RSAConference2016

San Francisco | February 29 – March 4 | Moscone Center

Connect to Protect

SESSION ID: PROF-M07

Cave Man to Business Man, the Evolution of the CISO to CIRO

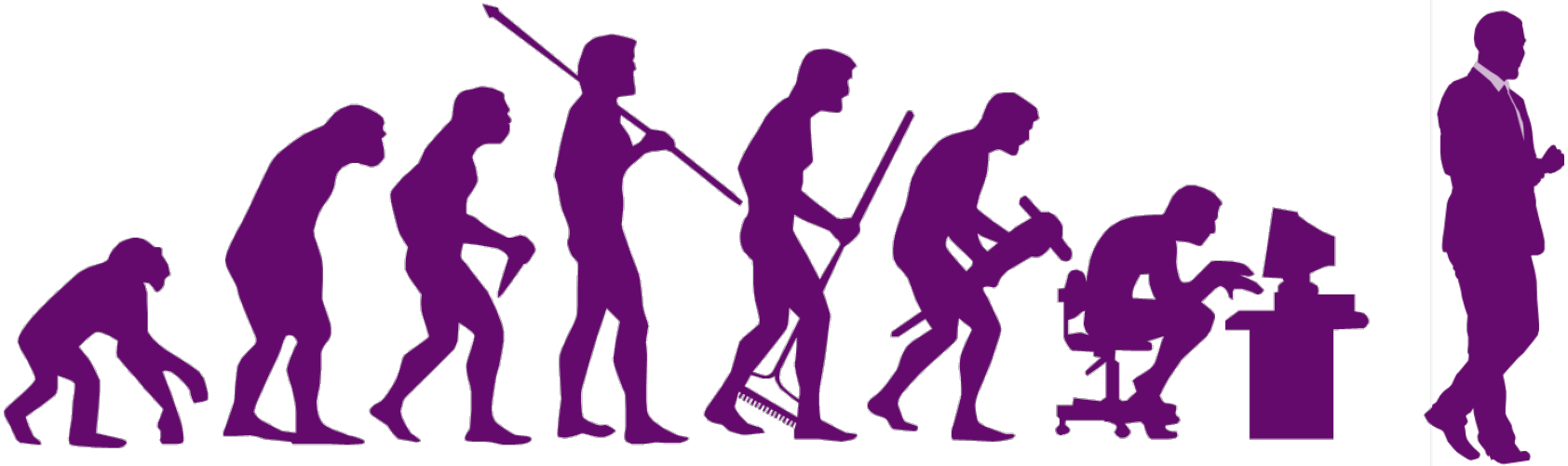
James Christiansen

VP Information Risk Management

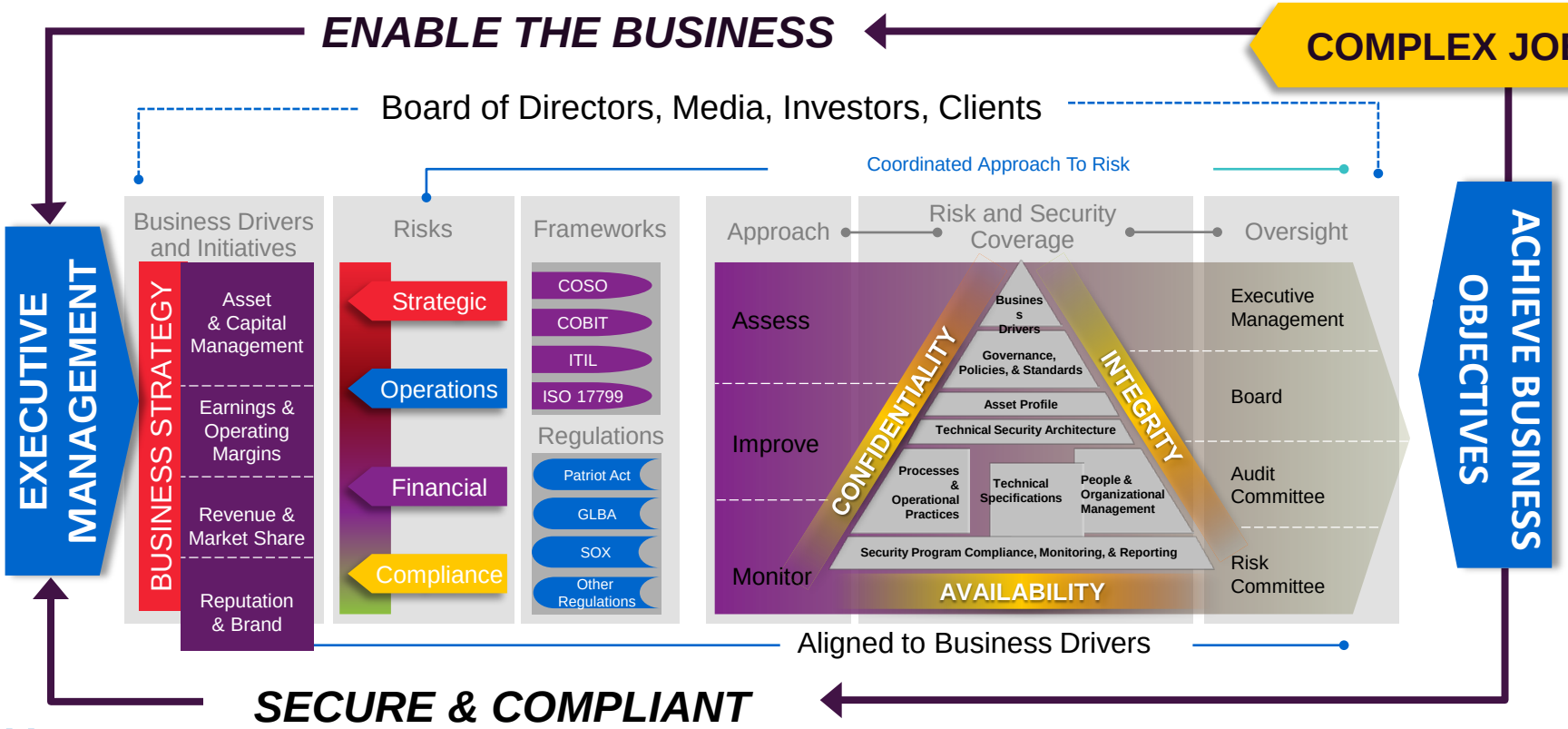
Optiv

#RSAC

The Evolution of the CISO



The Expanded Role of the CISO



Agenda

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

Introduction

- The role of information security is changing
- There is a disconnect between the objectives of the traditional CISO and the needs today
- The role of the CISO needs to change to meet the business needs

Common Complaints about the CISO

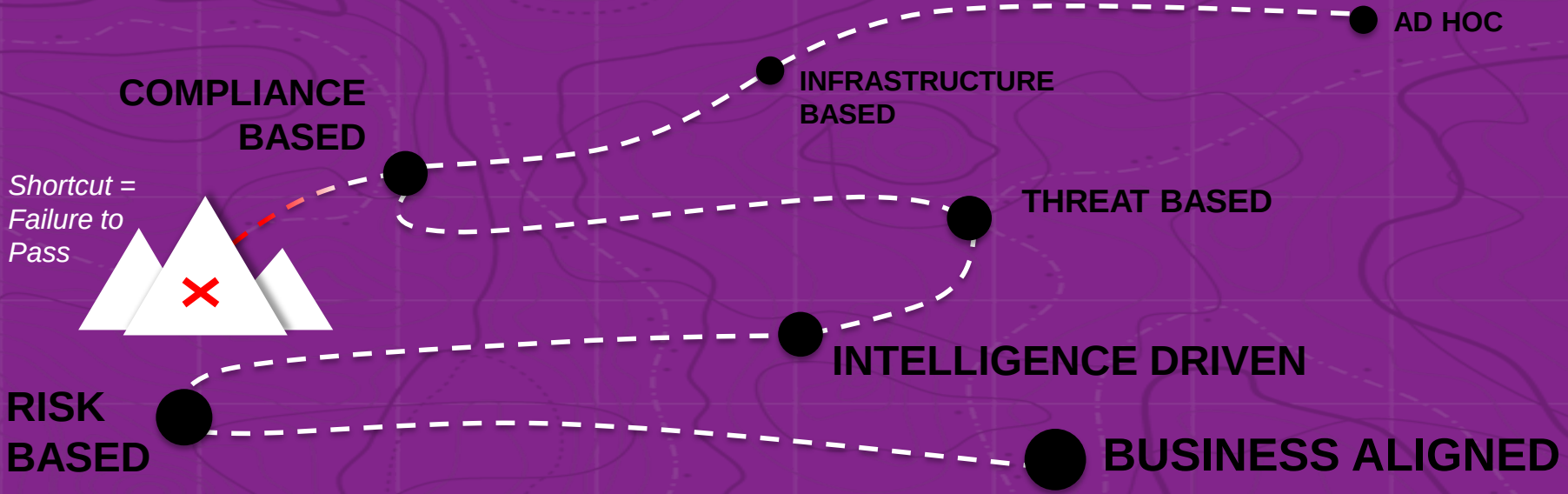
- Doesn't positively engage with the business
- Security strategy and spending does not align with the business strategy
- Focus on information protection at the expense of other corporate goals
- Roadblock to innovation and revenue growth
- Can articulate value to the business

We are going to change the perception of the executive team!

The Basics of the CIRO

The Security Journey

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

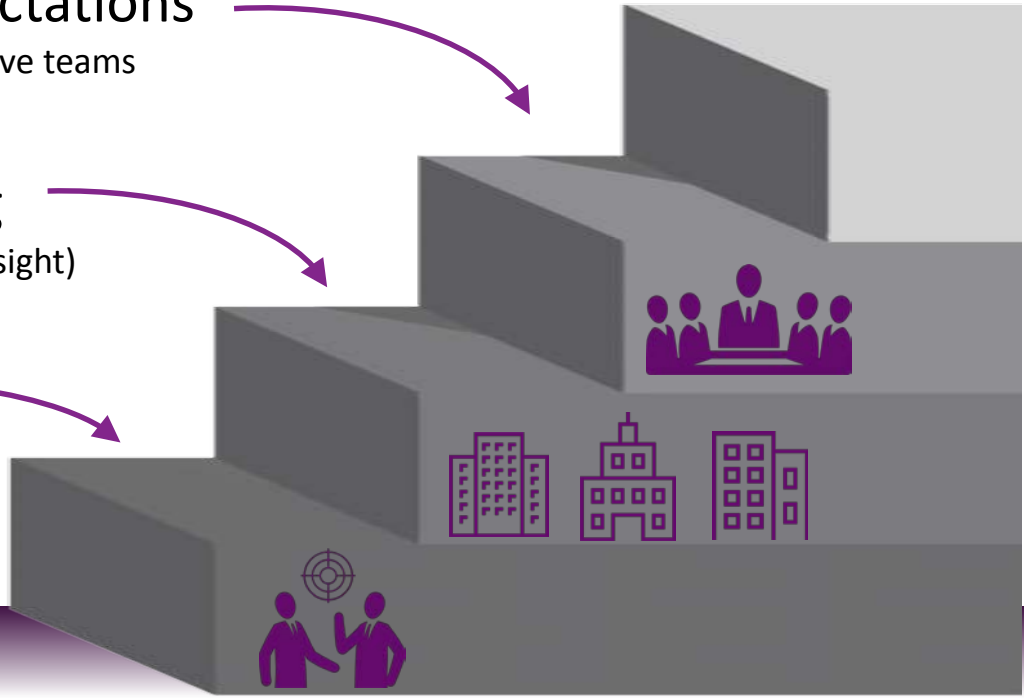


Drivers of the Emergence of the CIRO

Greater expectations
of boards and executive teams

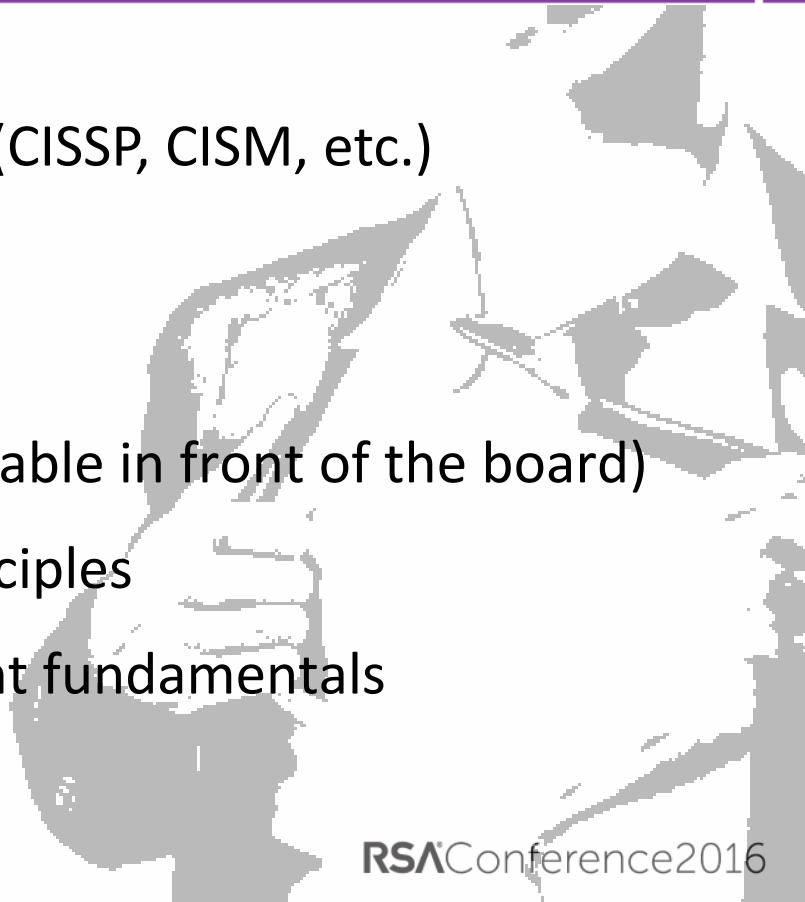
Increase in outsourcing
(greater emphasis on third party oversight)

Changing threat landscape
(need for risk based remediation)



Skills of the CIRO

- Has traditional security knowledge (CISSP, CISM, etc.)
- Exhibits business savviness (MBA)
- Thinks like a lawyer and a hacker
- Possesses leadership skills (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

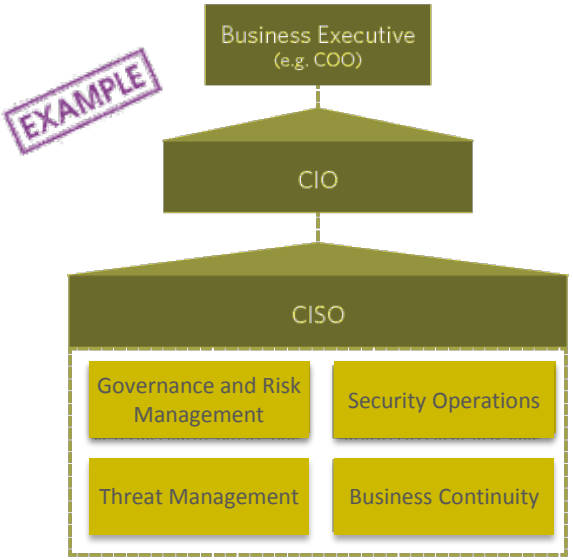
Information Risk Program

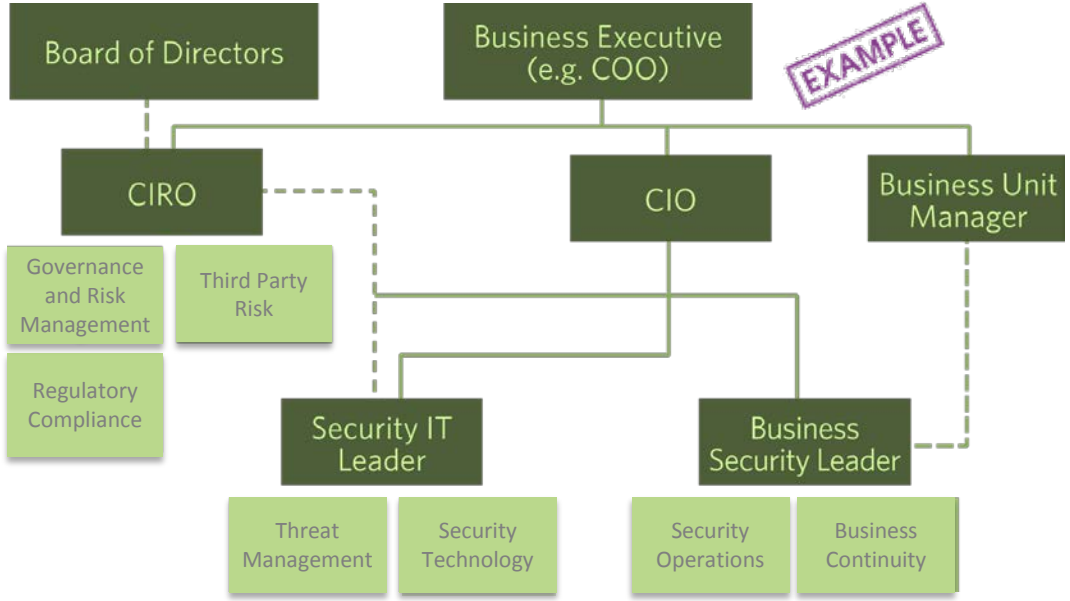
Three Lines of Defense to Achieve Effective Information Risk Management

1st Line of Defense IT Information Security	2nd Line of Defense Information Risk Office	3rd Line of Defense Audit and External
• Highly Skilled and Trained Staff • Processes to Protect, Detect and Respond • Implement Enabling Security Technologies	• Define and Enforce Information Security Policy • Program Strategy and Goals • Measure and Manage Information Risk • Oversee Industry and Regulatory Requirements	• Board of Directors Oversight • Internal and External Audit Validation • External Testing and Validation of Controls

OPTIV

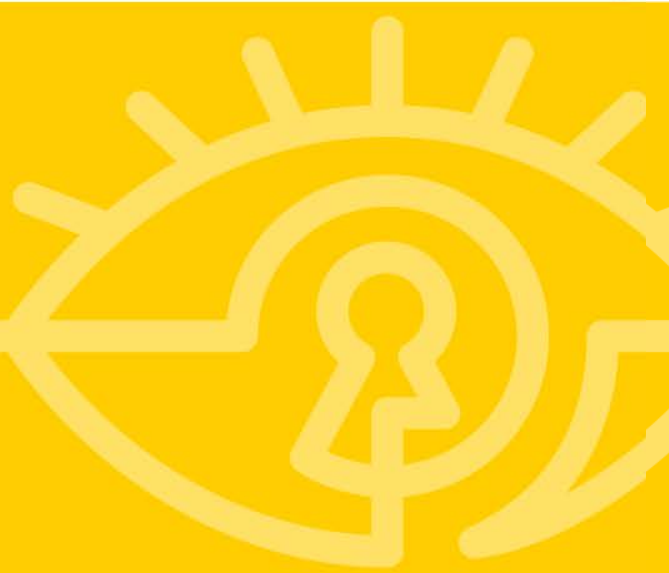
Reporting Structures, Old and New





Advantages of New Organizational Structure

- ✓ Aligns information risk with business priorities
- ✓ Visibility into organizational or product changes
- ✓ Supports shared responsibility for information risk
- ✓ Focus on risk of information regardless of location or form
- ✓ Able to address board, executive management and customers



The Skills of the CIRO

Skills Required to Make the CIRO Transition

Thorough understanding of risk management concepts

- e.g. 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 and Editors / Colleagues

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

How?

Know the Regulations:

- Establish a good working relationship with your attorneys
- Participate in standard setting and regulatory rulemaking processes (i.e., help shape the rules)
- Understand the privacy laws impacting your organization

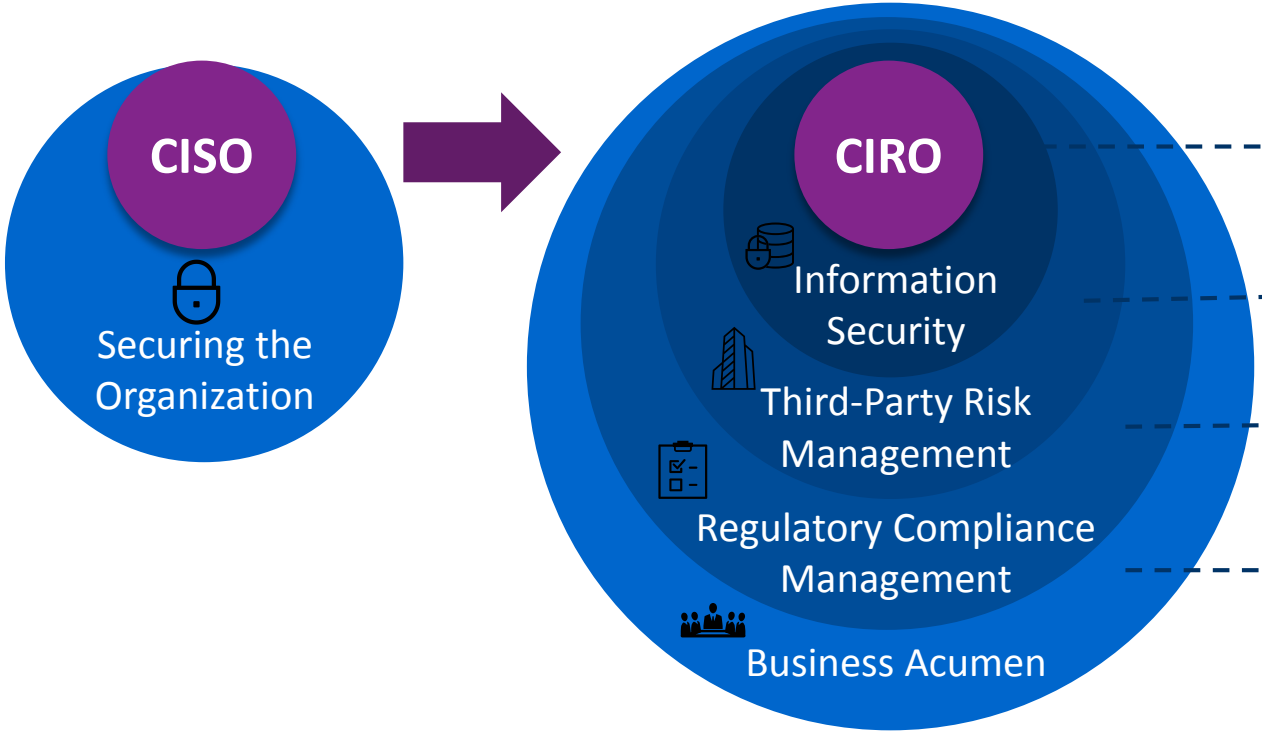
Determine Threat Landscape:

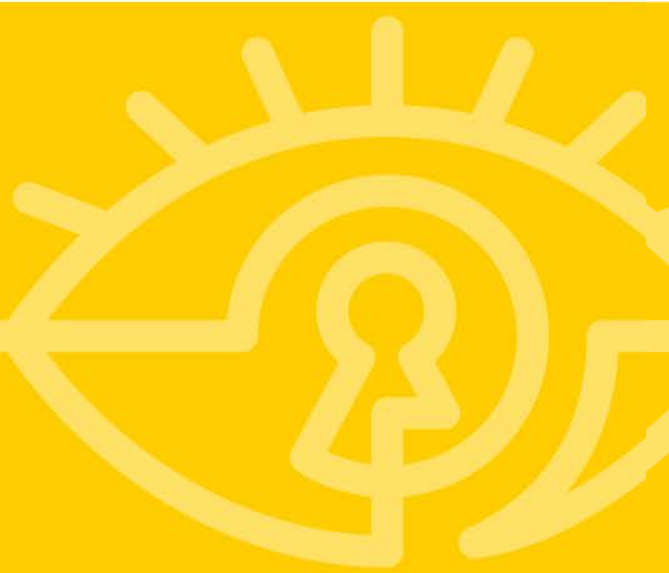
- Implement a threat analytics maturity model

Understand the Corporate Culture:

- Determine the risk aversion, rate of change, cultural differences and countries of operation

Evolution of the CISO to the CIRO





Speaking to the Board of Directors

Executive Management / Board – NACD

Guidance from the National Association of Corporate Directors (NACD)

PRINCIPLE 1:
Cyber security is an enterprise risk management issue, not just an IT issue

PRINCIPLE 2:
Understand legal implications of cyber risks

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

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

PRINCIPLE 5:
Discuss 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

OPTIV

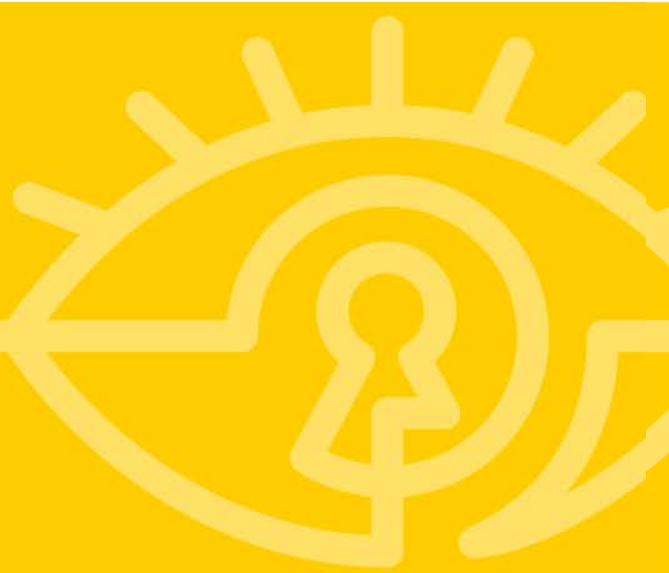
Source: nacdonline.org/cyber

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 risk inside and outside the organization
  - **New** risk highlights
  - **Trends** – What areas of risk are increasing and decreasing
  - **Overall goal** – Demonstrate the effectiveness of your information risk management program over time

Capability	Key Risks	Risk Level	IA/ 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



Driving Value Into Enterprise

Leveraging Information Risk to Drive Value

Concrete Examples:

- Enabling a new customer product through advanced security practices and knowledge of the privacy protection requirements
- 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

Summary

- The current CISO role is not meeting organizational needs
- CISO must adapt or will be replaced by person with needed skills
- 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 (Optiv.com/Resource Library)
- NACD – Cyber-Risk Oversight Handbook (nacdonline.org/cyber)
- Introduction to Factor Analysis of Information Risk (FAIR) (riskmanagementinsight.com)
- Six Forces of Security Strategy (Optiv.com/Resource Library)

Questions?

James.Christiansen@optiv.com