 1997; Reynaud & Richebé, 2007). C'est moins la règle que ses mécanismes d'élaboration et les interactions entre les individus qui sont au centre de la TRS. La règle est ici un construit social, le résultat d'un processus d'échange et de négociation dans une situation et un contexte donnés. Notre choix pour ce cadre théorique dans le domaine de la sécurité des

systèmes d'information est conforté par les travaux qui ont été réalisés dans les milieux industriels où les règles de sûreté[3] occupent une place importante dans la protection des personnes et des installations (de Terssac, 2013; de Terssac & Mignard, 2011). En informatique comme dans l'industrie chimique, les règles de sécurité sont faites de compromis, de négociations et d'accords en transformation permanente et jamais définitifs dans lesquels « les acteurs construisent un système d'échange et de coopération pour la production des règles » (de Terssac, 2012). La mobilisation de la TRS nous permet en outre de préciser ci-dessous les concepts que nous mobilisons pour cette étude.

1.1 LA RÈGLE

Jean-Daniel Reynaud précise sa définition de la règle : « la règle est un principe organisateur. Elle peut prendre la forme d'une injonction ou d'une interdiction visant à déterminer strictement un comportement. Mais elle est plus souvent un guide d'action, un étalon qui permet de porter un jugement, un modèle qui oriente l'action. Elle introduit dans l'univers symbolique des significations, des partitions, des liaisons » (Reynaud, 1997, p. xvi). La règle est le résultat d'un processus de construction sociale dans lequel elle est créée et vécue à travers les actions, fait l'objet de changements et disparaît. Elle est intimement liée aux activités des acteurs sociaux qui lui reconnaissent légitimité et efficacité (Reynaud, 1997, p. 42- 43).

1.2 LA SÉCURITÉ

Le concept de sécurité recouvre plusieurs sens. La sécurité peut faire référence à un sentiment de « tranquillité qui résulte de l'absence de danger » ou à « l'organisation des mesures destinées à assurer la sûreté » (Villers, 2009). Au niveau sociétal, selon Beck (2008), la sécurité est constitutive de la société du risque. Il entend par société du risque une société post-industrielle entrée dans un modernisme caractérisé par « les progrès technologiques effectués dans la rationalisation et les transformations du travail et de l'organisation » (Beck, 2008, p. 35). Pour cet auteur, la société produit des richesses, mais aussi des risques qu'elle distribue de manière

[3] Le concept de sûreté, c'est-à-dire la qualité d'une chose dont l'utilisation n'est pas susceptible de causer des blessures, est utilisé ici pour distinguer la protection des objets du monde physique de la sécurité, c'est-à-dire le fait de ceux-ci ne soient pas menacés par un quelconque danger.

inégale. La sécurité consiste alors à se prémunir et à gérer les conséquences des impacts produits par la société, ce qu'il appelle les effets induits des risques. Il souligne que la mise en place d'une sécurité dans la société implique une « réorganisation du pouvoir et des attributions » (Beck, 2008, p. 43). En effet, à mesure que les dangers augmentent, la prévention consiste à doter le moindre aspect de l'action de « contrôles et de planifications bureaucratiques », produisant ainsi une transformation, au moins partielle, du système. Cette transformation « jette les bases d'un autoritarisme scientifico-bureaucratique », légitime de la prévention. Par exemple, à la suite d'un incident de sécurité lors duquel une intrusion s'est produite dans les systèmes d'information, de nouvelles règles ont renforcé la standardisation, les contrôles et les surveillances : « *We recommend that the Company creates a patching procedure as well as standardized production systems to the same version of operating system and to the same set of application software installed*[4] » (extrait d'un rapport d'incident). Si ces situations présentent un vrai défi pour la démocratie (Beck, 2008, p. 139‑145), ce sont surtout les rapports de pouvoir et les négociations de règles dans lesquelles les acteurs sont impliqués en vue d'assurer leur protection qui sont ici questionnés. La sécurité consiste alors à poser des règles pour « garantir la continuité du fonctionnement productif d'un système sociotechnique » (de Terssac, 2013), ce qui se traduit sur le terrain par la mise en place de règles qui protègent des risques que représentent les vulnérabilités du système sociotechnique. À chaque nouvelle vulnérabilité, de nouvelles règles de contrôle tentent de rationaliser une situation qui semblait y avoir échappé. Par exemple, suite à l'internationalisation de nouvelles formes de fraudes aux cartes bancaires, les institutions bancaires ont ajouté des règles de sécurité qui n'existaient pas précédemment, elles sont relatives à la zone géographique dans laquelle la demande de retrait de billet est faite. « *Pour des raisons de sécurité, la Banque peut instaurer dans certains pays non européens des restrictions relatives aux modalités d'utilisation de la carte de banque. Cela peut avoir pour conséquence que, dans ces pays, le titulaire ne pourra pas effectuer de retraits d'argent ni d'opérations de paiement avec sa carte* » (« BNP Parisbas Fortis: Conditions générales relatives aux cartes de banque et aux services phone banking et pc banking », 2016).

[4] *"Nous recommandons que l'entreprise crée une procédure de "patching" ainsi que des systèmes de production standardisés sous la même version que le système d'exploitation et en installant le même ensemble de logiciels d'application."* (Traduction des auteurs)

1.3 LA RÈGLE DE SÉCURITÉ DES SYSTÈMES D'INFORMATION

Repartons de la définition de Reynaud (1997) ci-dessus et tentons de l'étendre à la sécurité des systèmes d'information. La règle de sécurité est un principe organisateur des activités qui visent à garantir la continuité du fonctionnement productif des systèmes d'information. Les acteurs font référence à la règle pour organiser les activités de protection. Les règles peuvent être préventives, c'est-à-dire qu'elles permettent aux acteurs d'anticiper la survenance des risques : utiliser un mot de passe complexe, le changer tous les 60 jours, etc. Mais elles sont le plus souvent réactives, en réponse à un risque qui s'est produit : bloquer l'accès en cas d'utilisation frauduleuse. Elle est un guide d'action pour les acteurs, un modèle qui oriente leurs décisions face aux situations rencontrées. Par exemple, la règle indique dans quelles circonstances et selon quelle procédure un utilisateur introduit une demande de remplacement de son mot de passe. Les règles de sécurité sont des principes opératifs permettant d'atteindre un objectif de sécurité, c'est-à-dire qu'elles sont conçues pour permettre d'éviter la production d'un accident (Hale, Heijer, & Koornneef, 2003; Leplat, 1998).

Comme les autres règles, celles de la sécurité permettent aux acteurs d'agir collectivement, elles sont des éléments indispensables à l'ajustement et à la coordination de leurs actions collectives. Les acteurs ne sont pas passifs, ils ne font pas que subir les règles ; ils sont en mesure de mobiliser les ressources pour les influencer : « ils les contestent lors de conflits, ils les élaborent lors de négociations », « ils s'efforcent de les rendre cohérentes ou du moins de limiter les effets destructeurs de leur incohérence » (Reynaud, 1999). Nous sommes bien dans une dynamique des règles et non dans une situation figée où les règles sont données une fois pour toutes. Cette dynamique est le résultat de l'activité de régulation que nous pouvons observer à travers les jeux des acteurs. C'est une activité de construction des règles de sécurité qui donne aux acteurs la possibilité de construire de nouvelles relations de coordination de leurs actions et de les changer selon leurs enjeux et leurs objectifs.

1.4 LA POLITIQUE DE SÉCURITÉ

En matière de sécurité des systèmes d'information, la littérature tant académique que professionnelle utilise largement le concept de politique de sécurité, *Security Policy*, pour désigner un ensemble de règles de sécurité regroupées sous un thème commun (Wood, 1995).

Les politiques de sécurité sont des règles affichées (de Terssac, 2013). Elles sont rassemblées dans un document structuré qui définit son champ d'action et forme ainsi un cadre normatif auquel les acteurs peuvent faire référence. Cette structure documentaire n'est pas seulement une liste de règles, elle en précise le contexte et son champ d'application et, de cette manière, constitue un « guide » pour les acteurs. Une politique de sécurité renseigne sur 1/ le but ou la raison d'être des règles, 2/ leurs objectifs poursuivis, 3/ l'applicabilité des règles, c'est-à-dire le contexte organisationnel et technique dans lequel elles sont considérées comme étant applicables, 4/ la distribution, c'est-à-dire quels sont les acteurs concernés, 5/ l'exécution, ou la condition de réalisation, et 6/ le suivi (Meynen, 2009). Ce dernier point fait référence aux moyens de contrôle de la mise en application et du respect des règles, ainsi que les sanctions prévues en cas de non-respect.

1.5 LA NORME DE TYPE ISO ET LA SÉCURITÉ DES SYSTÈMES D'INFORMATION

L'International Organization for Standardization (ISO) donne la définition suivante d'une norme : « document, établi par consensus et approuvé par un organisme reconnu, qui fournit, pour des usages communs et répétés, des règles, des lignes directrices ou des caractéristiques, pour des activités ou leurs résultats, garantissant un niveau d'ordre optimal dans un contexte donné » (International Organization for Standardization, 2016). D'une manière générale, une norme de type ISO est « un document qui fournit des exigences, spécifications, lignes directrices ou des caractéristiques qui peuvent être utilisées régulièrement pour assurer que les matériaux, produits, processus et services sont aptes à leur emploi » (« International Organization for Standardization », s. d.). Elles constituent un modèle à suivre lors de la mise en place et l'exploitation d'un système de gestion. Ce modèle intègre les éléments sur lesquels les experts dans le domaine ont atteint un consensus comme étant l'état de l'art international. En matière de sécurité des systèmes d'information, les normes auxquelles il est fait référence sont issues de la famille ISO 27000. Elles couvrent de nombreux aspects, les plus connues étant ISO 27001 – Information Security Management System (ISO/IEC 27001, 2013) et ISO 27002 – Code of Practice for Information Security Controls (ISO/IEC 27002, 2013). Elles sont aussi à la base d'autres normes spécifiques à certains domaines d'application et qui n'ont pas nécessairement le « label ISO ». C'est le cas de la norme PCI-DSS (Payment Card Industry-Data Security Standard) qui est utilisée comme référentiel normatif pour la sécurité des

informations de paiements électroniques par cartes de crédit afin de protéger les données de comptes bancaires.

2 RELATIONS DE POUVOIR : INTERPRETATION DE LA NORME ET NEGOCIATION DES REGLES

Dans une intéressante et très complète analyse, de Terssac et Mignard (2011) retracent la mise en place de règles de sécurité dans une usine chimique. Ils nous montrent notamment que la mise en œuvre de la sécurité se fait au terme d'un « travail de négociation et d'appropriation » dans lequel les relations de pouvoir entre les acteurs « d'en haut » et « d'en bas », c'est-à-dire entre les ingénieurs de la ligne hiérarchique et les ouvriers sur le terrain, ont toute leur importance dans l'élaboration et l'application des règles de sécurité. Pour ces auteurs, la négociation « désigne l'effort et les concessions que les protagonistes font pour élaborer des règles et les rendre communes » (de Terssac & Mignard, 2011, p. 244), le compromis qui en résulte est « tiré » par la position dominante d'une des parties engagées dans ces jeux d'acteurs (Reynaud, 1999, p. 15,20). Quant au travail d'appropriation, bien qu'il puisse prendre différentes formes et les combiner, c'est surtout par l'usage, c'est-à-dire par la mise en action des règles, que les individus les alimentent en significations et se les approprient (Terssac, Boissière, & Gaillard, 2009).

Pour Nizet et Pichault (2011; 2012), les règles sont en relation étroite avec, d'une part, les relations de pouvoir et, d'autre part, le travail interprétatif des acteurs en situation d'action. D'abord, les relations de pouvoir peuvent être plus ou moins symétriques entre les structures d'encadrement et les équipes dédiées à l'exécution des tâches. Empruntée au langage de la TRS, la présence de régulations de contrôle dominantes est l'expression d'une relation de pouvoir asymétrique, tandis que les régulations autonomes dominantes seront l'indication que la relation de pouvoir est symétrique, plus équilibrée. Ensuite, ces relations interviennent dans le caractère plus ou moins structurant des règles et dans l'intensité du travail interprétatif. Des relations de pouvoir symétriques favorisent un travail interprétatif fort, alors que des relations plus asymétriques les défavorisent. Le caractère plus ou moins intense de ce travail interprétatif est à la base du processus de construction collective de règles auxquelles les acteurs donnent sens (Weick, Sutcliffe, & Obstfeld, 2005; Weick & Vidaillet, 2003). La construction de ces règles de sécurité n'est pas le résultat d'une rationalité unique et optimale, mais celui d'un

processus social, d'une régulation sociale, dans lequel les acteurs négocient et interprètent les règles pour les faire évoluer tout en « collant » au mieux avec la norme. Elle constitue ainsi une base commune de règles tacites ou écrites auxquelles les acteurs peuvent faire référence.

C'est dans cette articulation et à travers les deux études de cas ci-dessous que nous proposons d'explorer les relations de pouvoir et le travail interprétatif des acteurs pour construire des règles de sécurité et ainsi mettre en œuvre une politique de sécurité, tout en faisant référence aux spécifications d'une norme externe de type ISO. Nous n'abordons pas le contenu de la norme ni les enjeux du choix et de la préférence d'une norme à une autre, cela dépasserait les limites que nous nous sommes données pour cet article.

Notre grille d'analyse va d'abord porter sur les relations de pouvoir ; ainsi, la présence dominante de régulations de contrôle indiquera des relations de pouvoir plutôt asymétriques tandis que des régulations autonomes plus présentes indiqueront que les relations de pouvoir sont plutôt symétriques. Ensuite, suivant Nizet et Pichault (2011), nous observerons chez les acteurs, l'intensité du travail interprétatif des normes de sécurité en vigueur dans leur domaine d'activité respectif pour finalement nous intéresser aux règles qui sont produites et qui constituent les politiques de sécurité.

3 DEUX CAS DE MISE EN ŒUVRE D'UNE POLITIQUE DE SECURITE

Le premier cas sur lequel repose de cette recherche est situé dans une entreprise du secteur bancaire pour laquelle l'enjeu est d'obtenir le certificat attestant de la conformité de leurs pratiques de sécurité à la norme PCI-DSS. Payment Card Industry - Data Security Standard (PCI-DSS) est une norme de sécurité définie et maintenue par le PCI Security Standards Council, un consortium composé notamment de American Express, Discover Financial Services, JCB International, MasterCard, et Visa Inc. (PCI Council, 2015). Cette norme est issue de deux sources normatives. D'abord, elle intègre une partie des normes de la famille ISO27000, essentiellement en ce qui concerne la structure des règles (Rowlingson & Winsborrow, 2006) ; ensuite, elle intègre largement les pratiques existantes dans ce secteur d'activité, et plus particulièrement en ce qui concerne la protection des données sensibles des comptes bancaires (Bonner, ORaw, & Curran, 2011; Morse & Raval, 2008). Le résultat,

actuellement la troisième version, est une norme à la structure et aux exigences précises, mais qui peuvent s'avérer complexes à mettre en œuvre (Bonner et al., 2011).

Le second cas est situé dans une entreprise du secteur de l'énergie, l'enjeu est ici de mettre en œuvre une politique de sécurité dans le département informatique tout en respectant la norme ISO27001. Si la sécurité physique, qui concerne la protection des personnes et des infrastructures industrielles critiques, est fortement ancrée dans la culture de l'entreprise, celle des systèmes d'information est peu développée tant dans le département informatique que dans les autres départements de l'entreprise, et les managers-dirigeants y sont peu sensibilisés. Une première initiative a été menée en 2007 et 2008, mais plus rien n'a été entrepris jusqu'en 2014. Dans ce cas, c'est déjà la norme ISO27001 qui sert de référence normative pour l'élaboration de la politique de sécurité et sa mise en œuvre. Le choix de cette norme s'est « imposé de lui-même », car, pour cette entreprise, il n'existe pas de contrainte externe spécifique au secteur d'activité.

Les deux cas que nous présentons ici ont été sélectionnés de manière à faire apparaître des contrastes quant aux relations de pouvoir et à leur rôle dans la mise en œuvre d'une politique de sécurité de l'information. Ils sont situés dans des entreprises technologiques de taille semblable d'environ 1000 personnes, dont 100 à 120 pour chacun des départements informatiques.

3.1 MÉTHODOLOGIE

À travers ces cas, nous souhaitons étudier le processus de production de règles sociales que les acteurs développent pour mettre en œuvre des règles de sécurité des systèmes d'information, avec un focus sur les relations de pourvoir entre les managers de la ligne hiérarchique et les ingénieurs du service informatique. Dans les deux cas, nous avons eu recours à une méthode qualitative nous permettant de collecter les points de vue, les avis, les perceptions des différents acteurs sur ce processus et de les recouper avec des observations participatives et non participatives et avec des analyses documentaires.

Dans le premier cas, la collecte des données a été réalisée sur le terrain de recherche de 2012 à 2013, dans une approche qualitative composée d'entretiens individuels de managers, d'ingénieurs et également de collaborateurs, d'observations non participatives et participatives réalisées principalement lors de réunions et de groupes de travail. Divers types de documents

ont également été collectés afin de corroborer les observations et interviews. Un ensemble de 20 interviews a été réalisé à partir d'un échantillon représentatif des intervenants de la sécurité.

Dans le second cas, l'approche qualitative repose sur un dispositif principalement composé d'observations non participatives et participatives et de collectes de documents clés, notamment la « politique générale de sécurité de l'information ». Ce dernier a fait l'objet d'une analyse documentaire plus détaillée. Finalement, plusieurs séances de restitution ont permis de présenter les résultats des analyses aux acteurs et recueillir leurs réactions. La présence sur le terrain dans le cadre de ce projet s'est étendue de 2014 à 2015.

3.2 LE PREMIER CAS

L'entreprise est présente dans le secteur bancaire pour le traitement des transactions de paiement depuis le début de l'existence des technologies de paiements par cartes, d'abord à piste magnétique, ensuite à puces et maintenant le paiement mobile. Elle bénéficie d'une bonne réputation dans le domaine et elle a toujours accordé une grande importance à la sécurité de ses opérations. Sa base de clients est large et cet acteur historique reste incontournable dans le secteur, malgré une certaine concurrence qui s'est développée ces dernières années grâce au programme européen SEPA (Single Euro Payments Area - Espace unique de paiement en euros).

Elle connaît bien la problématique de la sécurité des systèmes d'information elle y fait figure de pionnière. Dans le passé, elle a développé ses propres systèmes de sécurité et, encore aujourd'hui, grâce à un programme d'innovation, elle continue à les commercialiser. En revanche, ce qui est nouveau pour elle, c'est la nécessité, voire l'obligation, de conformer les systèmes d'information et les procédures de gestion aux exigences de la norme PCI-DSS. Il s'agit d'une norme externe à l'entreprise, un référentiel comportant 12 catégories d'exigences issues historiquement de la famille des normes ISO27000 (Rowlingson & Winsborrow, 2006) et adaptées au secteur bancaire. L'approche adoptée par les collaborateurs et la direction de l'entreprise consiste à mettre en œuvre une politique de sécurité qui satisfasse aux exigences de cette norme, mais surtout à rencontrer les attentes de l'auditeur-certificateur qui délivrera le certificat de conformité nécessaire au maintien de la licence d'exploitation des paiements électroniques. Un projet de grande envergure a débuté dès que la décision a été prise par la direction de mettre tout en œuvre pour obtenir la certification en deux années. L'objectif est

ambitieux, mais réalisable aux yeux des membres de l'entreprise. Ce projet, à travers des groupes de travail auxquels nous avons pu assister, a permis aux acteurs de construire des lieux d'échanges et d'élaboration de solutions.

Lors de notre présence sur le terrain, nous avons identifié les principaux acteurs de la sécurité : le département IT est composé d'ingénieurs qui maîtrisent les systèmes d'information et les équipements techniques de sécurité ; le département de Sécurité maîtrise les théories et les règles formelles de sécurité ; la direction veille au cap stratégique de l'entreprise. Dans un premier temps, l'autonomie du département IT assure la sécurité des systèmes d'information et procure une certitude de sureté et d'évitement des fraudes et des attaques. Dans un deuxième temps, l'obligation de certification interroge cette autonomie et s'accompagne de nombreuses remises en question sur la manière de « faire » de la sécurité. Le troisième temps est marqué par la négociation d'une nouvelle politique de sécurité plus en ligne avec les recommandations de la norme PCI-DSS. Les discussions portent également sur les modalités de mise en œuvre de la nouvelle politique. Dans le quatrième et dernier temps, la direction et le département de sécurité pérennisent la certification qui doit être renouvelée chaque année. Cela passe notamment par une régulation de contrôle dont le principal dispositif que nous avons identifié est un contrôle strict des budgets et des ressources au département IT. Cependant, à l'intérieur de ces contraintes, l'autonomie des ingénieurs du département IT est maintenue. À aucun moment, nous n'avons observé de mesures disciplinaires ni d'intervention d'autorité quand les instructions de la Direction ne sont pas suivies. C'est même le contraire qui a été observé : lors des interviews, certaines personnes ont déploré un certain manque d'autorité de la part de la Direction pour faire appliquer les décisions.

L'élaboration et la mise en œuvre des règles de la politique de sécurité interviennent lors du troisième temps que nous avons aussi appelé phase de la sécurité négociée. La politique est composée d'un ensemble de documents qui formalisent les choix techniques et les règles de sécurité, mais il n'existe pas un répertoire central qui contient toutes les composantes de la politique ni de document de synthèse auquel les membres de l'entreprise peuvent faire référence.

Lors du processus de construction de cette politique, les acteurs sont passés par une interprétation de la norme PCI-DSS qu'ils ont située dans leur contexte spécifique. Celui-ci est marqué par leur maîtrise des systèmes techniques et par leur conception de la sécurité centrée

sur leur expertise dans le domaine, ce qui leur confère une part importante d'autonomie tout en assurant un niveau élevé de sécurité. Un très haut niveau de disponibilité des services et un faible nombre de fraudes sont à leurs yeux la meilleure preuve de qualité.

Même si les membres de l'entreprise ne rencontrent pas de difficultés particulières avec les concepts techniques et organisationnels de la sécurité, il n'en reste pas moins que de nombreuses questions sont débattues lors des réunions de coordination du projet, parfois de manière intense. Nous avons identifié une quinzaine d'intervenants, dont une moitié sont des ingénieurs du département informatique et l'autre du département de Sécurité et de la Direction.

La nouvelle version de la norme PCI-DSS introduit de nouvelles exigences qui sont parfois perçues par les ingénieurs du département informatique comme inutiles voire comme une régression par rapport à leurs propres pratiques actuelles. La segmentation des environnements techniques est exigée par la norme pour éviter la propagation des attaques et des vols d'information, elle est emblématique des controverses qui ont existé lors du projet. En effet, les ingénieurs perçoivent cette exigence comme un désaveu de leur compétence à sécuriser les systèmes informatiques. Une compétence professionnelle, dont ils sont fiers, est alors remise en question. Des interrogations qui sont relayées par le département de sécurité et la direction qui leur demandent d'apporter la preuve du respect des exigences de la norme en passant par un audit de conformité.

C'est lors de ces réunions, parfois très animées, que nous avons observé que de nouveaux concepts émergent, produisant ainsi autant de nouvelles règles de sécurité. Pour les acteurs, il s'agit d'un travail interprétatif au cours duquel les acteurs construisent un sens aux exigences de la norme et apportent une solution à ce qui apparaissait un problème difficile à résoudre. Finalement, la nouvelle politique de sécurité apparaît comme la résultante des attentes de deux groupes d'acteurs : d'une part les attentes du département de Sécurité et de la Direction qui par divers dispositifs de contrôle veut s'assurer de la conformité à la norme et donc de la certification, et d'autre part les attentes des ingénieurs du département informatique de maintenir un niveau de sécurité compatible avec leurs propres représentations de ce qu'est une sécurité optimale, tout en gardant leur autonomie d'action et d'organisation.

3.3 LE SECOND CAS

Ce second terrain de recherche est situé dans une entreprise du secteur de l'énergie, principalement dans son département informatique. Au regard du marché de l'énergie en Belgique, fortement régulé par le législateur Belge, elle est un acteur historique incontournable. Elle compte plus d'1 million de foyers parmi ses clients. Il y a donc une longue tradition de la sécurité physique et de la protection des personnes (clients et travailleurs). Malgré cela la sécurité des systèmes d'information est peu développée à notre arrivée : il y a bien eu un premier essai de politique de sécurité en 2007 après l'attaque massive d'un virus informatique, mais en 2008 l'initiative semble être abandonnée jusque fin 2013 où la direction décide de la relancer. À cette date, la sécurité informatique est considérée comme relevant de la responsabilité des ingénieurs informaticiens et, à l'image de l'ensemble des utilisateurs, la ligne hiérarchique y est peu sensibilisée.

Dès le départ, la norme ISO27001 de sécurité de l'information est utilisée comme référence, un choix qui n'a jamais fait l'objet de débat ni de remise en question, il s'est imposé comme une évidence. En effet, dans les métiers historiques de l'entreprise, la standardisation des activités et des procédés est forte et les références à des normes sont omniprésentes. On trouve de nombreuses notes de travail, des méthodes et autant de procédures pour toutes les actions liées au métier de producteur et de distributeur d'énergie.

En 2013, la décision est prise de mettre en œuvre une politique de sécurité sous la responsabilité d'un manager situé hiérarchiquement dans un des services du département informatique. Les premières versions sont réalisées à partir des travaux initiés en 2007-2008, mais elle est également abandonnée, du moins en partie, pour repartir sur un nouveau document à la structure plus détaillée et en intégrant une version plus récente du standard ISO27001. Lors du développement de la politique de sécurité, nous n'avons pas identifié de sessions de travail (workshops) et peu d'échanges entre les ingénieurs du département informatique et le manager responsable de la sécurité. À ce stade de notre observation, il s'agit d'une production documentaire assez isolée. Même si les intervenants sont peu nombreux, nous nous sommes intéressés au processus de développement de ce document et nous avons tenté d'observer les relations entre eux. Ce processus est marqué par la présence marquée du directeur du département informatique, intervenant, contrôlant et ne laissant que peu de place au travail interprétatif de la norme par les autres intervenants. Certaines de ses interventions portent sur son propre rôle ou sur celui d'autres managers. Ainsi, des contrôles ont été ajoutés dans la

plupart des processus, parfois en contradiction avec la norme ISO à laquelle il est pourtant fait référence. En particulier, le principe d'indépendance du responsable de la sécurité visant à prévenir les conflits d'intérêts n'est pas respecté.

Les ingénieurs que nous avons rencontrés lors des séances de restitution craignent que les règles de cette politique soient inapplicables, car trop « verrouillées », c'est-à-dire leur laissant peu de marge d'action pour les mettre en œuvre sur le terrain à temps et en heure. Ils ont également utilisé le terme « trop théorique » pour exprimer leur perception de la distance des règles avec leur vécu quotidien qu'ils qualifient de pratique. Certaines règles sont perçues comme « démesurées », « inapplicables dans le contexte actuel ». Cette perception concerne l'effort à fournir pour mettre en œuvre la règle. Cet effort concerne moins les budgets que les changements dans les manières de travailler et la crainte d'alourdir encore un peu plus leurs activités par de nouvelles contraintes techniques et opérationnelles. Nous avons noté qu'ils craignent les conséquences de retards dans la livraison des projets dont ils seraient rendus responsables du fait de respecter les règles de sécurité. Des situations vécues comme un dilemme qui les incite à composer avec les règles de sécurité plutôt qu'avec les délais, la marge de négociation sur les délais de livraison des projets étant très faible.

Pendant cette période, nous avons observé un style de management mettant en œuvre une structure fortement hiérarchique avec parfois jusqu'à 6 niveaux pour les métiers d'interventions et faisant appel aux sanctions disciplinaires allant jusqu'au licenciement de cadres. Sans surprise, la division du travail est forte tant sur le plan vertical qu'horizontal. Par ailleurs, nous n'avons pas observé d'initiatives en faveur de la sécurité de la part des ingénieurs du département informatique. Enfin, nous avons noté que la sécurité des systèmes d'information ne fait pas partie des critères de l'évaluation individuelle.

La politique de sécurité et les règles qui la constituent ont été validées par le comité de direction, mais n'ont pas fait à ce jour (juin 2016) l'objet d'une communication à l'ensemble de l'entreprise.

4 DISCUSSION

4.1 DEUX CADRES NORMATIFS EN CONCURRENCE

Le premier point que révèle notre étude est que les acteurs naviguent en permanence entre deux cadres normatifs que sont d'une part la norme de sécurité des systèmes d'information et d'autre part la norme de gouvernance de leur département informatique ou de leur entreprise. Ils font l'expérience de tensions fortes qui les amènent à composer avec ces deux cadres et à « bricoler » des solutions afin de réduire les distances entre des situations contradictoires. Exemples : « je peux livrer ce projet à temps, mais pas en respectant toutes les règles de sécurité », « si je dois réduire les couts, je ne peux pas implémenter tel système de sécurité ».

La sécurité apparait plus comme une question de gouvernance que comme une question de sécurité et de protection des données. Cette dichotomie est plus marquée dans notre second cas où la principale production documentaire de sécurité a été appelée « gouvernance » et dans laquelle les processus, les rôles et les responsabilités occupent la plus grande partie. Cherchant d'abord à ne pas trop s'écarter d'une certaine idée de la conformité à la norme, ils ne jugent pas systématiquement que tous les termes de la norme sont acceptables et ils tolèrent une certaine non-conformité s'ils perçoivent que les efforts nécessaires sont disproportionnés ou si la solution leur paraît inapplicable.

Dans nos deux cas, ce processus est vu comme contingent, continu et complexe, et il exige de leur part une certaine capacité interprétative de la norme. Ce travail d'interprétation de la norme est crucial : sans lui la norme reste lointaine et déconnectée des situations que vivent les ingénieurs ou les managers, les changements qui apparaissent dans l'environnement sociotechnique risquent d'accroitre encore l'écart et rendre les règles obsolètes, voire inadaptées. Ce qui en matière de sécurité peut avoir des conséquences désastreuses.

4.2 INSTITUTIONNALISER LA SÉCURITÉ COMME PRATIQUE DU POUVOIR

Notre deuxième point fait apparaître l'institutionnalisation de la sécurité comme un objectif de formalisation et de pérennisation des règles en concurrence avec les finalités de sécurisation et de protection des systèmes d'information, et que les relations de pouvoir entre les managers de la ligne hiérarchique et les ingénieurs du département informatique sont un ingrédient important. En d'autres mots, institutionnaliser la sécurité relève d'une pratique du pouvoir qui, en la faisant entrer dans un espace de contraintes voire de coercitions, vise à imposer son acceptation, mais surtout « révèle des relations complexes entre ceux qui sont chargés du

fonctionnement de l'institution et ceux qui en subissent sa loi » (Fecteau & Harvey, 2005, p. 6‑10).

Dans notre premier cas, les relations de pouvoir sont marquées par des régulations autonomes dominantes : autonomie de gestion du département informatique, autonomie des choix technologiques. Les relations de pouvoir sont donc ici plutôt symétriques. Dans le second cas, nous avons observé peu de régulations autonomes dans un espace caractérisé par un « tout à la procédure » traduisant une vision planificatrice de l'informatique à laquelle les ingénieurs du département informatique peuvent difficilement échapper. Les régulations de contrôle sont ici dominantes : contrôle du temps de chacun à l'aide d'un système central de planification et de contrôle des activités quotidiennes ; contrôle accru des productions documentaires. Les relations de pouvoir sont dans ce cas plutôt asymétriques.

En même temps nous avons observé dans le premier cas que les échanges entre les acteurs sont nombreux et variés. Les réunions et les sessions de travail (workshop) sont les lieux de débats parfois intenses et passionnés où les acteurs discutent la norme de sécurité et construisent ensemble des concepts à la lumière de leur environnement sociotechnique. Nous pouvons dire que, dans ce cas, les acteurs sont engagés dans un intense travail interprétatif de la norme. Dans le second cas en revanche, la norme n'a pas fait l'objet de débat, les acteurs l'ont acceptée sans la contester ni la mettre au défi. Nous pouvons dire que le travail interprétatif est faible. Les échanges dans un petit nombre d'acteurs ont essentiellement porté sur l'institutionnalisation de la norme plutôt que sur ses apports à la sécurisation des systèmes d'information. Des questions comme la définition des rôles de chacun dans la sécurité, les niveaux de contrôles des activités et les moyens de vérification à mettre en œuvre pour s'assurer que rien n'échappe à l'institution ont dominé les questions de protection des systèmes d'information.

4.3 FAIRE FACE À L'INCERTITUDE SÉCURITAIRE

Notre troisième point met en évidence que l'intensité du travail interprétatif offre aux acteurs des marges de manœuvre qu'ils peuvent mobiliser pour jouer avec les règles et les orienter selon leurs avantages et leurs intérêts. Il met également en évidence que la norme de sécurité présente une certaine flexibilité instrumentale et interprétative (Orlikowski, 1992) grâce à laquelle les acteurs peuvent réinterpréter des règles et les instrumenter dans des dispositifs de sécurité (des usages, des technologies) adaptés à leur environnement. L'incertitude sécuritaire

amène les acteurs à devoir faire face à des événements impossibles à prévoir, mais ayant potentiellement des conséquences importantes quand ils se produisent. La capacité des acteurs à saisir cette flexibilité et à s'engager dans un travail d'interprétation leur permet de comprendre les événements de la nouvelle situation et à construire de nouvelles règles adaptées.

Les deux cas que nous avons analysés se distinguent également sur ce point. Dans le premier cas, des incidents de sécurité ont déclenché des quasi-crises qui ont pris la forme de vives critiques de la norme et des règles en place de la part de certains ingénieurs du département informatique. Les règles de sécurité et la capacité des acteurs à les questionner leur permettent de faire face aux changements et aux impondérables. Dans le second cas, quand tout se passe bien et que la situation semble sous contrôle, c'est que la règle et le processus sont bons, c'est-à-dire qu'ils ont fonctionné comme prévu par leurs concepteurs. Par contre, quand un incident se produit, c'est que la règle ou le processus n'ont pas été correctement respectés. Il y a personnalisation de la cause de l'incident, il s'agit de trouver le fautif et de renforcer le contrôle de la règle. La capacité de mettre en question les règles de sécurité face à un impondérable est ici assez faible. Il est à craindre que si un incident de sécurité inconnu venait à se produire, les acteurs aient des difficultés à identifier les règles inadaptées et à en construire de nouvelles. Pire, ils risqueraient de rester prisonniers de ces règles sans pouvoir faire face à un incident qui peut se transformer en catastrophe.

Le tableau suivant synthétise les points de discussion ci-dessus à travers les deux cas.

Tableau 1 Synthèse des cas étudiés

Premier cas	*Second cas*
Régulations autonomes dominantes Relations de pouvoir symétriques	Régulations de contrôle dominantes Relations de pouvoir asymétriques
Travail d'interprétation de la norme fort	Travail d'interprétation de la norme faible
Professionnalisation de la norme	Institutionnalisation de la norme

Production de règles de sécurité principalement orientées vers les métiers et les professions	Production de règle de sécurité principalement orientée vers le contrôle et l'organisation
Règles de sécurité adaptables aux changements sociotechniques	Règles de sécurité peu adaptables aux changements sociotechniques

5 CONCLUSION

Dans des environnements où la présence de normes externes de type ISO est forte, notamment pour des questions de sécurité des systèmes d'information, la nature des règles de sécurité produites est étroitement liée aux relations de pouvoir à l'œuvre dans ces organisations. Elle est le lieu d'un travail de négociation et d'interprétation plus ou moins intense de la norme. Des relations de pouvoir symétriques dans lesquelles les régulations autonomes sont dominantes, le travail interprétatif de la norme est plutôt intense et les règles de sécurité sont orientées vers les métiers. Cette situation facilitera l'adaptation des règles face aux changements sociotechniques et aux impondérables de la gestion de la sécurité des systèmes d'information. À l'inverse, des relations de pouvoir asymétriques dans lesquelles les régulations de contrôle sont dominantes, le travail interprétatif de la norme est plutôt faible et les règles de sécurité sont associées aux fonctions institutionnelles. Cette situation favorise une gestion de la sécurité basée sur les dispositifs de contrôles des processus et des acteurs pour imposer les règles de sécurité. Celles-ci peuvent se révéler peu adaptables aux changements et aux situations imprévues dans les processus.

Cela nous permet d'envisager des pistes d'intervention et d'actions managériales dans les missions de mise en œuvre de politiques de sécurité informatique en fonction des relations de pouvoir en place dans l'organisation. Dans le premier cas, lors d'une intervention, il convient de vérifier que l'adaptation au terrain respecte encore les minimas nécessaires pour avoir une politique de sécurité adaptée à la réalité externe. Le risque d'une trop grande spécificité est qu'elle ne soit pas adaptée aux exigences de l'évaluation externe par des auditeurs. Dans le second cas, l'intervention veillera à trouver des méthodes qui compensent la tendance

planificatrice et contrôlante et permettent de faire émerger des règles plus adaptées à la réalité du terrain d'où surgissent des événements de sécurité imprévus et potentiellement menaçants.

Notre contribution n'est évidemment pas sans limites. Malgré la grande richesse des cas, notre base empirique est de petite taille et il conviendrait de l'élargir pour aller plus loin dans les propositions que nous formulons et aux implications managériales que nous pourrions proposer. Plusieurs relations seraient à développer et à explorer, à mettre en regard des pratiques et des méthodologies. Citons déjà le rôle de la culture et de l'histoire de l'organisation dans l'interprétation des normes, le rôle de l'environnement politique et du contexte économique. Notre analyse ne les a pas envisagées à ce jour.

Notre étude soutient une approche des règles de sécurité dans les organisations qui intègre la question des relations de pouvoir. Notre approche peut être qualifiée de critique en ce sens qu'elle ouvre aussi à la remise en question de l'utilisation des modèles dominants dans la gestion des systèmes d'information, qu'elle cherche à intégrer la parole de tous les acteurs, convaincue que chacun est le lieu d'interprétations cherchant à donner du sens à ses actions et aux actions des autres.

6 REFERENCES/BIBLIOGRAPHIE

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

BNP Parisbas Fortis: Conditions générales relatives aux cartes de banque et aux services phone banking et pc banking. (2016, décembre 4). BNP PARISBAS FORTIS. Consulté à l'adresse https://www.bnpparibasfortis.be/pics/BE/common/fr/lib_download/doc_server/ds03056.pdf?contract_type=sta

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.

Crozier, M., & Friedberg, E. (1977). *L'acteur et le système: les contraintes de l'action collective* (Le Seuil). Paris.

de Terssac, G. (2012). La théorie de la régulation sociale : repères introductifs. *Revue Interventions économiques. Papers in Political Economy*, (45). Consulté à l'adresse http://interventionseconomiques.revues.org/1476

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.

Fecteau, J.-M., & Harvey, J. (2005). *La Régulation Sociale Entre l'Acteur et l'Institution / Agency and Institutions in Social Regulation: Pour une Problématique Historique de l'Interaction / Toward an Historical Understanding of Their Interaction*. PUQ.

Hale, A. R., Heijer, T., & Koornneef, F. (2003). Management of Safety Rules: the case of railways. *Safety Science Monitor*, *7*(1), 1–11.

Hardy, G. (2006). Using IT governance and COBIT to deliver value with IT and respond to legal, regulatory and compliance challenges. *Information Security technical report*, *11*(1), 55‑61.

Hatch, M. J., & Cunliffe, A. L. (2009). *Théorie des organisations: de l'intérêt de perspectives multiples*. De Boeck Supérieur.

International Organization for Standardization. (2016). Les normes dans le monde d'aujourd'hui. Consulté 7 décembre 2016, à l'adresse http://www.iso.org/sites/ConsumersStandards/fr/1_standards.html

International Organization for Standardization. (s. d.). Consulté 20 février 2015, à l'adresse http://www.iso.org/iso/home/standards.htm

ISACA. (2015). COBIT 5: A Business Framework for the Governance and Management of Enterprise IT. Consulté 12 novembre 2015, à l'adresse http://www.isaca.org/cobit/pages/default.aspx

ISO/IEC 27001. (2013). Information technology — Security techniques — Information security management systems — Requirements.

ISO/IEC 27002. (2013). ISO/IEC 27002 - Code of practice for information security controls.

IT Governance Institute. (2006). *Information security governance guidance for boards of*

directors and executive management. Rolling Meadows, Ill.: IT Governance Institute. Consulté à l'adresse http://www.books24x7.com/marc.asp?bookid=30815

Leplat, J. (1998). About implementation of safety rules. *Safety Science*, *29*(3), 189‑204. https://doi.org/10.1016/S0925-7535(98)00022-8

Meynen, P. (2009). How to Write a Security Policy. *ISACA Journal*, *1*. Consulté à l'adresse http://www.isaca.org/Journal/Past-Issues/2009/Volume-1/Documents/How-to-Write-a-Security-Policy.pdf

Morse, E. A., & Raval, V. (2008). PCI DSS: Payment card industry data security standards in context. *Computer Law & Security Review*, *24*(6), 540‑554. https://doi.org/10.1016/j.clsr.2008.07.001

Nizet, J., & Pichault, F. (2011). L'interprétation des standards en situation extrême : le pouvoir fait-il la différence? *Management & Avenir*, *41*(1), 394. https://doi.org/10.3917/mav.041.0394

Orlikowski, W. J. (1992). The Duality of Technology: Rethinking the Concept of Technology in Organizations. *Organization Science*, *3*(3), 398‑427.

Orlikowski, W. J. (2000). Using Technology and Constituting Structures: A Practice Lens for Studying Technology in Organizations. *Organization Science*, *11*(4), 404‑428.

Orlikowski, W. J., & Robey, D. (1991). Information technology and the structuring of organizations. *INFORMATION SYSTEMS RESEARCH*, *2*, 143--169.

PCI Council. (2015). What Is the PCI Security Standards Council? Consulté 30 janvier 2015, à l'adresse https://www.pcisecuritystandards.org/security_standards/role_of_pci_council.php

Perrow, C. (1984). *Normal Accidents: Living with High Risk Technologies (Updated)*. Princeton University Press.

Pfeffer, J. (1981). *Power in organizations* (Vol. 33). Boston: Pitman Marshfield, MA.

Pichault, F., & Nizet, J. (2012). *Coordination du travail et théorie des organisations*. Dunod.

Reynaud, J.-D. (1997). *Les Règles du jeu: l'action collective et la régulation sociale*. Paris: A. Colin.

Reynaud, J.-D. (1999). *Le conflit, la négociation et la règle* (Édition : réimpression 2007). Toulouse: Triades.

Reynaud, J.-D., & Richebé, N. (2007). Règles, conventions et valeurs. *Revue française de sociologie*, *Vol. 48*(1), 3‑36.

Rowlingson, R., & Winsborrow, R. (2006). A comparison of the Payment Card Industry data security standard with ISO17799. *Computer Fraud & Security*, *2006*(3), 16‑19. https://doi.org/10.1016/S1361-3723(06)70323-2

Simonsson, M., Johnson, P., & Wijkström, H. (2007). Model-based IT governance maturity assessments with COBIT. In *ECIS* (p. 1276‑1287).

Terssac, G. de, Boissière, I., & Gaillard, I. (2009). *La sécurité en action* (Édition : Premiere edition). Toulouse: Octares Editions.

Tuttle, B., & Vandervelde, S. D. (2007). An empirical examination of CobiT as an internal

control framework for information technology. *International Journal of Accounting Information Systems*, *8*(4), 240‑263.

Villers, M. E. de. (2009). *Multidictionnaire de langue française*. Montréal: Québec Amérique.

Weick, K. E., Sutcliffe, K. M., & Obstfeld, D. (2005). Organizing and the Process of Sensemaking. *Organization Science*, *16*(4), 409‑421. https://doi.org/10.1287/orsc.1050.0133

Weick, K. E., & Vidaillet, B. (2003). *Le sens de l'action : Karl Weick : sociopsychologie de l'organisation*. Metz: Vuibert.

Wikipedia. (2015, novembre 6). CobiT. In *Wikipédia*. Consulté à l'adresse https://fr.wikipedia.org/w/index.php?title=CobiT&oldid=120237685

Wood, C. C. (1995). Writing infosec policies. *Computers & Security*, *14*(8), 667–674.