CONVOTIS

Business IT · Managed IT · Platform IT

Security governance integration in fast-growing environments

Introduction & Case Study

Nikola Dinic, Group CISO

19.09.2023

AGENDA

01 Overview

02 Security Governance

03 High-growth pace

04 Implications & Measures

05 Open points & Questions

01

Overview

Overview

Security governance

- Definition & Anti-Definition
- Major elements
- High-growth pace
- Challenges
- Conclusions

02

Security Governance

Security governance

Definition[1]

- Security governance is a process for overseeing the cybersecurity teams who are responsible for mitigating business risks
- Security governance leaders make the decisions that allow risks to be prioritized so that security efforts are focused on business priorities rather than their own
- They also govern the interplay of mitigating identified business risks, addressing internal and external threats, and dealing with compliance requirements

[1] https://www.gartner.com/en/information-technology/glossary/security-governance

Security governance

Anti-Definition – what is it not?

- Solely IT-risk-oriented, inflexible approach
- Antipole to agile methodology
- Methodology set to quantify all security governance aspects
- Solely compliance-based requirement
- One man task
- Everyone's task

Security governance
Major Elements

Major Elements[1]

- Setting clear roles and responsibilities
- Comprehensive cyber strategy
- Cyber security in existing risk management
- Promotion of culture of cyber resilience
- Planning for cyber security incidents

[1] Cyber Security Governance Principles, Australian Institute of Company Directors, October 2022

03

High-growth pace

Growth

Substantial growth in all business aspects

- Growth of 3-4 newly acquired entities per year
- Approx. 50-100 new employees per year
- Substantial geographical dispersion (Europe, North America, Africa etc.)
- Vast variety of different security cultures, company backgrounds & services as well as compliance requirements and governance maturities
- Repeating changes in the management board
- Strong financial and expansion goals

04

Implications & Measures

High-growth pace

Implications I

- **Setting clear roles and responsibilities**
  - Cyber risk and cyber strategy not featuring periodically on board agendas
  - Chair and board not annually reviewing skills to ensure that directors have a minimum understanding of cyber security risk
  - Limited or no external review or assurance of cyber risk controls and strategy
  - No clear lines of management responsibility for cyber security
- **Comprehensive cyber strategy**
  - Lack of formal documentation of the organisation's approach to cyber security in critical areas: IAM, Asset Management etc.
  - Limited identification and management of key digital assets and data, who has access and how they are protected
  - The cyber strategy and risk controls are not subject to internal and external evaluation and periodic refinement relative to evolving threats
  - Lack of data governance framework to guide how data is collected, held, protected and ultimately destroyed
  - Prolonged vacancies in key cyber management roles

[1] Cyber Security Governance Principles, Australian Institute of Company Directors, October 2022

High-growth pace

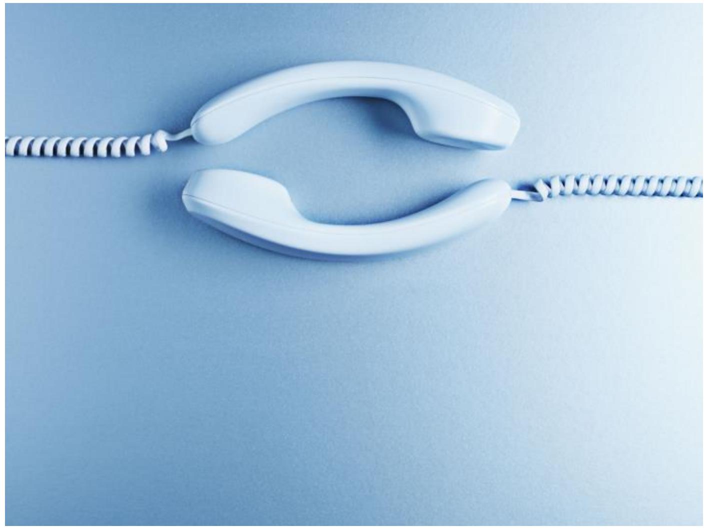
Implications II

- **Cyber security in existing risk management**
  - Cyber risk not reflected and addressed in existing risk management frameworks
  - Low coverage of key business players in risk identification & contextualization
  - Over reliance on the cyber security controls of key service providers (e.g. cloud software providers)
  - Implementation of operational measures to fight high-risk areas
- **Promotion of culture of cyber resilience**
  - Communication from leaders does not reinforce the importance of cyber resilience to staff (cyber is seen as an issue only for frontline staff to manage)
  - There is a culture of ‘exceptions’ or workarounds for board and management with respect to cyber hygiene and resilience
- **Planning for cyber security incidents**
  - The board and senior staff have not undertaken scenario testing or incident simulations to test the Response Plan
  - Likely scenarios and consequences are undocumented with lessons from simulations not being captured
  - No post incident review with board and management involvement

Measures

Security governance & Communication

- Identification of key IT and Management Stakeholders
- Setting open and direct communication culture
- Regularity and quality of communication content
- Communication channel selection depending on audience size and type
- Multi-layer approach



Measures
Security Strategy

- Integration with/based on IT Strategy
- Focus on business goals and perspectives
- Responding to changing threat environment
- Responding to changing internal environment
- Continuous review and enhancements
- Documentation and avaialibilty of key policies/procedures

Measures

Security Risk Management

- Identification of key IT and Management Stakeholders
- Adequate identification & context reflection
- Implementation of mitigation measures
- Quantification of relevant risks
- Regular review & assessment

Measures

Security Awareness & Project Management

- Real life scenarios with financial & reputational impact
  - One-Click evolvement chain
  - Video Material & Live sessions
  - Memory Markers
  - Recaps

- Involvement facilitation through no-blame culture

- Timely and agreed security project management
  - Sound scoping
  - Finishing up
  - Available & Accesible documentation
  - Realistic Budget allocation

05

Open points & Questions

Security governance integration in fast-growing environments

Thank you!

CONVOTIS

Business IT

Managed IT

Platform IT