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, 2, 3]. 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 [4]. 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 [5, 6]. 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 [7, 8]. 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, Cybersecurity researcher: youssef.sellami@md6.fr
- Adrien GIRARDEAU, DevSecOps Engineer: 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 four email addresses: jessie.pallud@em-strasbourg.eu, laura.g.schaffner@em-strasbourg.eu, youssef.sellami@md6.fr and adrien.girardeau@md6.fr.

About MD6:

MD6 Consulting, based in Entzheim, specializes in strategic roles centered around information technologies and critical infrastructure. The company offers innovative solutions and services to support its clients in their digital transformation and the optimization of their IT infrastructures.

MD6 Consulting's core areas of expertise include:

- Data Center Infrastructure: Providing and implementing robust, high-performance infrastructures to meet the growing demands of data storage, processing, and resource management—covering everything from disaster recovery (DR) to business continuity (BC), with integrated operator connectivity.
- Application Modernization: Supporting businesses in optimizing their development processes and continuous integration through DEVOPS technologies, with a strong focus on containerization.
- Cybersecurity: Offering IT audits, consulting, and governance. MD6 acts as a technology integrator, implementing advanced protection solutions to secure information systems, safeguard sensitive data, and ensure compliance with regulatory requirements.
- Cloud and Managed Services: Managing private cloud infrastructures with customized hosting, outsourcing, and managed service solutions that ensure system performance, security, and scalability.

With its deep expertise and tailored solutions recognized at the national level, MD6 Consulting empowers businesses to meet their technological challenges with confidence. For further references see `https://www.md6.fr/enterprise/about?`

Architecture de gestion adaptative de la cybersécurité : valorisation du capital informationnel et de la BPM au service de la maîtrise des risques et de la création de valeur

Mots clés: Gestion des risques, normes de sécurité, capital informationnel, intelligence artificielle, systèmes cyber-physiques, création de valeur pour l'entreprise

Contexte:

La gestion de la cybersécurité et la gestion des processus métier (BPM) sont essentielles pour faire face à la complexité croissante des menaces numériques et à la transformation digitale [1, 2, 3]. La littérature scientifique souligne l'importance du capital informationnel dans l'évaluation des risques et la création de valeur, notamment en ce qui concerne la confidentialité, l'intégrité et la disponibilité (CID) des données [4, 9]. Toutefois, mesurer l'impact des normes de sécurité (ISO 27001, NIST, MITRE, NIS2) sur la performance des entreprises demeure un défi majeur.

Par ailleurs, l'émergence de technologies telles que l'intelligence artificielle (IA), les systèmes cyber-physiques et les solutions de connectivité avancées redéfinit les pratiques de gestion de la sécurité [5, 6]. Les cadres de sécurité existants souffrent souvent de fragmentation et d'un manque d'intégration entre les stratégies offensives et défensives de cybersécurité, ce qui entraîne des inefficacités dans la réduction des risques et le respect des obligations réglementaires.

Ce poste de thèse CIFRE est financé par MD6, une entreprise spécialisée dans la cybersécurité et la transformation numérique. L'objectif principal est de développer un modèle unifié de gestion de la cybersécurité, en s'appuyant sur des méthodologies visant à améliorer la planification des projets, la gestion des risques et la résilience organisationnelle. La recherche visera à établir un modèle appliquant la gestion des processus métier (BPM) à l'optimisation des processus de cybersécurité, tout en assurant la conformité réglementaire et en renforçant les opérations de sécurité et la création de valeur [7, 8]. Cette recherche a également pour but de mieux comprendre l'adoption des processus de cybersécurité par les entreprises, tous secteurs confondus, afin d'identifier les trajectoires et stratégies différenciées. Les facteurs favorisant ou freinant cette adoption devront être examinés.

Le ou la candidat(e) idéal(e) devrait avoir une formation en gestion des systèmes d'information, en gouvernance d'entreprise, avec un intérêt marqué pour la cybersécurité. La maîtrise de langages de programmation tels que Python (ou autres) constituerait un atout précieux.

Le poste implique une présence sur site au siège de MD6, avec des déplacements réguliers au laboratoire de recherche partenaire situé à Strasbourg.

Organisations:

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

Date de début souhaitée:

- $1er$ septembre 2025

Encadrants de thèse:

- Jessie PALLUD, HDR, Professeur des universités: jessie.pallud@em-strasbourg.eu
- Laura GEORG SCHAFFNER, PhD, Maître de conférences: laura.g.schaffner@em-strasbourg.eu
- Youssef SELLAMI, PhD, Chercheur en cybersécurité: youssef.sellami@md6.fr
- Adrien GIRARDEAU, Ingénieur DevSecOps: adrien.girardeau@md6.fr

Les candidats doivent envoyer une candidature par email comprenant les documents suivants :

- Un CV détaillé
- Une lettre de motivation
- Les relevés de notes de Master 1 et Master 2
- Le mémoire de Master 2 (le cas échéant).

La candidature doit être envoyée simultanément aux quatre adresses email suivantes : jessie.pallud@em-strasbourg.eu, laura.g.schaffner@em-strasbourg.eu, youssef.sellami@md6.fr and adrien.girardeau@md6.fr.

À propos de MD6 :

MD6 Consulting, basé à Entzheim, se spécialise dans des rôles stratégiques axés sur les technologies de l'information et les infrastructures critiques. L'entreprise propose des solutions et des services innovants pour accompagner ses clients dans leur transformation numérique et l'optimisation de leurs infrastructures informatiques.

Les domaines d'expertise principaux de MD6 Consulting comprennent :

- Infrastructure de Data Center : Fourniture et mise en place d'infrastructures robustes et performantes pour répondre aux exigences croissantes du stockage des données, du traitement et de la gestion des ressources — couvrant tout, de la reprise après sinistre (DR) à la continuité des affaires (BC), avec une connectivité opérateur intégrée.
- Modernisation des applications : Accompagnement des entreprises dans l'optimisation de leurs processus de développement et d'intégration continue grâce aux technologies DEVOPS, avec un accent particulier sur la conteneurisation.
- Cybersécurité : Réalisation d'audits informatiques, de conseils et de gouvernance. MD6 agit en tant qu'intégrateur technologique, mettant en œuvre des solutions de protection avancées pour sécuriser les systèmes d'information, protéger les données sensibles et garantir la conformité aux exigences réglementaires.
- Cloud et services managés : Gestion des infrastructures de cloud privé avec des solutions d'hébergement sur mesure, d'externalisation et de services managés garantissant la performance, la sécurité et l'évolutivité des systèmes.

Avec son expertise approfondie et ses solutions sur mesure reconnues au niveau national, MD6 Consulting permet aux entreprises de relever leurs défis technologiques en toute confiance. Pour de plus amples références, consultez `https://www.md6.fr/enterprise/about?`

References

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

[2] Laura Georg-Schaffner and Enrico Prinz. Corporate management boards' information security orientation: an analysis of cybersecurity incidents in dax 30 companies. *Journal of Management and Governance*, 26(4):1375–1408, 2022.

[3] Elodie Manthé, Rémi Mencarelli, and Jessie Pallud. The dark side of crowdsourcing of complex tasks: a systematic literature review. *Information & Management*, page 104108, 2025.

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

[5] 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.

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

[7] 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.

[8] 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.

[9] Laura Georg-Schaffner, Elodie Behnam, and Jessie Pallud. Cyber risk disclosure: How transparent are cac40 companies in their annual reports? *Forthcoming in French Journal of Management Information Systems.*, 2025.