SUPPORTING THE CISO FOR OVER 20 YEARS

As CISO, if you don’t have a clear understanding of the threat actors and attacks paths that relate to your specific business, if you only have partial visibility of business information assets and no clear understanding of the impact of a breach, and if you don’t know where the edge of the business is and paths across it, then I fail to see how CISO’s are able to report the true level of Cyber Risk to the Board and deliver proportional risk treatment plans.

With a bottom up focus on increasingly complex and costly technical mitigations, I believe the Enterprise Security & Risk functions needs to focus just as much resources on an effective method to gain visibility, model, describe, and understand the functions, structures and interrelationship of business & security components within the enterprise. Security Innovation Europe are uniquely positioned to provide that insight for the CISO.

Alex Port
CISO
Security Innovation Europe Ltd
# Table of Contents

- Enterprise Cyber Security Strategy .............................................. 2  
- Enterprise Security Architecture Blueprint ............................. 3  
- Security Solution Architecture .................................................. 4  
- Cyber Security Consultancy Services ........................................ 5  
- Secure DevOps Services ............................................................ 6  
- About Us ................................................................................. 7
The pace of digital innovation and the disruption this introduces as businesses evolve is outpacing the ability for business strategy to adapt to Cyber requirements. This is especially true where:

- Enterprises are becoming ever more complex in their digital operations.
- Information and privacy related risks are already unsighted.
- New dynamic threats are regularly emerging.
- Threat actors are targeting cyber-naive Enterprises.

The ability to properly understand and deal with all these elements is critical to an organisation’s success, so as not to negatively impact operations, finances or their reputation (commercially or with regards to protecting data).

Managing today’s risk means that Enterprises must now transform the role of Cyber within their enterprise risk function and address this cyber risk not as an IT problem but as a Business owned issue.

By implementing a Cyber Security Strategy, based on a known baseline of cyber control capabilities, with a defined Enterprise Security Architecture (ESA) Blueprint based on the business’ appetite for risk, allows Enterprises to effectively manage a dynamic threat landscape.

This approach delivers to the CISO an understanding of the true value of the Enterprise’s information assets as well as insight into the business impact of likely cyber events. This can now be clearly articulated to gain board-level support for a business aligned, risk based, proportional response.

Board level reporting now becomes understandable in terms of current and projected business risks, threat priorities and trends. ROI can now be clearly identified in terms of reduction in risk operating costs. This is supported by enhanced security controls to enable each line of business and IT function to address current and future risks, understand threat priorities and consider Cyber Security by Design embedded as part of the business change function.
Our process enables a repeatable measurement of risk and the effectiveness of proportional control improvements. This continuous assessment philosophy allows enhanced visibility of the true level of information risk and the detailed reporting a contemporary CISO demands.

Using a dynamic contextual risk model, an architectural blueprint supported by technical patterns gives the CISO clear situational awareness of their enterprise risk and how RoI is managed.

This visualised of risk in the enterprise allows the security professional to model the security architecture and controls as Risk, Attack and Threat models evolve.

The components referenced in the Security Architecture, perform functions to protect the confidentiality, integrity and availability of information assets and information systems in the environment.

Always contextual to the business risk appetite, these will include a combination of people, process and technology based security controls, security services and security products. Details are captured in use case driven security patterns designed to reduce both the likelihood of an attack being initiated or a breach being successful.

Users of the Security Architecture patterns will come from across all business functions and include business, application & technical architects, information security and risk practitioners, project managers, software developers, IT implementers and 3rd parties. Patterns ensure that both business and technology stakeholders have trusted cyber security guidance and approved solutions.

This approach to treating cyber security requirements by design allows the business to evolve at pace without accruing additional cyber risk.

Once the Cyber Security Strategy and Architecture has been defined, establishing wholesale improvements across an organisation usually requires changes addressing several areas covering policy, people, operational process and technology. A Cyber Security Transformation Programme is generally used as the means of coordinating complex changes across your business, whether its delivering missing foundational security capability or looking at Cyber maturity improvements.
Our deep technical foundation allows us to fulfil an effective and active technical stakeholder role in the delivery of a business or technology roadmap. With consideration of governance, functional and non-functional requirements, oversight and assurance to both high and low level design detail.

We comfortably work with Executive & Senior Technical Stakeholders, Business Analysts, Project and Programme Managers with exposure to formal methodologies such as Prince2.

This wide and deep experience permits a significant contribution to successful strategic and tactical architecture, program & project delivery and to engage, support and challenge at the most senior management and executive levels.

---

**Strategic**

- *Current & Future Stage Analysis*
- *Enterprise Security Transformation*
- *Enterprise Security Planning*

---

**Tactical**

- *Security Technical Solution Design*
- *Project Delivery*
- *Tactical & Strategic Deployments*
- *Security Solution Integration*
With the increasing likelihood of cyberattacks and data breaches, it is important to know your business has the appropriate level of cyber defence in place for your threat profile and risk appetite.

As part our wider Strategic and Architectural services we offer a range of capabilities to help measure, manage and control Cyber Risk within your organization, we provide several Cyber Security Consultancy services, to help you select and implement the right cyber defence for your business.

---

**Enterprise Risk Modelling**

- **Contextual Business Impact Assessment**
- **Enterprise Security Benchmarking**
- **Prioritised Threat Modelling**
- **Attack Path Analysis**
- **Risk Scenario Modelling**
- **Dynamic Visualisation & Trend Reporting**

**Cyber Security Health Checks**

- **Determine your ability to identify, protect and defend your critical information against attacks**
- **Security Penetration tests your internal and external infrastructure to identify weaknesses**

**Benefits**

- **Supports business decision on security investment**
- **Benchmark of current capability & risk**
- **Based on industry standards**
- **Identifies areas requiring immediate attention**
- **Helps plan allocation of resources and finance**
- **Determine if past remediation activities have been successful**
- **Remediation can be prioritised and planned according to appetite for risk**

Security Innovation Europe promotes a pragmatic, good practice, SABSA aligned architectural methodology. Our expertise allows us to develop and deliver business aligned, risk based, security reference architecture blueprints. As part of an associated strategy & road-maps this wide and deep Security Architecture experience permits a significant contribution to successful program & project delivery.
Our Secure DevOps Services identify critical issues and exposures, and deliver a prioritised set of recommendations required to align with agreed business risk appetite.

Delivered as part of a planned improvement program, or single activity, our services are led by our certified Cyber Security Consultants include

Health Checks

- Application vulnerability assessment
- Infrastructure and network penetration testing
- Web application penetration testing
- SDLC Maturity Assessment

Services

- Threat Modelling (TTP’s)
- Static code analysis & defect remediation prioritisation
- SATS / IAST / DAST integration with DevOps
- DevOps training
- Build hardening security review
About Us

From global brands to FTSE100 listed financial services firms, Security Innovation Europe has helped organisations assess and build effective Enterprise Cyber Security Strategies, Security Architectures and roadmaps. Delivering a demonstrable ROI showing sustainable, long term cyber risk reduction whilst still enabling secure business transformation. Furthermore, Security Innovation Europe has supported the technical delivery of business transformation, program and project level initiatives.

Security Innovation Europe promotes a pragmatic, good practice, SABSA aligned architectural methodology. Our expertise allows us to develop and deliver business aligned, risk based, security reference architecture blueprints. As part of an associated strategy & road-maps this wide and deep Security Architecture experience permits a significant contribution to successful program & project delivery.

We understand organisations are at different levels of enterprise architectural maturity or may not even been aware of some of the concepts. We can provide expertise and services aligned to your current level of architectural maturity.

For a confidential discussion contact

Marc Dunlop
Operations Director

Tel: +44 0203 597 5020
Mob: +44 07956 895 005
e-mail: Marc.Dunlop@securityinnovationeurope.com