RSA Conference 2015
San Francisco | April 20-24 | Moscone Center

CHANGE
Challenge today's security thinking

SESSION ID: CXO-W04

Don't Get Left in the Dust:
How to Evolve from CISO to CIRO

James Christiansen
VP – Information Risk Management
Accuvant
jchristiansen@accuvant.com

Bradley J. Schaufenbuel, CISSP
Director of Information Security
Midland States Bank
bschaufenbuel@midlandsb.com

Agenda

- The Evolution of the Role
- Drivers of CIRO Emergence
- What Makes the CIRO Different
- Making the Transition
- How to Apply
- Summary

Introduction

- The security landscape is changing.
- There is a disconnect between the objectives of the traditional CISO and the businesses they serve.
- It is time to evolve with the organizations we serve.

The Six Forces Require a Resilient Security Strategy

Progression of this Field…

1990-1998
IT Security

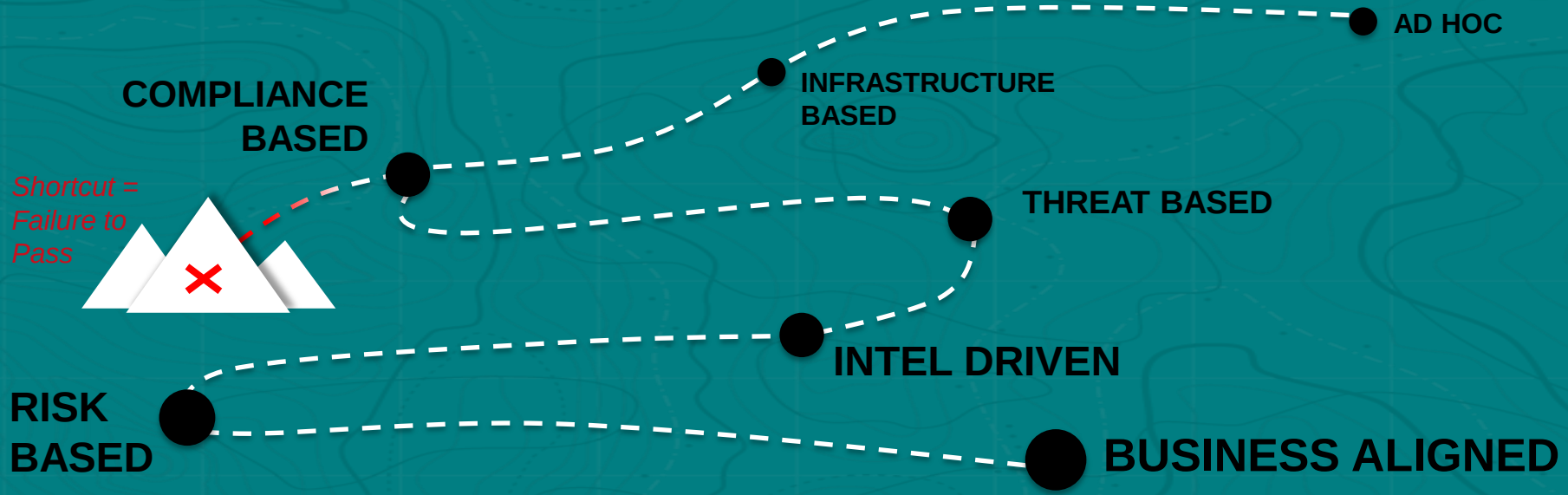
1999-2004
Info Sec

2005-2014
IT Risk Management

2015-???
Information Risk Management?

The Security Journey

A business aligned strategy includes understanding the business and compliance objectives, threats, and risks



Executive Management / Board – NACD

Guidance from the National Association of Corporate Directors (NACD)

PRINCIPLE 1: Cybersecurity is an enterprise-wide risk management issue, not just an IT issue

PRINCIPLE 2: Understand Legal implications of cyber

PRINCIPLE 3: Have regular updates and access to cyber security experts

PRINCIPLE 4: Establish an enterprise-wide cyber-risk management framework with adequate staffing and budget

PRINCIPLE 5: Discussion of which risks to avoid, accept, mitigate, or transfer through cyber insurance

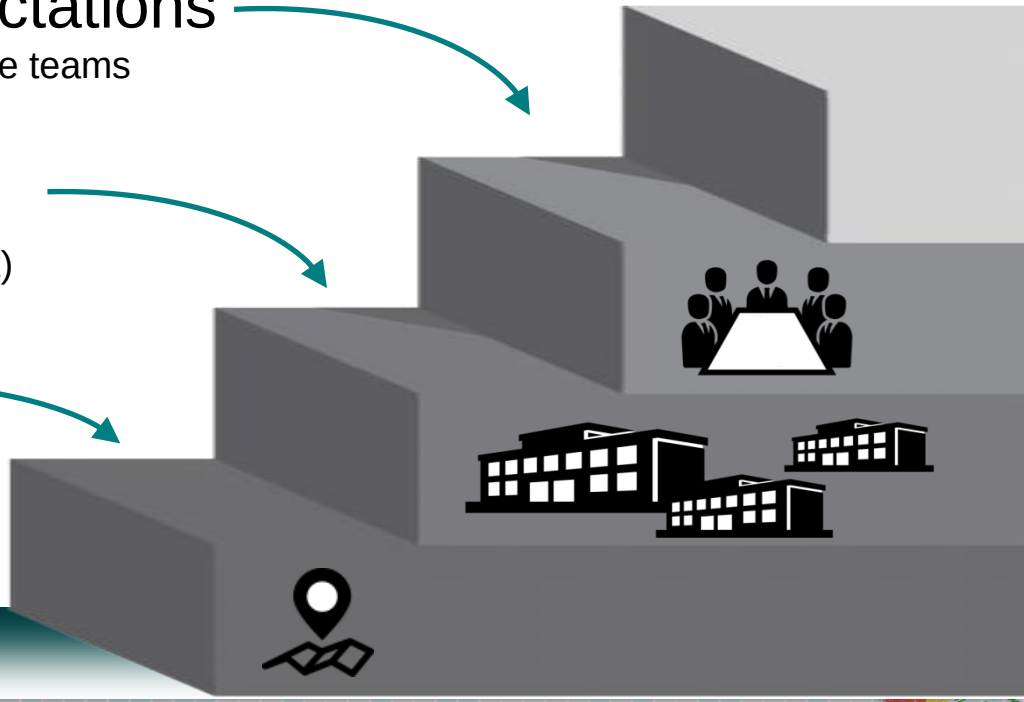
- ***Guidance includes specific questions about program maturity, breach notification, situational awareness, strategy and incident response***

Drivers of the Emergence of the CIRO – 1/2

Greater expectations
of boards and executive teams

Increase in outsourcing
(greater emphasis on third party oversight)

Changing threat landscape
(need for risk based remediation)

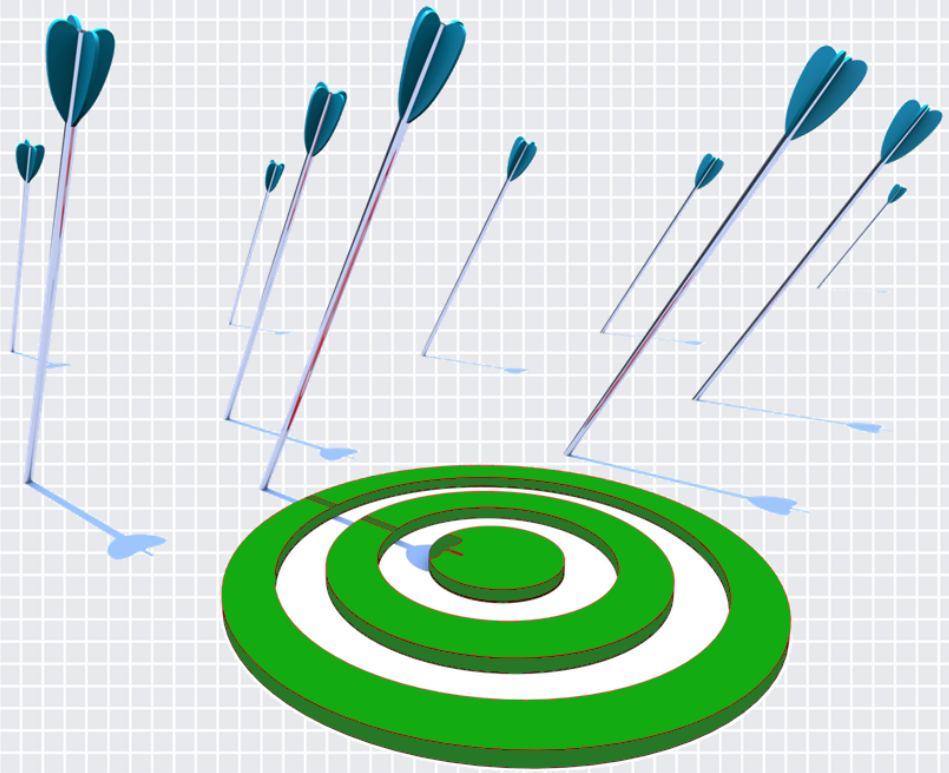


Drivers of the Emergence of the CIRO – 2/2

- Misalignment of security spending with business risk
- Lack of support for taking calculated risks
- Divergence amongst existing information governance functions

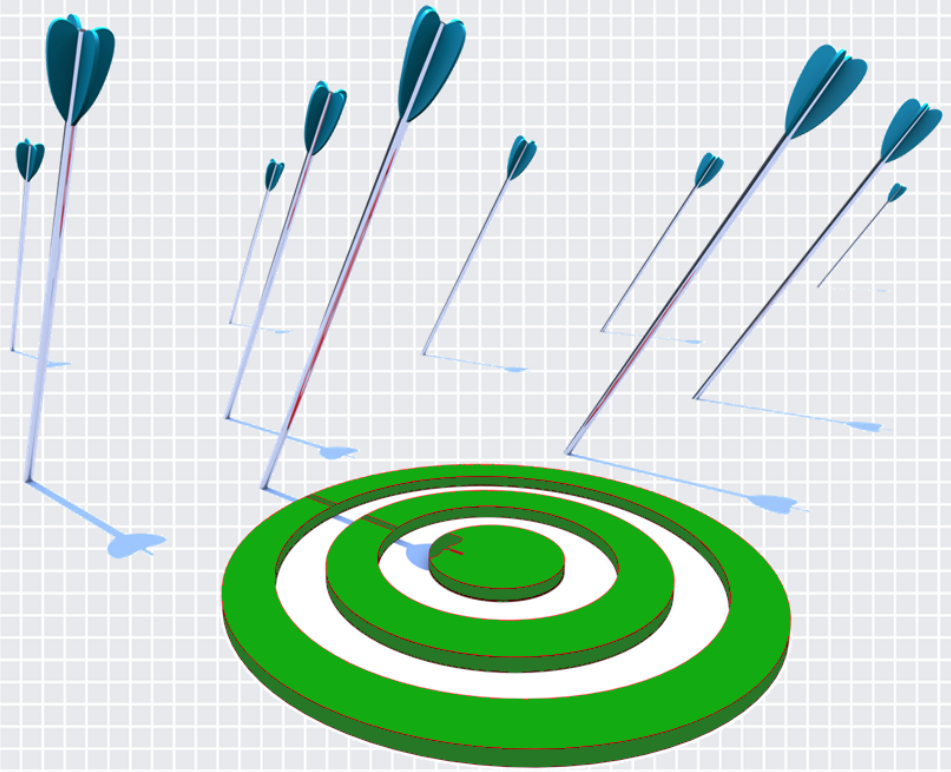
Where CISOs Fall Short – 1/2

- Focus on information protection at the expense of other corporate goals. Information risk is a business problem with a shared budget responsibility
- Focus on technology solutions in lieu of other controls (continual search for the next silver bullet)



Where CISOs Fall Short – 2/2

- Emphasize risk elimination instead of risk optimization (‘no’ instead of ‘yes – if we …’)
- Even “risk enlightened” leaders are fixated on technology risks (focus on ‘IT’ risk instead of ‘information’ risk)



The Ideal CIRO

- Traditional security knowledge (CISSP, CISM, etc.)
- Business savvy (MBA)
- Thinks like a lawyer and a hacker
- Leader (comfortable in front of the board)
- Understands risk management principles
- Can implement project management fundamentals

The Successful Chief Information Risk Officer

Information Security is a Business Imperative

- Enable Business to Securely Deliver Product and Services
- Positive Interaction With Partners, Third-parties and Regulators

Information Driven Decision Making

- Strategic and Operational Metrics / Dashboard
- Information Risk Assessment and Management
- Integration with Enterprise Risk Management

Shared Budget Responsibility

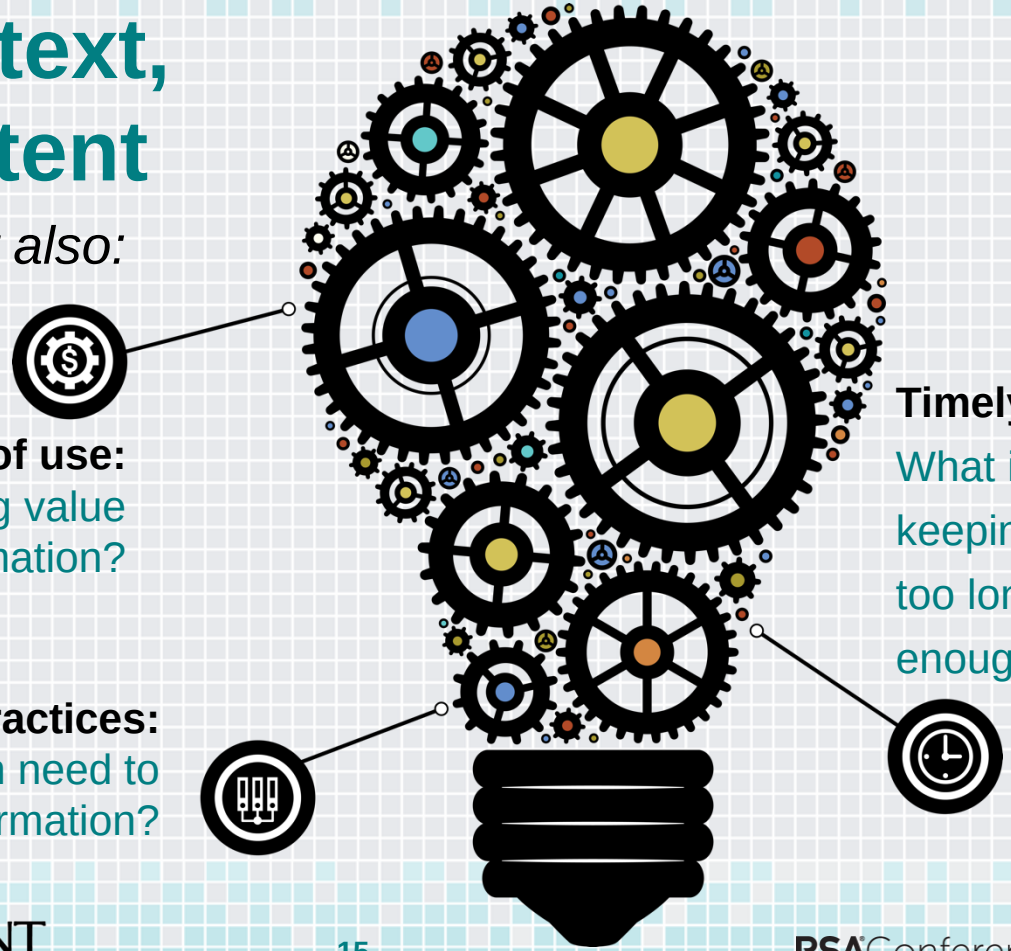
- Corporate and Business Unit - Balanced Risk and Cost
- Prioritization With Other Strategic Business Projects

What Makes the CIRO Different?

- Organizational profile – Executive team member with board access
- Organizational alignment – Strategy dovetails with organization's
- Depth and breadth of skills
- Business risk based approach
- Leadership

Not Just Context, but Also Content

Not just protection, but also:



Optimization of use:
Are we extracting value from information?

Collection practices:
Do we even need to obtain the information?

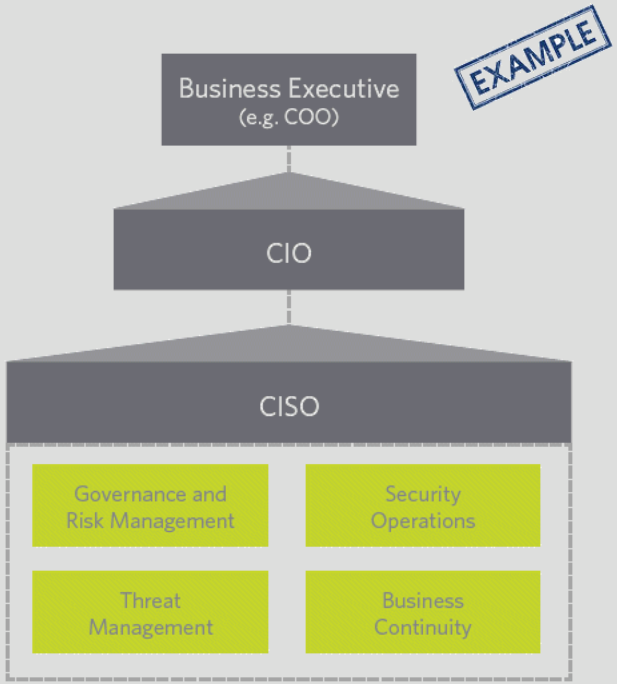
Timely destruction:
What is the risk of keeping information too long or not long enough?

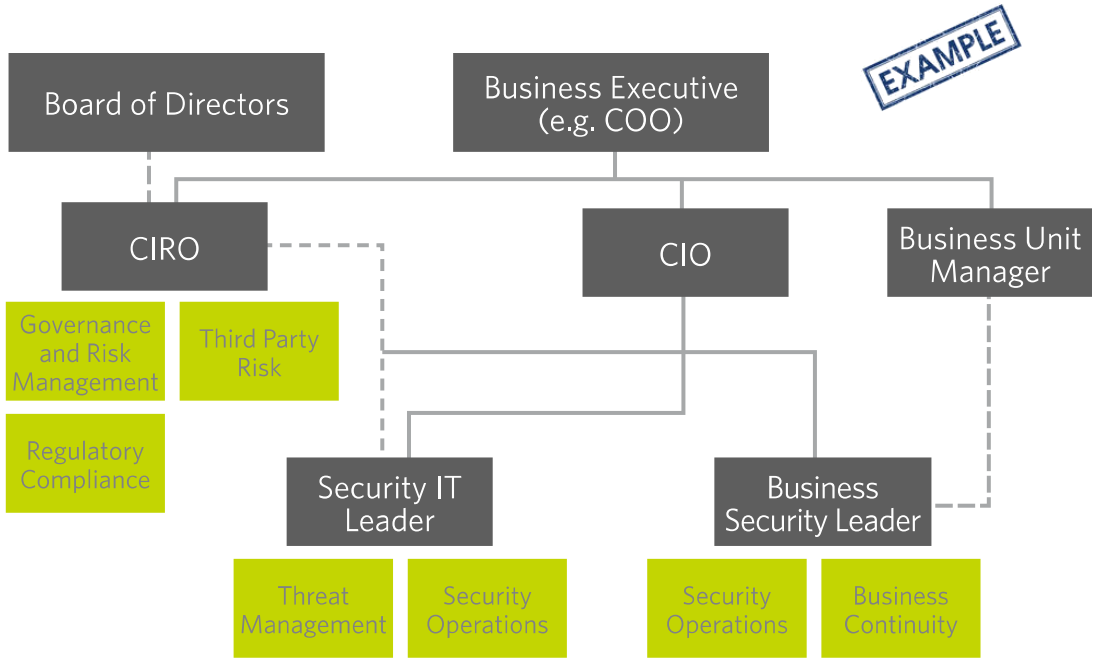
What Functions Fall Under CIRO?

May include parts of:

- Traditional Information Security
- Legal and Regulatory Compliance
- Privacy
- Third Party Oversight
- Business Resilience
- Physical Security

Reporting Structures, Old and New





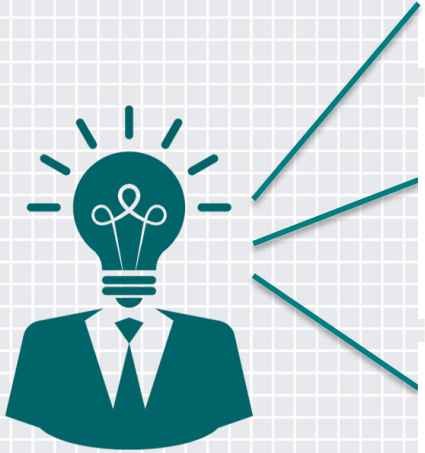
Advantages of New Organizational Structure

- ✓ Aligns information risk with business priorities
- ✓ Visibility into organizational or product changes
- ✓ Supports shared responsibility for information risk
- ✓ Ensures that all types of information risk are addressed
- ✓ Able to address board, executive management and customers

Do We Need Another C-Level Position?

- Value of information (and associated risk) rising.
- Executive composition should parallel board's fiduciary duties.
- Consolidation of existing C-level positions (CPO, CISO / CSO, etc.)

Skills Required to Make the CIRO Transition



Thorough understanding of risk management concepts

- Factor Analysis of Information Risk (FAIR)[1]

Thorough understanding of your organization's business, objectives and growth plans

- Regular meetings with business executives

Executive level communication skills

- Presentation Skills – Toastmasters
- Written Skills – College & Editors / Colleagues

[1]Source: Risk Management Insight (riskmanagementinsight.com)

The Information Risk Transformation

- Transition yourself from law enforcement / military mindset to that of a business risk manager

- Add risk management skill set to staff (through training or hiring)

- Don’t forget about information in non-electronic format

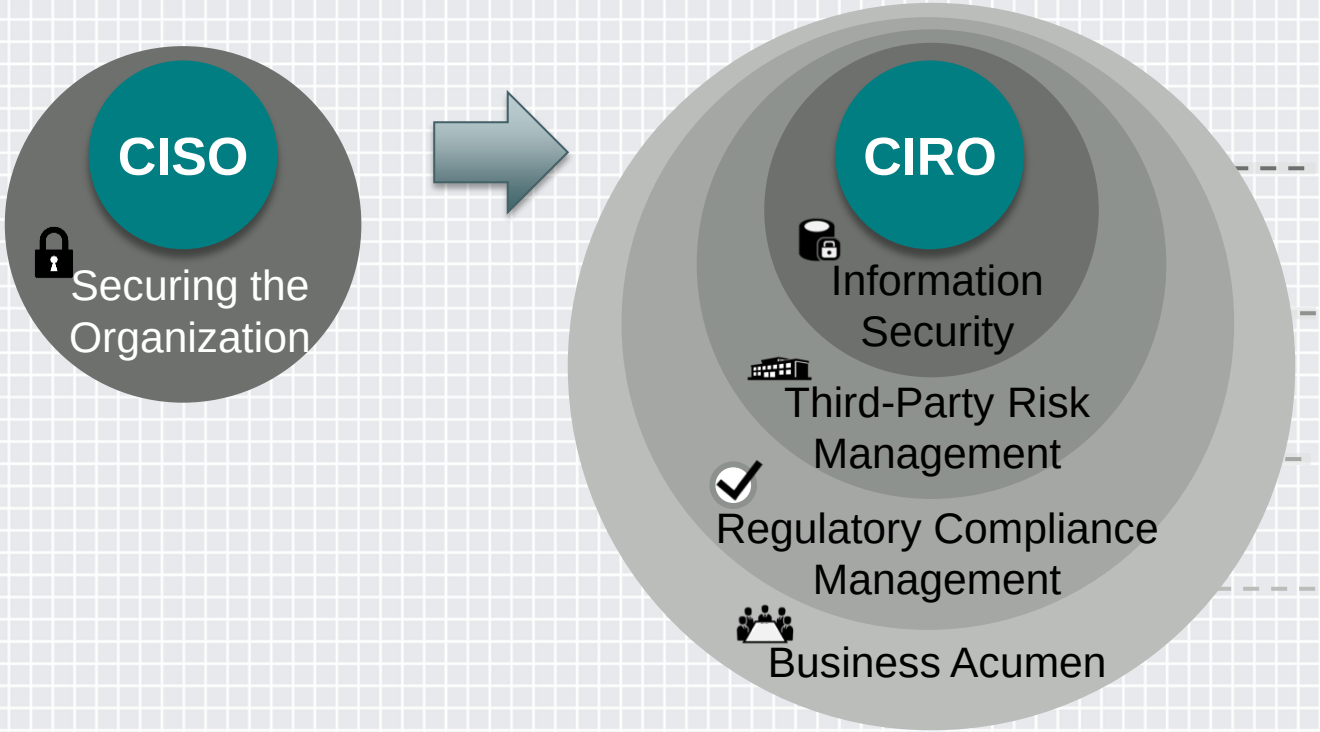
How?

- **Understanding Regulations:**
  - Translate legal regulations to internal activities to meet spirit (legislative intent) and letter of the law. Establish a good working relationship with your attorneys. Participate in standard setting and regulatory rulemaking processes (i.e., help shape the rules).

- **Threat Landscape:** Implement threat analytics maturity model

- **Understand the corporate culture:** Risk aversion, rate of change, cultural differences, countries of operation

Evolution of the CISO to the CIRO



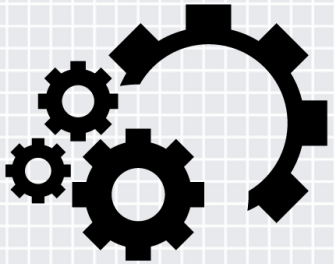
Executive Management / Board – Tips

- Keep it short and concise – Typically they will want pre-materials
- Never guess at an answer – They read people very well!
- Information Risk Dashboard
  - Include areas of risk inside and outside the organization
  - Trends – What areas of risk are increasing and decreasing
  - New risk highlights
  - Overall goal – Demonstrate the effectiveness of your information risk management program over time.

Capability	Key Risks	Risk Level	# Regulatory Findings	Regulatory Finding(s)	Trend
Information Security Program Management	The information security program is not aligned with business requirements	L	1	4	↑
	Policies and procedures have not been established for information security	H	6	4	↓

Source: NACD, Cyber-Risk Oversight, Directors Handbook 2014

Using Existing Enterprise Risk Management (ERM) Program (or Create One)



- Leverage the existing enterprise risk management (ERM) program (if one exists).
- Information risk is a subset of enterprise risk.
- If there isn't an enterprise risk management program, sponsor one (position yourself to be CRO).

Leveraging Information Risk to Drive Value

Concrete Examples:

- Factoring in an information risk discount on an acquisition valuation / purchase price
- Leveraging fraud and security data to improve customer experience

Contributing to the Organization's Success

- Revenue Contribution
  - Enable Business Efficiency
  - Product Delivery
  - Brand Name Confidence
- Earnings Contribution
  - Reduced Operating Expenses Related to Security Failure
  - Long Term Reduction of Security Program Costs
  - Circumvent Costs of Regulatory Non-compliance

Managing Information Risk

Information Risk Management

Information Security | Regulatory Compliance | Third Party Risk

People

Process Improvement

Information Technology

Enhanced Security

Governance

Global Execution

Effective Compliance

Regulations

Ease of Doing Business

Third Parties

The Reward

- Earned respect from organizational peers
- Inclusion in your organization's strategic decision making processes and forums
- Perception shifts from marginal cost center to value adding unit

Midland States Bank

ACCUVANT

Summary

We have established:

- The current CISO role is not meeting organizational needs
- CISO must adapt or go the way of the Dodo bird
- A focus on managing information risk offers a superior alignment to the organization's objectives
- There are steps you can take to position yourself for this transition

Apply It

- Immediate actions: Assess you and your program's readiness to make the CIRO transition

- Establish **YOUR** plan to gain and implement necessary skills

- Take steps to realign skill sets, focus, and organizational structure to an information risk based approach

Resources

- The Evolution of the CISO (accuvant.com/resources/risk-and-the-ciso-role#sthash.TUMIWWV7.dpuf)
- NACD – Cyber-Risk Oversight Handbook (nacdonline.org/cyber)
- Introduction to Factor Analysis of Information Risk (FAIR) (riskmanagementinsight.com)
- Six Forces of Security Strategy (accuvant.com/resources/accuvants-six-forces-of-security-strategy)

Questions?

jchristiansen@accuvant.com

bschaufenbuel@midlandsb.com