

# Business At the Speed of Cyber

Understanding the CISO Dilemma

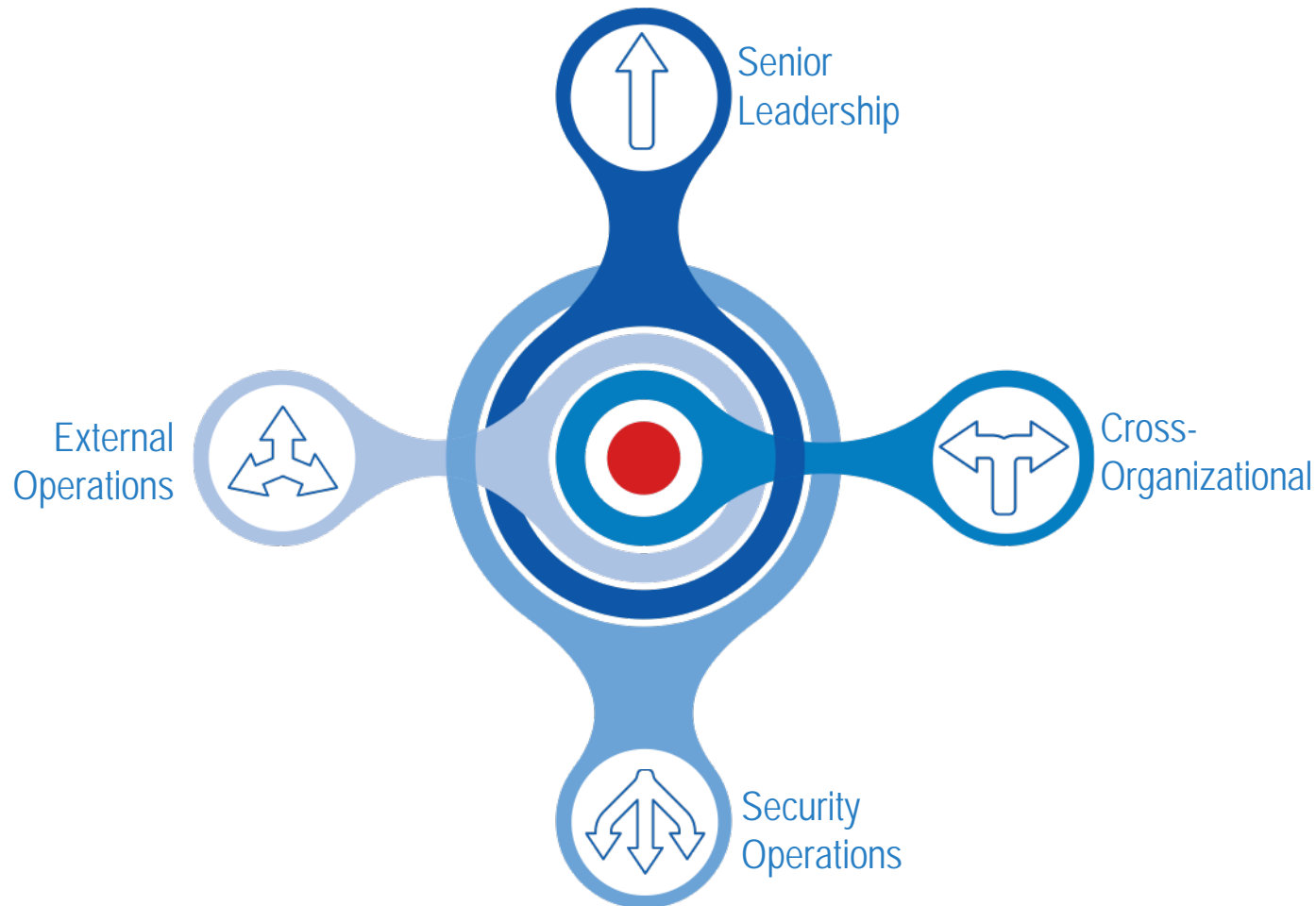


*ISACA Denver  
October Chapter Meeting*

Ian Bramson  
Siemens

# RISK IS GOOD

# The CISO dilemma: expanding accountability and shrinking control



Most Senior Leadership are very concerned about cyber security, but have little understanding of what it is



Senior Leadership



*High Exposure,  
Low Understanding*

- Cyber fatigue
- Strategic alignment
- Business context
- Executive reporting
- Risk reduction

**85%** of board executives feel security information is too technical  
*-- Osterman*

**39%** organizations failed to report Ransomware attacks to CEO or Board  
*-- SentinelOne*

**35X** cyber security budgets have increased 35 times over the last thirteen years  
*-- Cybersecurity Ventures*

**70%** of the value of publicly traded companies are "intangible assets"  
*-- Commission on the Theft of American Intellectual Property*

# Cyber security attackers exploit traditional organizational stovepipes and organizational divisions



Cross-Organizational



*Managing Other Executives*

- The people problem
- Span of control and accountability
- Business enabler, not inhibitor
- Partnership with business
- Cyber security and IT

**95%** of all security incidents involve human error

-- IBM

**65%** of those who carry confidential information don't protect it

-- Ponemon

**63%** of confirmed data breaches involve weak, default or stolen passwords

-- Verizon

**60%** of fired employees steal important corporate data

-- Global HR

# CISOs are struggling to address expanding cyber threats with severe talent shortages



## Security Operations



*Doing More with Less*

- Talent shortage
- Operational reporting and metrics
- Business impacts of technical operations
- Career paths

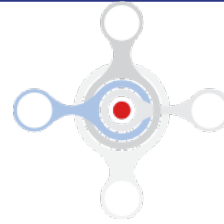
**3.5 Million** unfilled cybersecurity jobs by 2020  
*-- Cybersecurity Ventures*

**52%** of organizations that suffered successful cyber attacks aren't making changes to their security  
*-- Barkly*

**37%** of organizations say that the ability of the security staff to keep up with the threat landscape is inadequate  
*-- ESG*

**41%** of workers will be temps, contractors or consultants by 2018  
*-- CyberArk*

CISOs inherit the risks posed by their external partners, suppliers, and customers



External Operations



*Managing Risks from the Outside*

- Elastic attack surface
- Supply chain cyber challenges
- Vendorpalooza and vendor leverage
- Compliance conundrum
- Cyber insurance

**90%** of organizations lack full confidence in their IoT security

-- AT&T

**\$120 Billion** cyber security market in 2017 (it was \$3.5 Billion in 2004)

-- Wired

**50X** increase in data volume by 2020

-- Microsoft

**88%** of organizations lack full confidence in the security of their business partners' connected devices

-- AT&T

# MANAGING RISK IS GOOD