RSA Conference2015

San Francisco | April 20-24 | Moscone Center

SESSION ID: CXO-W04

#### CHANGE

Challenge today's security thinking

#### **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

**ACCUVANT** 

- What Makes the CIRO Different
- Making the Transition
- How to Apply
- Summary

Midland 🔳





## Introduction

- The security landscape is changing.
- There is a disconnect between the objectives of the traditional CISO and the businesses they serve.

ACCUVANT

 It is time to evolve with the organizations we serve.

Midland



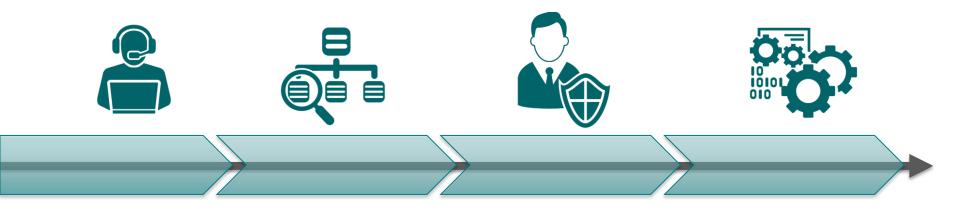
## The Six Forces Require a Resilient Security Strategy

ACCUVANT

Midland



#### **Progression of this Field...**



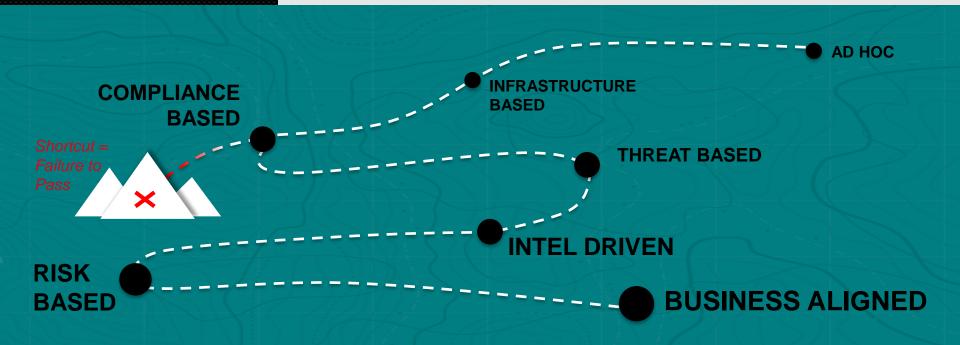
**#RSAC** 

1990-19981999-20042005-20142015-???IT SecurityInfo SecIT Risk ManagementInformation Risk<br/>Management?



# The Security Journey

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





JC-JC

**RSA**Conference2015

6

#### **Executive Management / Board – NACD**

Guidance from the National Association of Corporate Directors (NACD)



PRINCIPLE 1: Cybersecurity is an enterprisewide risk management issue, not just an IT issue

Midland

JC-BS



**PRINCIPLE 2:** Understand Legal implications of cyber

ACCUVANT



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



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

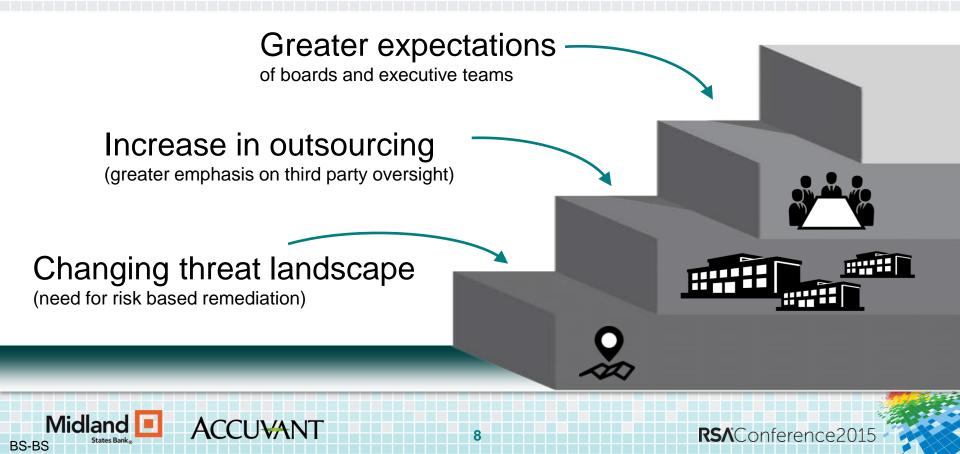


**PRINCIPLE 5:** Discussion of which risks to avoid, accept, mitigate, or transfer through cyber insurance

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



#### **Drivers of the Emergence of the CIRO – 1/2**



# 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



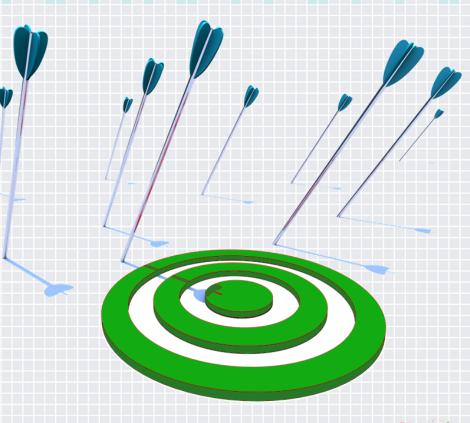
RSA

BS-BS

#### #RSAC

## 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)

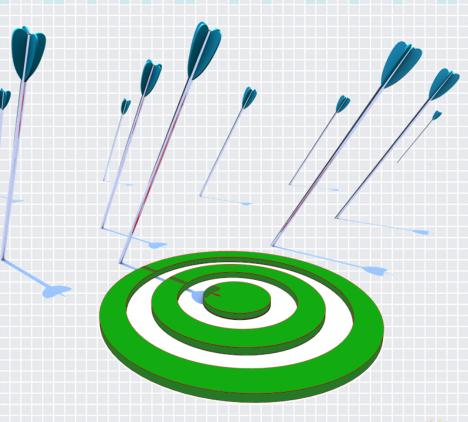






### Where CISOs Fall Short – 2/2

- 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)





**RSA**Conference2015

#### **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

ACCUVANT

CIRO

Midland

JC-JC

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

RSAConference2015

#### 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

Midland



### Not Just Context, but Also Content

Not just protection, but also:

Midland

JC-JC



Optimization of use: Are we extracting value from information?

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

**ACCUVANT** 



15

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

#RSAC

enough?



RSAConference2015

#### What Functions Fall Under CIRO?

16

#### May include parts of:

- Traditional Information Security
- Legal and Regulatory Compliance

**ACCUVANT** 

Privacy

Midland

JC-JC

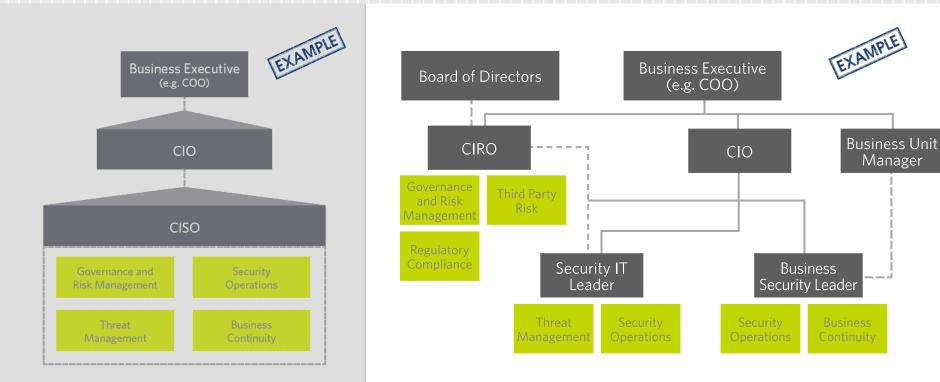
- Third Party Oversight
- Business Resilience
- Physical Security



RSAConference2015

#RSAC

## **Reporting Structures, Old and New**



Midland ACCUVANT

**RSA**Conference2015

#RSAC

17

### Advantages of New Organizational Structure

**ACCUVANT** 

✓ 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?**



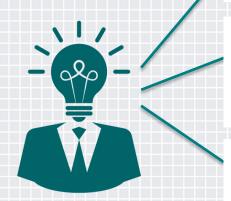
 Value of information (and associated risk) rising.

 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)<sup>1</sup>

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

Midland ACCUVANT

<sup>1</sup>Source: Risk Management Insight (riskmanagementinsight.com)

#### **The Information Risk Transformation**



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

**ACCUVANT** 

Midland

BS-BS



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

 Don't forget about information in nonelectronic format

**RSA**Conference2015



#### 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

**RSA**Conference201



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



## **Evolution of the CISO to the CIRO**

Securing the Organization

**ACCUVANT** 

Midland

JC-JC

CISO

**CIRO** R Information Security -----**Third-Party Risk** Management **Regulatory Compliance** Management \*\*\* **B**usiness Acumen

Secure the internal organization

#RSAC

Manage the risk of third parties

Manage regulatory risks

Communicate
 current status and
 risks to board

#### **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

Midland

JC-BS

 Overall goal – Demonstrate the effectiveness of your information risk management program over time.

ACCUVANT

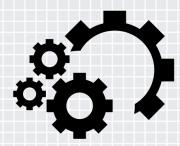
	Capability	Key Risks	Risk Laval	W Regulatory Findings	Regulatory Finding(s)	Trend
_	Information Security	The information security program is not aligned with business requirements	L	1	4	1
_	Program Management	Policies and procedures have not been established for information security	н	6	4	Ţ

**RSA**Conference2015

**#RSAC** 

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

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



BS-BS

 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).



**RSA**Conference2015

#RSAC

# 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

ACCUVANT

Earnings Contribution

Midland

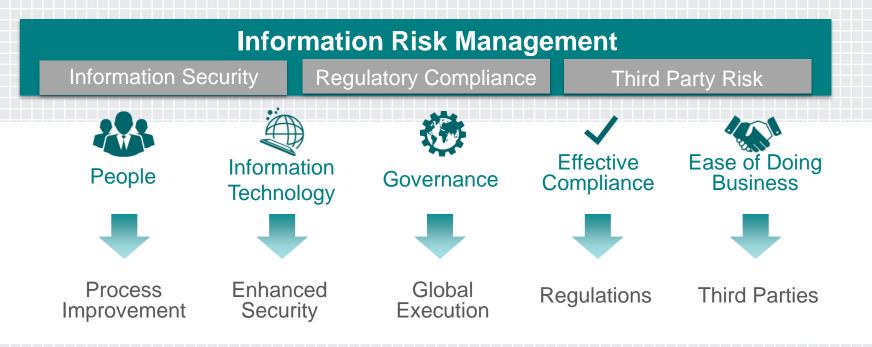
JC-JC



**#RSAC** 

- Reduced Operating Expenses Related to Security Failure
- Long Term Reduction of Security Program Costs
- Circumvent Costs of Regulatory Non-compliance

#### **Managing Information Risk**



**#RSAC** 





# The Reward

CCUVANT

Midland

JC-BS

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

RSAConference2015

29



#### 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

**ACCUVANT** 

Midland

BS-BS



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

RSAConference2015

#### Resources

Midland

BS-BS

- The Evolution of the CISO (accuvant.com/resources/risk-and-the-cisorole#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-sixforces-of-security-strategy)

ACCUVANT



Just as information technology priorities change year after year at most organizations, so should the way we view the security landscape. To best address the constant shifting, organizations must realign and reorganize. Over the past five years the role of the Chief Information Security Officer (CISO) has changed dramatically. Organizations need to observe this role in a whole new different way, while changing the way they view risk. The focus is no longer just on information technology, but also on analyzing and reducing vulnerabilities associated with cyber security risks. Because of this new separation, we must consider changing the way we think about security. At one time, it felt appropriate to combine the risk associated with a company's assets with how we protect those assets. Now, we must focus on managing the risk associated with our data, rather than just how we're protecting it. The question then remains, who is managing this risk and how are you

#### A Change in Responsibility

To focus on who is managing asset risk, we typically look to the Chief Information Security Officer, or CISO, of an organization. This position is typically viewed as a technical role, coming up through the ranks with an IT background and then moving into security. Their main job function has historically been the implementation of security technologies within the organization with an emphasis on the infrastructure and keeping the internal systems secure. As the "5" in CISO implies - the focus was on

Over the past few years, the responsibilities of the CISO have expanded beyond the security of the enterprise. Now, the role must concentrate on managing the risk of the information, regardless of where it resides. Today's CISO has evolved into the Chief Information Risk Officer (CIRO), with a growing list of ponsibilities - including all or some of the below, depending on the industry and company demographics.

#### Information Risk Management

A CIRO needs to understand all aspects of threats to the organization's information and business operations. The security strategy should be focused on enabling the business and imizing the risk to the information

ACCUVANT



# **Questions?**



jchristiansen@accuvant.com

bschaufenbuel@midlandsb.com

Midland ACCUVANT

**RSA**Conference2015

33