CONFERENCE DE SEPTEMBRE 2021 DU GROUPE EUROPEEN D'ADMINISTRATION PUBLIQUE
BRUXELLES

SÉCURITÉ DES SYSTÈMES D'INFORMATION
QUAND LA SCIENCE ORIENTE L'ACTION VERS L'IMPACT

Jean-Jacques Viala[1]

Résumé

Face à l'accroissement exponentiel des attaques informatiques, la mise en sécurité numérique a été élevée au rang de politique nationale, même si ses modalités opérationnelles sont de la responsabilité des acteurs locaux. Les Responsables de la Sécurité des Systèmes d'Information dans les établissements jouent donc un rôle fondamental. Pourtant, la littérature ne dégage pas de 'fil conducteur' permettant de formuler des hypothèses sur leurs choix stratégiques essentiels. L'étude du corps de connaissance du *« Certified Information Security Manager »* - certification professionnelle dont l'orientation gestionnaire est la plus marquée - met en lumière l'importance de la démarche stratégique de capabilisation du personnel (traduction en français d'*empowerment*). Celle-ci est néanmoins rendue malaisée du fait d'un langage technique peu accessible aux non-initiés. Un récent modèle de maturité des pratiques de cybersécurité (*« Cybersecurity Maturity Model Certification »*) présente l'avantage de favoriser l'inspiration du personnel, d'autant plus efficacement qu'il a une base scientifique. La science ne pourrait-elle pas orienter l'action dans d'autres politiques publiques?

[1] Maitre d'enseignement en gestion de projet ;
Master en sciences de gestion (GESTS552 Field Project Management), Solvay Brussels School of Economics and Management, Université Libre de Bruxelles *; c*ourriel : jean-jacques.viala@ulb.be

« Nouvelle pandémie », telle est une labellisation désormais utilisée s'agissant de l'accroissement exponentiel des attaques informatiques (Escande 2021, Stacey 2021).

Elle renvoie à la politique de sécurité numérique (ici indifféremment qualifiée de sécurité informatique, de sécurité des systèmes d'information ou de cybersécurité).

La France a mis en place une « Stratégie nationale pour la cybersécurité » en mettant en place des solutions technologiques, des soutiens institutionnels et des formations (ANSSI 2021).

Il s'agit typiquement de ce que certains auteurs ont qualifié de « politique constitutive », signifiant par-là que le dispositif de l'État exclut réglementation ou dotation budgétaire spécifique aux organisations publiques locales (Lowi 1972). Les modalités du traitement opérationnel de la sécurité numérique restent à inventer localement (Thoenig et Duran 1996), dans les établissements.

L'appellation « pandémie » évoque par ailleurs des travaux sur le sida qui avaient notamment conclu qu'un leadership technico administratif efficace pouvait garantir des résultats (Setbon 1993).

De ce point de vue, l'un des principaux responsables français de la sécurité numérique indique que les projets de mise en sécurité informatique, s'ils sont bien conduits, « durcissent » les systèmes au point de prévenir les attaques (Poupard 2021), malgré un contexte international agressif (Boyer 2020, TASS 2021).

La présente communication entend se focaliser sur les choix stratégiques du responsable de la sécurité des systèmes d'information dans un établissement (RSSI) en vue de décrire des caractéristiques de l'efficacité de son pilotage.

Une revue de la littérature rendra compte des travaux existants sur la mise en sécurité informatique, lesquels ne permettent pas de comprendre comment le RSSI fonctionne et décide de son projet. Un code de pratiques professionnelles de référence sera ensuite présenté et confronté à deux théories stratégiques. On fera apparaître qu'en sécurité informatique, la capabilisation du personnel (traduction en français d'*empowerment*) et l'utilisation d'un modèle de maturité fondé sur la science constituent deux facteurs clés de succès. On conclura en s'interrogeant sur la portée de ces résultats dans le contexte d'autres politiques publiques.

1 La mise en sécurité informatique comme choix stratégique

La mise en sécurité informatique est une discipline quinquagénaire. Les travaux ont comporté une perspective technique (1.1) ou managériale (1.2) sans dégager les principes des choix stratégiques essentiels du RSSI dans une organisation (1.3).

1.1 Les approches techniques

À lire certaines grandes institutions scientifiques et techniques, la sécurité informatique est née en même temps que l'ordinateur et a, depuis, mobilisé les ingénieurs au point de considérer qu'ils devraient tous en avoir lu les premiers travaux (NIST 1998).

La réalité est plus nuancée. Il y a encore cinq ans, la sécurité des systèmes d'information n'était pas enseignée dans les dix meilleurs bacheliers américains de science informatique (Jackson Higgings 2016). En fait, les pratiques sont travaillées par une offre commerciale de technologies que chaque nouvelle vague d'attaques stimule (Hoo 2021).

La mise en sécurité numérique se présente dès lors sous la forme d'une collection de contrôles, regroupés par types ou sous-familles telles que les contrôles de processus de gestion, les actions de formation ou la protection physique, et les contrôles fondés sur une technologie particulière comme la cryptographie (NIST 1995).

La littérature technique sur la mise en sécurité est une littérature grise qui fait du responsable de la sécurité des systèmes d'information un metteur en œuvre (NIST 2017).

Certains auteurs évoquent toutefois de façon intéressante un effort de cohérence avec le mouvement de normalisation et de certification professionnelle en cybersécurité. Ils soulignent l'importance des corps de connaissance associés à la certification (Whitman et Matord 2018). Notre démarche de recherche s'alimentera de cette perspective.

1.2 Les approches managériales

L'émergence d'Internet et son utilisation croissante dans les affaires auraient, selon certains auteurs, favorisé une conception plus managériale de la cybersécurité, et suscité une attention plus soutenue de la part des dirigeants (von Solms 2000).

Pourtant, des revues de la littérature pointent le nombre relativement faible de publications traitant de la dimension stratégique du travail du responsable de la sécurité des systèmes d'information et la quasi absence d'attente des dirigeants à cet égard. (Whitten 2008, Onibere Ahmad and Maynard 2017).

Une recherche extensive fait toutefois apparaitre l'activité des RSSI des organisations vis-à-vis des parties prenantes, leurs tâches de pilotage, leurs actions de communication, mais aussi la nécessité pour eux d'impliquer les personnels (Johnson and Goetz 2007).

La question est alors de dégager des 'fils conducteurs' de la mise en sécurité numérique permettant de formuler des hypothèses sur les choix stratégiques essentiels du RSSI.

1.3 Deux théories stratégiques pour la sécurité des systèmes d'information

Les contributions managériales sur la sécurité des systèmes d'information suggèrent de considérer deux théories stratégiques:

- l'alignement avec la *« meta-governance »* de la politique constitutive de sécurité numérique, qui se traduit par la gestion de la performance, la coordination externe, le pilotage interne et l'attention aux dimensions culturelles (Peters 2010),
- l'approche quasiment inverse, qui part du fait que les employés sont intelligents et qui valorise leur engagement interne ; Ceci suppose de favoriser leur capabilisation c'est-à-dire leur implication dans la définition des objectifs et des moyens de les atteindre (Argyris 1998).

La phase actuelle d'« institutionnalisation » de la cybersécurité (von Solms 2000) invite à prendre en considération le mouvement de certification des responsables. Notre objet d'étude le reflètera.

2 Capabiliser le personnel et s'appuyer sur la science pour mettre en sécurité numérique

Dans cette partie, nous allons présenter rapidement notre dispositif d'étude (2.1). La double nature stratégique du rôle du responsable de la sécurité des systèmes d'information dans un établissement sera explicitée (2.2). Nous traiterons enfin des enjeux d'un modèle de maturité de la cybersécurité qui est basé sur la science (2.3).

2.1 Le corps de connaissance du « *Certified Information Security Manager* » comme objet d'étude

Avec le *« Certified Information Systems Security Professionals »* dont l'orientation technique est plus marquée, le *« Certified Information Security Manager »* (*CISM*) constitue l'un des certificats les plus enviables pour les responsables de la sécurité des systèmes d'information, et même pour les professionnels en général (Global Knowledge, 2021).

L'examen du *CISM* comporte 150 questions et recouvre quatre domaines (gouvernance de la sécurité de l'information, conformité et gestion du risque de l'information, développement et gestion du programme de sécurité de l'information et gestion des incidents de sécurité de l'information) qui constituent autant d'étapes d'un projet de mise en sécurité.

L'association mondiale ISACA qui fédère des professionnels informatiques depuis 1967, l'a décerné à plus de 46 000 praticiens. Nous allons analyser le contenu de son manuel d'étude lequel alimente les questions de l'examen (ISACA 2015).

La dualité des démarches stratégiques sous-jacentes, de gouvernement de la mise en sécurité numérique et de capabilisation du personnel d'une organisation, y est aussi manifeste que problématique.

2.2 L'enjeu de la capabilisation du personnel dans la mise en sécurité numérique

Nous avons analysé chaque section du manuel d'étude du *CISM* pour identifier les deux dimensions, d'une part l'alignement avec la *« méta-governance »* (gestion de la performance, coordination externe, le pilotage interne et l'attention aux dimensions culturelles), et d'autre part la capabilisation du personnel (implication dans la définition des objectifs et dans les moyens de les atteindre).

La synthèse de ce codage fait apparaître que la capabilisation du personnel est une composante significative de la mise en sécurité, avec d'autant plus de poids qu'il s'agit de tâches de conception.

Chapitre du manuel du *CISM*	Occurrences de l'alignement avec la *« meta-governance »*	Occurrences de la capabilisation du personnel
Gouvernance de la Sécurité de l'Information	100%	50%
Conformité et gestion du risque de l'Information	100%	57%
Développement et gestion du programme de sécurité de l'information	100%	28%
Gestion des incidents de sécurité de l'information	100%	7%

Tableau des occurrences des deux types de démarches stratégiques dans le manuel du *CISM*

Cette dualité n'est pas sans soulever une série de difficultés pour les responsables de la sécurité des systèmes d'information.

On a pu considérer qu'elle nécessite d'être reconnue et l'effort de capabilisation du personnel développé au maximum dans les organisations (Argyris 1998). Tel est d'ailleurs le fondement de certaines questions – discriminantes – de l'examen du *CISM*.

Le domaine de la cybersécurité comporte des difficultés liées à son langage technique peu accessible aux non-initiés (Parenty and Domet 2020). À cet égard, l'utilisation d'un modèle de maturité des pratiques de cybersécurité, présente un intérêt certain.

2.3 L'étalonnage de la cybersécurité comme deuxième facteur clé de succès: le cas du *« Cybersecurity Maturity Model Certification »*

Les modèles de maturité des pratiques de sécurité numérique (ISACA 2015) constituent des outils précieux du RSSI dans ses tâches de mobilisation des dirigeants de leur établissement (Parenty and Domet 2020).

Ils sont aussi une source d'inspiration à destination du personnel. Le *« Cybersecurity Maturity Model Certification »* dévoilé en mars 2020 dans le contexte de la préservation des informations militaires, présente l'atout supplémentaire d'une solide base scientifique (2020-1).

En effet, en condensant des recherches financées durablement par l'État fédéral américain (Carnegie Mellon University 2020-2), ce *« Cybersecurity Maturity Model Certification »* définit l'impact des mesures techniques, procédurales et organisationnelles de sécurité numérique en proposant des niveaux d'efficacité croissants. Il devient possible de choisir effectivement un niveau de sécurité numérique.

S'il était maintenu et utilisé par plusieurs établissements, ce modèle constituerait un outil de quantification précieux pour évaluer la politique de sécurité numérique, contribuant ainsi à résoudre une difficulté typique des politiques constitutives (Thoenig et Duran 1996).

Conclusion La science au secours des politiques publiques ?

Notre contribution s'intéresse à la dimension stratégique de la mise en sécurité informatique en partant du constat qu'elle a été insuffisamment étudiée.

L'objet d'étude est le corps de connaissance du *« Certified Information Security Manager »*. En effet, parmi les certifications professionnelles exigeantes qui sont proposées aux responsables de la sécurité des systèmes d'information dans les établissements, c'est celle dont l'orientation gestionnaire est la plus marquée. Une analyse du contenu de ce code de pratiques professionnelles dévoile une démarche stratégique d'alignement avec la *« meta-governance »* de la sécurité numérique qui représente un renforcement des capacités de gouvernement d'un établissement, et une autre qui vise la capabilisation du personnel.

Cette dualité pèse sur le travail des responsables de la sécurité des systèmes d'information. Ceux-ci peuvent néanmoins s'appuyer sur un modèle de maturité de la cybersécurité (*« Cybersecurity Maturity Model Certification »*) qui gomme les difficultés liées à la technicité du langage, et qui est mobilisateur parce que fondé sur une approche scientifique du niveau de sécurité.

La validité de notre étude aurait bénéficié d'un double codage des dimensions stratégiques identifiées dans le corps de connaissance du *CISM*, et d'autres contributions sont nécessaires pour augmenter le niveau de confiance dans nos résultats.

Les travaux ici exposés invitent à en examiner la portée s'agissant d'autres politiques publiques. La capabilisation des acteurs fait partie des intentions stratégiques notamment dans certaines politiques constitutives (Viala 2002). L'enrichissement des agendas de recherche sur le management des projets (Svejvig and Anderson 2015) pourrait faire progresser la connaissance sur la mobilisation de référentiels basés sur la science.

Références

Agence Nationale de la Sécurité des Systèmes d'Information – ANSSI (2021), *Cybersécurité, faire face à la menace : la stratégie française*, 18 février

Argyris C. (1998), Empowerment: the Emperor's New Clothes, *Harvard Business Review*, vol 76(3), pp 98-105

Boyer B. (2020), *Guerilla 2.0 : guerres irrégulières dans le cyberespace*, Ligne de front

Carnegie Mellon University and The John Hopkins University (2020-1), *Cybersecurity Maturity Model Certification*, March 18

Carnegie Mellon University (2020-2), *Building the Cybersecurity Maturity Model Certification*, July 28

Escande P. (2021), Piratage : la nouvelle épidémie, *Le Monde*, 9 mars, p 19

Global Knowledge (2021), *Get the skills. Get the certifications. Get the higher salary*,

Hoo E. (2021), Cyberattacks surged, and investors came knocking, *The New York Times - International Edition*, 28 July, p 7

Jackson Higgings K. (2016), Top US Undergraduate Computer Science Programs Skip Cybersecurity Classes, *DARKReading*, 4 July

Johnson E. and Goetz E. (2007), Embedding Information Security into the Organization, *IEEE Security and Privacy Magazine*, 5(3), pp 16-24

Lowi T. (1972), Four systems of policy, politics and choice, *Public Administration Review*, July-August, vol 32, n°4, pp 298-310

National Institute of Standards and Technology – NIST (1995), *Special Publication 800-12: an introduction to computer security*, Computer Security Resource Center

National Institute of Standards and Technology – NIST (1998), *Early Computer Security Papers (1970-1985)*, Computer Security Resource Center

National Institute of Standards and Technology – NIST (2017), *Special Publication 800-12r1: an introduction to computer security*, Computer Security Resource Center

Onibere M. Ahmad A. and Maynard S. (2017), The Chief Information Security Officer and the Five Dimensions of a Strategist, *Proceedings of the Pacific Asia Conference on Information Systems*, July 19

Parenty T. and Domet J. (2020), A leader's guide to cybersecurity: why boads need to lead – and how to do

Peters G. (2010), Meta governance and public management, in *The New Public Governance*, Routledge, pp 36-51

Poupard G. (2021), Les Etats sont aggressifs dans l'espace cyber, *Le Monde*, 11 juin, p 20

Setbon M. (1993), *Pouvoirs contre sida*, Seuil

Stacey K. (2021), Lunch with the FT: Chris Krebs, *Financial Times - Life and Arts*, 7 February, p 3

Svejvig P. and Andersen P. (2015), Rethinking project management: A structured literature review with a critical look at the brave new world, *International Journal of Project Management*, vol 33, pp 278-290

TASS (2021), Cyber attacks against Russia carried out from US, Germany, the Netherlands, experts say, 7 July

Thoenig J.C. et Duran P. (1996), l'Etat et la gestion publique territoriale, *Revue Française de Science Politique*, 46ème année, n°4, pp 580-623

von Solms B. (2000), Information Security – The third wave ?, *Computers and security*, vol 19 (7), pp 615-620

Viala J.J. (2002), Le développement du contrôle de gestion dans les administrations de l'État, *La Lettre du Management Public*, n°40, juillet-août, pp 3-4

Whitman M. & Mattord H (2018), *Principles of Information Security Sixth Edition*, Cengage Learning

Whitten D. (2008), The Chief Information Security Officer: an analysis of the skills required for success, *Journal of Computer Information System*, vol 48(3)