STORMGuidance

Cyber Security Governance:
Latest Trends, Threats and Risks. January 2024

The Importance of Effective Cyber Security governance

-an incident responders view

Introduction

Mark Saunders
Cyber/Infosec bod

- Senior Cyber Advisor for STORM Guidance, a niche independent cyber advisory
- Information Security Consultant, Incident Responder & Digital Investigator
- Worked and advised on many incidents across a broad range of organisations and industries

STORM Guidance

Full service offering for reinsurers, insurers, brokers and clients

Assess

Lightweight cyber risk assessments to enable clients to learn and improve their cyber risk management maturity levels.

Plan

Helping insured clients to create, learn (through training) and exercise/test their plans in dealing with different types of cyber incidents in the context of their business.
NCSC Accredited CIE provider

Respond

Delivering a fully coordinated and Integrated Cyber Incident Response Team (I-CIRT).

ReSecure: full service offering for insured clients and CIR verification for insurers.

CyberCare: retainer and subscriber for cyber crisis response and proactive services.

What is Governance for Cyber Security?

A quick and dirty description

Generally –

A framework of policies, practices and procedures aimed at the protection and management of information or data assets.

Aligning cyber security strategy with an organisation's business objectives

Why is it useful?

What are the benefits of good governance

- Provides guidance on (hopefully) secure and mature behaviours and standards
- Provides a consistency in approach across the organisation
- Allows for processes that can control or reduce risks to the organisation
- Can ease regulatory and legal compliance
- Helps enforce accountability and responsibility
- Helps ensure strategic alignment of cyber security with organisation’s goals and values
- Can aid with effective resource allocation
- Can help foster a culture of awareness, training, and understanding
- Prepare the organisation for adverse incidents

An important note

No matter how great your governance framework is on paper, it is meaningless unless:

- It is properly implemented
- Effectively monitored
- Rigorously enforced

Without this, its effectiveness is severely limited and can expose the organisation to risk

Common Failures

Cyber Security Governance is a large domain, so I will cover highlights of areas where poor governance has led to issues (and STORM's involvement).

This is not an exhaustive list by any means.

Separation of duties

A fundamental control mechanism to prevent fraud, ensure accountability, and enhance the integrity of processes

Examples:

- Payment processing
- System Admins and audit processes
- Procurement & Approval
- Access Control
- HR & Payroll

Separation of Privileges

A control to limit usage of privileged accounts

Examples:

- Separation of admin and user accounts
- Separation of different privilege levels for specific purposes

Documentation & Document Control

A control to ensure knowledge is codified and available to the organisation when needed

Examples:

- Asset register
- Network Diagrams
- Service Manuals
- IR & DR plans
- Policies, standards, & procedures
- Training

Data Governance

Controls to ensure data is secure (CIA) & managed in accordance with the organisation's requirements

Examples:

- Access & security controls required
- Lifecycle (ownership, consent, retention, purpose, destruction)
- Compliance
- Threat modelling
- Data flow documentation
- Training

Personnel

Controls to ensure personnel adhere to governance imperatives

Examples:

- Contractually documented security responsibilities
- Background checks
- Training
- Starters/Movers/Leavers
- RBAC and PoLP

IR & DR

Plans for when things go bad and testing them

Examples:

- Security Incidents
- Insider threats
- System failure
- Supply issues
- Key personnel unavailable

Closing thoughts

- Effective governance helps ensure controls are in place and working
- Failure in coverage, implementation, and enforcement can leave an organisation exposed
- It is not easy, but not impossible either.
- Effort and resource is required, as is SLT support and buy-in
- Technology comes and goes, good governance is forever (and evolves)

STORMGuidance

THANK YOU

CONTACT DETAILS

W: **www.stormguidance.com**
E: **contact@stormguidance.com**


STORMGuidance