Auteur: Nick Nieuwenhuis MSc, Cyber Security Researcher and Consultant. Feel free to reach out to nick@nicknieuwenhuis.com for any questions or inquiries

Integrating Cyber Security and Enterprise Architecture to improve Risk Management

Cyber risks have evolved from mere annoyances to catastrophic events, posing challenges for enterprises worldwide. This article highlights the findings of recent research on the integration of Cyber Security and Enterprise Architecture to Improve Cyber Risk Management, executed within the Cyber Security research centre of the Utrecht University of Applied Sciences.

As organizations take on various digital transformation initiatives to deliver value to their stakeholders, cyber security (CS) has never been more important. IBM's Ponemon institute estimates the average cost of a data breach to be at an all-time high: 4.88 million USD. Additionally, organizations must comply with growing laws and regulations, such as the renewed NIS2 directive (cyberbeveiligingswet), Cyber Resilience Act (CRA), and the Digital Operational Resilience Act (DORA). These challenges underscore the need for a holistic and integrated approach to manage cyber risks.

Enterprise Architecture (EA) can be a promising vehicle to manage these cyber risks because of its holistic capacity overarching the business, data, application and technology domains. Prior research on EA benefits highlighted that EA could improve risk management, quality management and business-and-IT alignment. Unfortunately, CS and EA are isolated departments in most enterprises, resulting in ineffective cyber risk management that keep enterprises vulnerable.

Research Method

This research aimed to bridge the gap by studying how CS and EA could be integrated, by identifying blockers and enablers for this integration. Furthermore, the research aims to understand how this integration impacts Cyber Risk Management. The central question in this research is: How can Cyber Security and Enterprise Architecture be integrated in relation to Cyber Risk Management within enterprises? To collect data, a literature review on the state-of-the-art of CS and EA integration was combined with a focus group (6 participants) and interviews (4 participants). Participants where seasoned experts in the EA and/or CS domain, from various backgrounds and had at least 10 years of professional experience. The participants were chosen to ensure a rich diversity of perspectives.

Findings

This section summarizes the most important findings of this research. Before starting in-depth questions around CS-EA integration, participants were asked to what extent CS and EA are currently integrated within enterprises based on their experience. The answer was a 3.2 on a five-point scale, which translates to 'somewhat integrated'. Participants mentioned that CS is already part of some EA frameworks, such as TOGAF and SABSA. Another participant mentioned that architects work in close collaboration with the CISO.

To validate the existing literature on CS-EA integration, participants were asked to rate six strategies for integrating CS and EA in order of perceived importance. The results and their respective score (0-100) can be found below:

1. Integrating Cyber Security into EA Frameworks (29.2)
2. Adopting the Security-by-Design paradigm (25.8)
3. Integrating business requirements with security requirements (18.4)
4. Leveraging EA to provide input for Cyber Risk Assessment (15)

5. Mapping identified cyber risks to EA components (5.8)
6. Managing cyber risks by aligning business & IT activities (5.8)

Other strategies not mentioned in literature are:

- Giving security representation in the (enterprise) architecture board
- Making security an explicit part of the architecture
- Improving Security awareness of EA professionals

Blockers

A score of 3.2 meant that there is room for improvement. Participants were asked which blockers hinder the level of integration. Three main themes emerged:

1. **Different mindsets & focus:** Both CS and EA teams work mostly in isolation and have different goals and purposes. A participant remarked: 'Enterprise Architects thinks in possibilities, while CS professionals think in limitations'
2. **Organizational misalignment:** Both departments usually report to different managers, and only 'meet' each other late in the process. Security is therefore often seen as an afterthought.
3. **Skills & knowledge gaps:** CS professionals usually do not have the architecture skills to make (strategic) decisions. EA professionals on the other hand lack the in-depth security knowledge to fully incorporate security in architectural processes and documents.

Enablers

The research also highlighted enablers that facilitate the integration of CS and EA. The main themes that emerged were:

Security integration in EA Frameworks: Security is to some extent already integrated within EA frameworks, which makes decision-making, modeling concerns and viewpoints, and establishing a common language easier.

Adopting Secure Development Methodologies: Secure software development methodologies, especially DevSecOps and Security by Design, also facilitate integration, because security measures are added upfront instead of reactively.

Security Awareness in the Business: Another enabler of the integration is rising security awareness in the business. This means more non-technical employees are aware of cyber risks, such as phishing and fraud. This makes it easier to implement security controls from an architectural standpoint.

Impact on Cyber Risk Management

Ultimately, sound integration of CS and EA impacts Cyber Risk Management. To assess how this was impacted, participants were asked to map improvements to the ISO 27005 cyber- and information security risk management process. The (perceived) improvements and their respective process step can be found below.

Context establishment: The integration of CS and EA makes it easier to identify and assess risks on the organizational and process level, including identifying supply chain risks and stakeholder dependencies.

Risk Assessment: The integration of CS and EA improves risk identification, analysis and evaluation because EA can clarify dependencies in process and technology and the risks involved.

Risk Treatment: Most improvement could be mapped to risk treatment phase, especially risk mitigation (reducing the risk to an acceptable level). CS-EA integration realizes faster and more structural solution for risk mitigation that can be reused, aligning security controls with the architecture.

Monitoring and Review: CS-EA integration makes it easier to monitor security controls for their expected and desired effects.

Overall, multiple improvements were mentioned by all research participants. Although these are qualitative statements and thus no statistically significant conclusion can be drawn upon this, it shows the promising effects of CS-EA integration and the positive impact it can have on Cyber Risk Management.

Conclusion

This research highlights that integrating security into EA frameworks, adopting secure development methodologies, improving skills and knowledge, and aligning both departments in the organizational structure can yield benefits for enterprises seeking to improve their Cyber Risk Management capabilities. Although future research is necessary to validate and extend these findings, EA shows to be a promising vehicle for managing cyber risks.

For more information, references and further reading, please find the full and free to download thesis 'Towards the Integration of Cyber Security and Enterprise Architecture to Improve Cyber Risk Management' (pdf) here.