Cyber Security:

Benefits of a business aligned and risk based approach

Duaine Styles

February 9th, 2016

Standard disclaimer:

- This discussion is intended for educational purposes only and does not replace independent professional judgement in sizing information security governance, risk and strategy activities for any given organization. Statements of fact and opinions expressed are those of the presenter and not Torchmark or any subsidiaries of Torchmark.

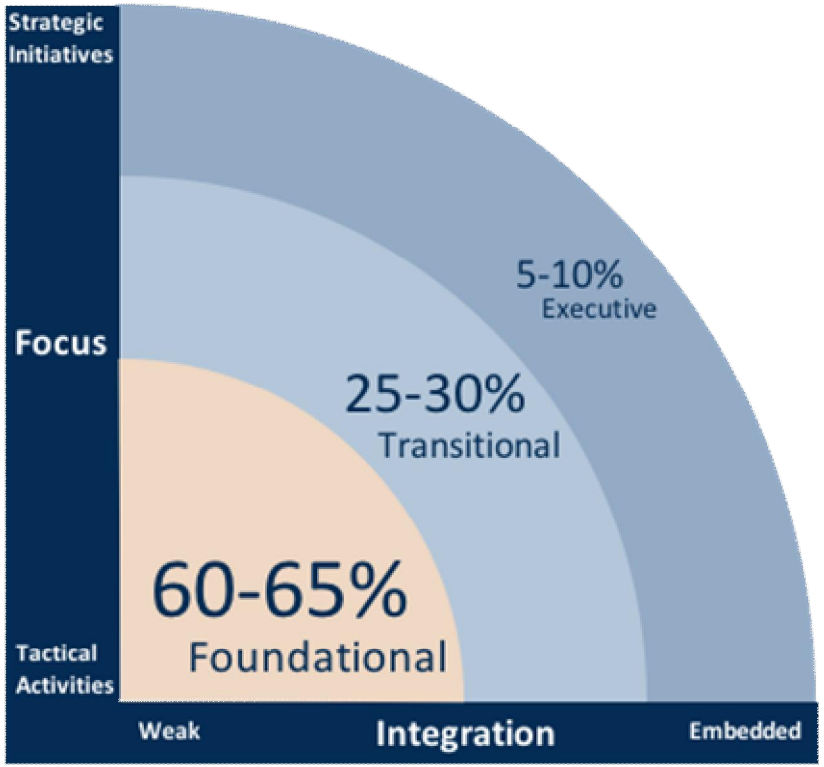
The Great Debate: What is Information Security?

- Service Aligned view: S/he who delivers the service, owns the service and strives for excellence.
  - CISO reports into IT.
    - Governs with IT Policies
    - Delivers technical security services
    - Monitors compliance with standards
    - “owns” security

Is Security this?

- Business Aligned view: S/he who makes the gold and pays the bills, owns the risk and makes the decisions about service delivery levels, funding and risks to accept.
  - CISO reports to BoD or Exec. business management
    - Advises executives who own risk and authorize Enterprise Policy.
    - Security services are set to the organization's risk tolerance
    - Identifies information risk in the context of brand, reputation and cash flow impact.
    - Aligns security services with business strategy, regulations and the threat environment
    - Provides a framework for assurance to flow to BoD and Executives.
    - Security becomes an attribute that is delivered as part of another standard process.

CISO Impact Quotient (CIQ)



Source: IANS Research 'The 7 Factors of CISO Impact' Copyright 2015.

Most mature industries for Cyber Security

- Finance
  - FFIEC Examination Handbooks since 1996
  - Latest changes Fall 2015
- Insurance
  - NAIC Examination Handbooks
  - Latest changes 2016
- Health Care
  - HIPAA/HITECH

Trends in Cyber Security Governance

- FFIEC IT Examination Handbook – Management (Revised Nov. 2015)
  - …While in the past the office of the CISO was considered a technology function, the role has become a strategic and integral part of the business management team. The CISO should be an enterprise-wide risk manager rather than a production resource devoted to IT operations.
  - To ensure independence, the CISO should report directly to the board, a board committee, or senior management and not IT operations management.

Risk Ownership and Security Service Delivery

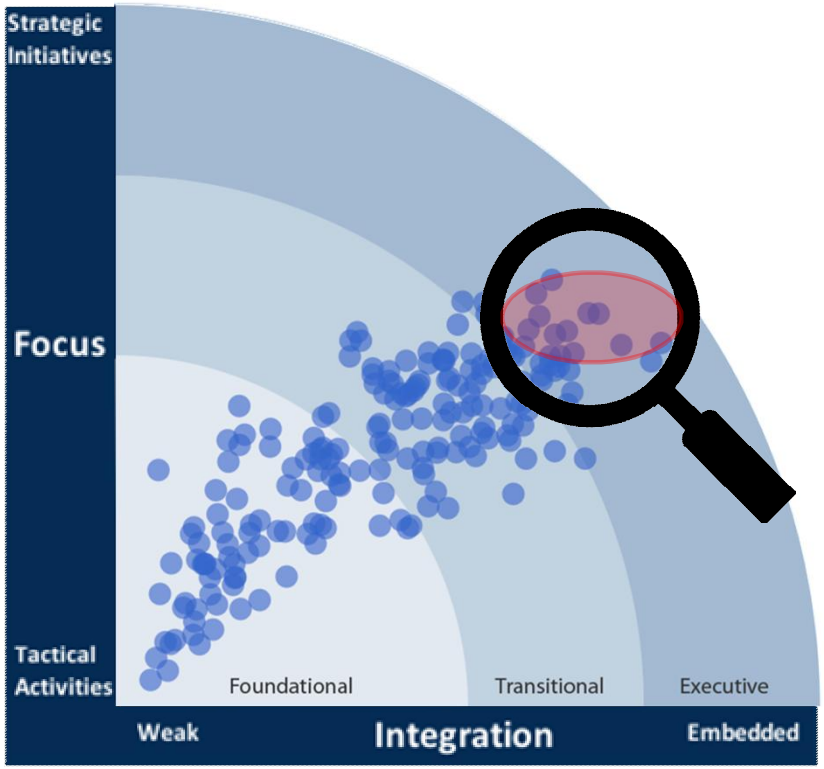
- Who owns risk?
- Who delivers security services as a part (attribute) of their normal processes.
  - IT Operations: About 1/3
  - IT Applications: About 1/8
  - Human Resources, Facilities & Physical Security: About 1/4
  - Procurement & Legal: About 1/8

*Back of the napkin assessment. Results vary base upon organizational structure and responsibilities.

Examples of security delivered as a part of standard processes

- HR
  - Background checks for employees who access sensitive information
- IT
  - Provisioning User Accounts to business roles
  - Managing Technical Vulnerabilities via configurations and patching
  - Running security technologies
- Physical Security
  - Escorting vendors in secured areas
  - Monitoring secured areas
- Facilities
  - Implementing cameras and door swipes to security design

The best think and look differently



CISO Impact Quotient (CIQ)

Source: IANS Research 'The 7 Factors of CISO Impact' Copyright 2015.

A possible structure

- Information Security Governance
  - Executive Steering Committee and Board reporting
  - Information Security Charter
  - Enterprise Security Policy
  - Security Strategy
  - Enterprise Security Architecture
  - 3rd party Information Risk Program
  - Internal Information Risk Program
  - Information Security Metrics
- Operations
  - Those who deliver security services throughout the company
- Compliance
  - Internal SLA monitoring by management
  - Internal Audit
  - External Regulatory review and External Audits

Enterprise Security Architecture: Providing Traceable results

The Business View	The Facility Manager's View	Business Strategy, Regulations, Threats & Risks	Enterprise Risk Appetite <	Metrics →
The Architect's View		ISO/ 27001/27002 Aligned Policy and Standards & Security Stratey		
The Designer's View		Security Programs that define what services are necessary by risk levels.		
The Builder's View		Protocols, procedures, logging, detection and other security mechanisms.		
The Tradesman's View		Firewalls, IPS, AV, SIEM, Identity Management Tools…		

Example: Disposing of IP/PII/PHI

The Business View	The Facility Manager's View	GLBA, HIPAA, Brand for sales growth & Cash Flow					Business Risk
The Architect's View		Policy: Media should be disposed of securely when no longer required.					Risk in the context of overall requirements
The Designer's View		Asset Management Program specifies destruction criteria and standards					
The Builder's View		IT Proc., Facilities Proc., Physical Security Proc. & Vendor Contracts					SLA Monitoring and Custodian Attestation
The Tradesman's View		Host Systems	End User Systems	Office Systems	Cloud Serv.	Shred Bins	

The CISO's view:

Data Disposal		Service Custodian	IA Findings	External Findings
Div: 1				
	Host		0	0
	End User		0	0
	Fax/Copier		0	0
	3rd Party Vendors		3	1
	Paper		2	1
Div: 2				
	Host		5	1
	End User		0	0
	Fax/Copier		0	0
	3rd Party Vendors		1	0
	Paper		1	0

Board reporting example:

		Custodian	IA	External
Broad Security Objective		Attestation	Findings	Findings
Is all PII disposed of Properly?			12	3

- May also include:
  - Quarter or quarter comparison of risk rating
  - General risk trend information
  - Inherent risk vs. residual risk
  - Summarized risk statements

Benefits of Business Aligned Security

- A business aligned and enterprise wide risk management approach:
  - Creates more complete coverage of security services.
  - Puts risk ownership at the level that funding is decided.
  - Provides traceable results that connect the business risk to the implementation.
  - Gives various levels of management metrics in their context for maximum impact.
  - Sets the security service levels to the risk appetite of leadership.

The End!