Adaptive Cybersecurity Management Framework: Leveraging Information Capital and BPM for Risk Mitigation and Value Creation

Keywords: Risk Management, Security Standards, Information Capital, AI, Cyber-Physical Systems, Business Value Creation

Context:

Cybersecurity management and Business Process Management (BPM) are critical to address the increasing complexity of cyber threats and digital transformation [1]. The scientific literature highlights the significance of information capital in risk assessment and value creation, particularly in relation to the confidentiality, integrity, and availability (CIA) of data [2]. However, measuring the impact of security standards (ISO 27001, NIST, MITRE, NIS2) on business performance remains a major challenge.

Furthermore, the rise of emerging technologies such as artificial intelligence (AI), cyberphysical systems, and advanced connectivity solutions is reshaping security management practices [3, 4]. Existing security frameworks often struggle with fragmentation and lack of integration between offensive and defensive cybersecurity strategies, creating inefficiencies in risk mitigation and compliance.

This CIFRE Ph.D. position is funded in collaboration with MD6, a company specialized in cybersecurity and digital transformation. The primary objective is to develop a unified cybersecurity management framework, using methodologies to improve project planning, risk management, and organizational resilience. The research will establish a framework that applies BPM to streamline cybersecurity processes, ensuring regulatory compliance while improving security operations and value creation [5, 6]. This research also aims to understand companies' adoption of cybersecurity processes across industries to identify different trajectories and strategies. Factors that inhibit or encourage the adoption of cybersecurity should be investigated.

The ideal candidate should have a background in information systems management, corporate governance, accounting with an interest in cybersecurity. Familiarity with programming languages such as Python (or others) would be considered a valuable asset.

The position requires on-site presence at MD6's headquarters, with regular travel to the partner research laboratory (located in Strasbourg).

Organizations:

- HuManiS (Humans and Management in Society, UR 7308), EM Strasbourg Business School, University of Strasbourg
- MD6

Desired starting date:

- 1^{st} September 2025

Thesis supervisors:

- Jessie PALLUD, PhD, Full Professor: jessie.pallud@em-strasbourg.eu
- Laura GEORG SCHAFFNER, PhD, Associate Professor: laura.g.schaffner@em-strasbourg.eu
- Youssef SELLAMI, PhD: youssef.sellami@idemoov.fr
- Adrien GIRARDEAU: adrien.girardeau@md6.fr

Candidates should send an application by email including the following documents:

- A detailed curriculum vitae
- A cover letter
- A transcript of Master 1 and Master 2 grades
- The Master 2 thesis (if applicable).

The application must be sent simultaneously to the following three email addresses: jessie.pallud@em-strasbourg.eu, laura.g.schaffner@em-strasbourg.eu and youssef.sellami@idemoov.fr

References

[1] Chris Florackis, Christodoulos Louca, Roni Michaely, and Michael Weber. Cybersecurity risk: The data. *Chicago Booth Research Paper*, (23-01), 2023.

[2] R Blank and P Gallagher. Nist special publication 800-30 revision 1 guide for conducting risk assessments. *National Institute of Standards and Technology*, 2012.

[3] Emilie Bout, Valeria Loscri, and Antoine Gallais. How machine learning changes the nature of cyberattacks on iot networks: A survey. *IEEE Communications Surveys & Tutorials*, 24(1):248–279, 2021.

[4] Muhammad Mudassar Yamin, Mohib Ullah, Habib Ullah, and Basel Katt. Weaponized ai for cyber attacks. *Journal of Information Security and Applications*, 57:102722, 2021.

[5] Qusai Ramadan, Daniel Strüber, Mattia Salnitri, Jan Jürjens, Volker Riediger, and Steffen Staab. A semi-automated bpmn-based framework for detecting conflicts between security, data-minimization, and fairness requirements. *Software and Systems Modeling*, 19:1191–1227, 2020.

[6] Ikechukwu Oranekwu, Lavanya Elluri, and Gunjan Batra. Automated knowledge framework for iot cybersecurity compliance. In *2024 IEEE International Conference on Big Data (BigData)*, pages 6336–6345. IEEE, 2024.