Vers un principe de conception sûre des systèmes cyber-économiques

Stéphanie Thiéry, Didier Fass

Titre : Vers un principe de conception sûre des systèmes cyber-économiques

Comment prendre en compte les facteurs techniques, humains et organisationnels pour améliorer la sécurité des systèmes cyber-économiques

Penser la cyber-économie à l'interface des facteurs techniques, humains et organisationnels.

Auteurs : Stéphanie Thiery-Dubuisson (1,2) et Didier Fass (1,3)
1. ICN, Nancy Metz
2. CEREFIGE Université de Lorraine
3. MOSEL, LORIA UMR CNRS 7503, Université de Lorraine

Résumé :
Actuellement l'approche audit contrôle concerne la maîtrise de l'organisation et la fiabilité du reporting financier des entreprises.
Les actifs intangibles valorisés selon les normes internationales sont particulièrement sensibles aux manipulations et aux attaques internes ou externes.
Or la prise en compte du risque cyber couvre essentiellement les risques techniques informatiques (du SI) interne. Les aspects facteurs humains et organisationnels ne sont ni clairement connus ni clairement identifiés, en particulier par les instances de décision (CA, CS, comex…)

Penser l'entreprise comme un système intégré « *sécurité critique* » et les risques inhérents à son domaine d'activité sont un enjeu théorique et pratique.
Notre approche se fonde sur une analyse critique épistémologique et méthodologique, en particulier de l'intégration humain-systèmes et du contrôle audit.

Notre présentation aura pour but de clarifier :
- Les concepts de bases associant forensic, lutte contre la criminalité économique, contrôle et « safety by design »
- les enjeux de l'intégration facteurs techniques, facteurs humains et organisationnels (juridiques, managériaux, culturels…)

Nous illustrerons notre présentation par des exemples issus des domaines de l'aérospatial et de l'audit.

Références :

1. NACD, Cyber-Risk Oversight, ed. Larry Clinton, Director's Handbook Series, National Association of Corporate Directors, Washington DC, USA (2017)
2. Clark, M. E. and Harrell C., Unlike chess, everyone must continue playing after a cyber-attack, Journal of Investment Compliance, vol. 14, 4, pp. 5 - 12 (2013)
3. KPMG, Boardroom Questions. Cybersecurity - What does it mean for the board (2016) https://home.kpmg/content/dam/kpmg/be/pdf/boardroomquestions/boardroom-questions-cyber-security-what-does-it-mean-for-the-board.pdf
4. Kamiya, S. Kang, J.K., Kim, J., Milidonis A. and Shulz R.M, What is the impact of successful cyberattacks of target firms?, Fisher College of Business Working Paper Series (2018)
5. Thiery-Dubuisson, S. *L'audit*. Paris: La Découverte. (2009). https://doi.org/10.3917/dec.thier.2009.01
6. Fass, D. Augmented Human Engineering: A Theoretical and Experimental Approach to Human Systems Integration, Systems Engineering - Practice and Theory, Boris Cogan, IntechOpen, DOI: 10.5772/33373. (2012)