RSA CONFERENCE 2014

FEBRUARY 24 – 28 | MOSCONE CENTER | SAN FRANCISCO

Share.
Learn.
Secure.

Capitalizing on
Collective Intelligence

# Making Audits Work For You

SESSION ID: SEM-M02

Justin Peavey

CISO, Omgeo LLC

# Why Audit?

# What is Internal Auditing (IA) ?

- *Internal Auditing is an independent, objective assurance and consulting activity designed to add value and improve an organization's operations. It helps an organization accomplish its objectives by bringing a systematic, disciplined approach to evaluate and improve the effectiveness of risk management, control, and governance processes.*
- The IA activity evaluates risk exposure relating to the organization’s governance, operations and information systems in relation to:
  - Effectiveness and efficiency of operations
  - Reliability and integrity of financial and operational practices
  - Safeguarding of assets
  - Compliance with policies, standards, laws, regulations and contracts

*Source: The Institute of Internal Auditors (http://www.theiia.org)*

# What is Regulation?

- Regulation is “controlling human or societal behavior by rules or restrictions”[1]
  - Regulation attempts to produce outcomes or prevent outcomes which otherwise might not occur in the desired manner.
- Schneier on Regulation[2]: “[it] is all about economics”
  - In a capitalist system, companies make decisions on their own self interest.  Normally this is a good thing, but some effects of the decisions, *externalities*, are not borne by the companies.
  - Regulation and Liability force the *externalities* to be part of the self-interest of the company and become included factors in the decision making.

[1] Bert-Jaap Koops et al. Starting Points for ICT Regulations, Deconstructing Prevalent Policy One-liners, Cambridge University Press, Cambridge: 2006, p. 81

[2] Bruce Schneier.  Do Federal Security Regulations Help?.

# Principle-based vs. Rules-based Regulation

- Principle-based vs. Rules-based Regulation
  - Principle-based is less proscriptive and generally weathers time better.  It also generally leaves more room for interpretation by both you and the regulators.
  - Rules-based is more proscriptive and therefore generally more straightforward to ‘pass’, but the rules can quickly be dated as new approaches emerge and the goal of the regulation can easily be lost sight of.
- Key: Regulation is all about achieving a specific set of goals, understand what that goal is – demonstrate to the regulator how your program achieves that goal.

# Preparing for the Audit

# Auditing Standards

- **Generally Accepted Auditing Standards** (GAAS), 10 standards developed by American Institute of Certified Public Accountants (1947). 1-6 address general standard (*paraphrased below*), 7-10 address reporting:

  1. Auditors should have adequate technical training and proficiency as an auditor.
  2. Independence in mental attitude is to be maintained by the auditor
  3. professional care is to be exercised in the planning and performance of the audit and the preparation of the report.
  4. The auditor must adequately plan the work and must properly supervise any assistants
  5. The auditor must understand the entity and its environment, including its internal control, to assess the risk
  6. The auditor must obtain sufficient appropriate audit evidence by performing audit procedures to afford a reasonable basis

# IT Governance Standards

- COBIT
  - Control Objectives for Information and related Technology - ISACA
- ISO 17799/27001
  - Information Security Management Systems Standards
- ITIL
  - IT Infrastructure Library
- PMBOK
  - Project Management Body of Knowledge
- FFIEC IT Handbook
  - Federal Reserve Board, FDIC, National Credit Union, Office of the Comptroller of the Currency, Office of Thrift Supervision

# Preparation

- Review past audit findings.
    - Good auditors will be looking to verify that previously 'corrected' controls are properly functioning.
- Review the focus areas of the audit.
    - Regulatory audits – understand both the goal and the 'rules' within the regulations.
        - Understand what your peers are doing to implement required controls; if your approach is different, be prepared to demonstrate how it is effective.
    - Internal Audits – understand the audit/governance standards that are going to be used and perform your own risk assessment against those standards.
        - In areas that are 'weaker', what is the risk implication? If it is low, prepare to discuss this with the auditor. If it is not low, be prepared to discuss your approach for mitigating the risk.
- Appoint roles for internal staff
    - Audit coordinator: who will be the interface point to the auditors and will manage the requests from the auditors.
    - Reviewers/Approvers for evidence: who will be the second set of eyes/approver for evidence requests. Always require an evidence review before sending the evidence to audit to ensure it is correct and in-scope.

# Audit Walkthrough

# A Typical Audit Process

1. Notification & Request for Preliminary Information
2. Planning
3. Opening Meeting
4. Fieldwork
5. Communication
6. Draft Report
7. Management Responses
8. Closing Meeting
9. Report Distribution
10. Follow-up

# Fieldwork / Audit Techniques

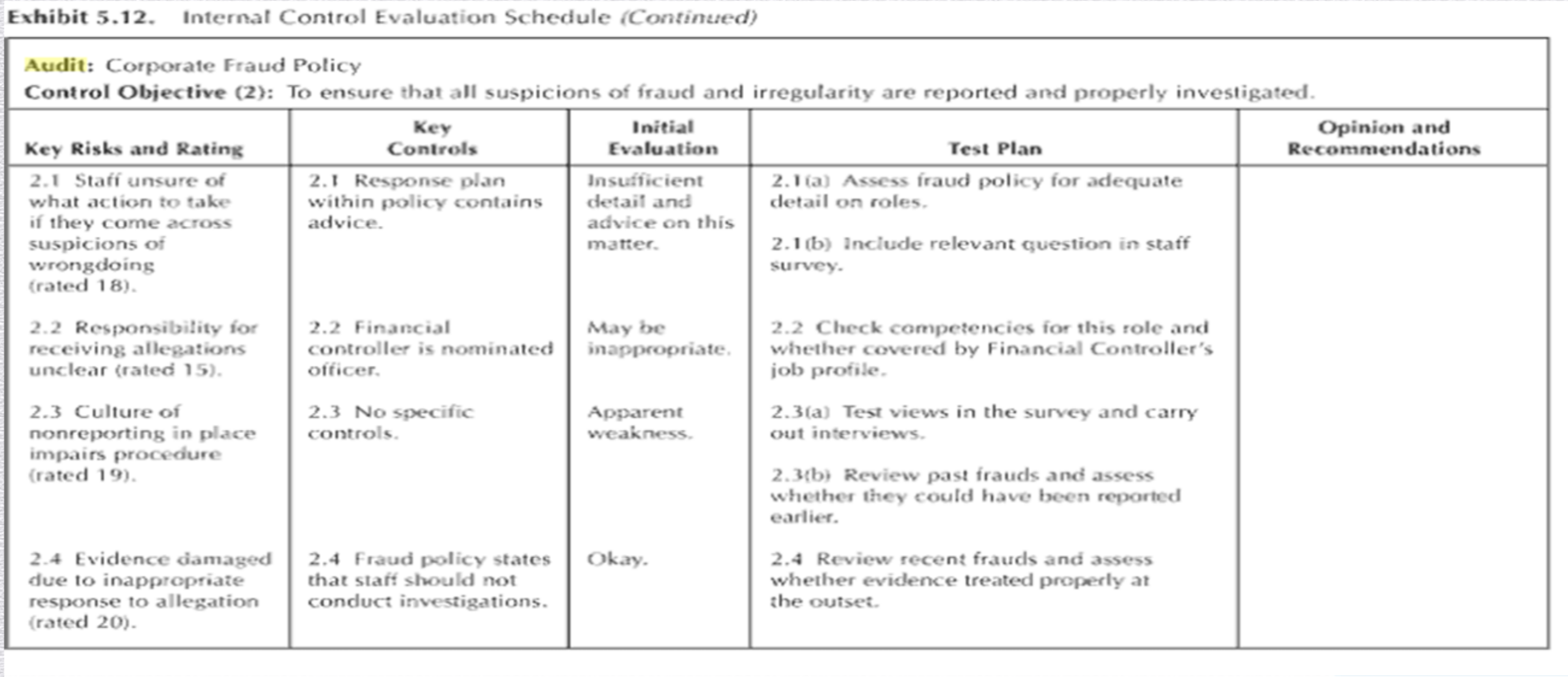


**Exhibit 5.12.** Internal Control Evaluation Schedule *(Continued)*

**Audit:** Corporate Fraud Policy

**Control Objective (2):** To ensure that all suspicions of fraud and irregularity are reported and properly investigated.

| Key Risks and Rating | Key Controls | Initial Evaluation | Test Plan | Opinion and Recommendations |
|---|---|---|---|---|
| 2.1 Staff unsure of what action to take if they come across suspicions of wrongdoing (rated 18). | 2.1 Response plan within policy contains advice. | Insufficient detail and advice on this matter. | 2.1(a) Assess fraud policy for adequate detail on roles.<br>2.1(b) Include relevant question in staff survey. | |
| 2.2 Responsibility for receiving allegations unclear (rated 15). | 2.2 Financial controller is nominated officer. | May be inappropriate. | 2.2 Check competencies for this role and whether covered by Financial Controller's job profile. | |
| 2.3 Culture of nonreporting in place impairs procedure (rated 19). | 2.3 No specific controls. | Apparent weakness. | 2.3(a) Test views in the survey and carry out interviews.<br>2.3(b) Review past frauds and assess whether they could have been reported earlier. | |
| 2.4 Evidence damaged due to inappropriate response to allegation (rated 20). | 2.4 Fraud policy states that staff should not conduct investigations. | Okay. | 2.4 Review recent frauds and assess whether evidence treated properly at the outset. | |

Source: Pickett, K.H. Spencer; The Internal Auditor at Work, 2004

# Communication / Draft Report

- Allow the auditors and management to discuss the findings prior to the release of the draft report
  - Identify discrepancies in the findings
  - Discuss potential risks and other mitigating controls
  - Identification of themes

- Beware: The “Draft Report” is often the actual audit findings, it is “Draft” in the sense that it does not yet have the management response
  - It may be too late to easily change wording or provide backup evidence at this point. It is *critical* to understand the audit process and schedule being used.

# Some Audit Vocabulary

- **Control:** A policy, procedure, or process whose objective is to reduce risk and increase the likelihood that established management goals and objectives will be achieved
- **Control Environment:** The attitude, awareness, and actions of the board, management, owners, and others about the importance of control. This includes integrity and ethical rules, management's philosophy and operating style, commitment to competence, board or audit committee participation, organizational structure, assignment of authority and responsibility, and human resource policies and practices.
- **Finding:** Condition requiring corrective action as identified by auditors in the course of their work. US Government audit standards require a finding to consist of four attributes: condition, criteria, cause and effect, with which Lawrence Sawyer's booker, Internal Auditing, agrees. To avoid negative connotations, the word observation is sometimes used rather than the term finding, deficiency or issue.
- **Management Response:** The official written response from the unit being audited covering the opinion of the findings, may contain a discussion of mitigating controls, situations or circumstances that relate to the findings and the strategies or steps the unit may take to resolve or mitigate the risks.

http://www.projectauditors.com/Auditor_Dictionary

# The Findings (example)

- *“Patch management is a critical process that can help to alleviate many of the challenges of securing computing systems. As vulnerabilities in a system are discovered, attackers may attempt to exploit them, possibly causing significant damage. Malicious acts can range from defacing Web sites to taking control of entire systems and thereby being able to read, modify, or delete sensitive information; disrupt operations; or launch attacks against other organizations’ systems. When a software vulnerability is discovered, the software vendor may develop and make a patch or work-around to mitigate the vulnerability”.*
- *“SEC does not have an effective patch management program. For example, SEC has not installed patches for critical vulnerabilities on two audit log servers and a network device. Because SEC has not installed and maintained the latest patches, its computing systems are more vulnerable to attackers taking advantage of outdated, less secure software”.*

2006 GAO Audit of the SEC; http://www.gao.gov/new.items/d06408.pdf

# The Findings (example)

- Recommendations – ideally focused on risk and not prescriptive on how to accomplish the goals and actionable
  - *"To help establish effective information security over key financial systems, data, and networks, we recommend that the SEC Chairman direct the Chief Information Officer to take the following seven actions to fully develop, document, and implement an effective agencywide [sic] information security program:*
    - *Fully document and implement a process for assessing risks for its information systems.*
    - *Finalize comprehensive information security policies and procedures.*
    - *Ensure that all system users comply with annual security awareness training requirements"*

# Management Response

- Do…
  - Management agrees….
  - Demonstrate understanding
  - Outline the approach
  - Highlight progress
  - Provide dates and auditable artifacts
- Don't …
  - Provide dates that are overly aggressive
  - Specify the particular solution unless it is a sure thing

# Management Response (example)

- *"We believe the GAO's recommendations are appropriate and actionable, and we are focused on supporting them fully. Specific corrective action plans, including specific milestones and timing for each of the audit recommendations…"*

# Take Home

- Don’t manage for compliance, manage for security and risk and compliance will follow
- Know why the regulation exists. Don’t manage for compliance, manage for security and risk and compliance will follow *(yes, I just said that)*
- Auditing is a tough job and many auditors are generalists, not specialists, so expect to need to teach why and how your approach meets to goal.
  - By demonstrating you know the goal, you win points.
    - If there are findings, now they are more likely about differences of approach and less likely about deficiencies is key control areas.
  - If you find that an auditing generalist knows more about operations your area than you do, it may be time to look for a new job.
- Understand your particular auditor’s process and schedule. Know when your opportunities are for discussing/debating the findings *before* they are finalized. If you are not active in this process, your findings will suffer.
- Risk Relevant findings are not bad – and should be the mutual goal

RSACONFERENCE2014
FEBRUARY 24 – 28 | MOSCONE CENTER | SAN FRANCISCO

Share.
Learn.
Secure.
Capitalizing on
Collective Intelligence

# Developing Cross Functional Leadership Skills

SESSION ID: SEM-M02

Doug Graham
EMC Corporation

# Defining Leadership

- A plethora of definitions - most synthesize to the following components:
  - Behaviors & activities
  - Influence & motivate
  - Change & effectiveness
- ***A process of social influence, which maximizes the efforts of others, towards the achievement of a goal.*** ***(Kevin Kruse, Forbes, 2013)***
- NOT - a position in a company
- NOT – a job title

# Why Does Leadership Matter

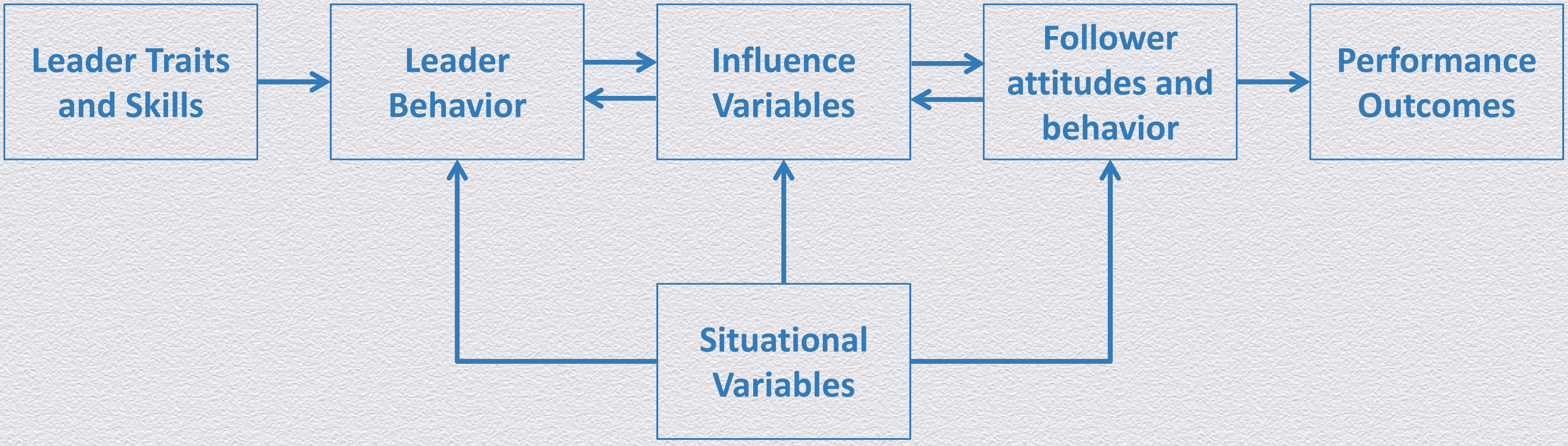
- Security programs change. Organizations change. Goals change.
  - Leaders are integral to change, not subjects of change
  - Change is inevitable whether we lead it or not
- Leaders can (and do) influence attitudes, beliefs, and values
  - It’s hard to find a technology to do that
  - Ultimately if we don’t get user behaviors we don’t get security
- Leaders strive for the best solution for their organization
  - Balanced solutions that take multiple options into account
  - There is no one size fits all for security

# The Problem

- Leadership development cannot be accomplished by HR and educational services alone (however it is often left to them)[1]
- The individuals and their managers need to have a shared responsibility[2]
- Most executives see improving and leveraging leadership talent as a top priority, and yet their leadership development (LD) program is going nowhere fast[3]
- The best way to get more leaders is to have leaders develop leaders[2]
- If we fail to develop leaders we fail to lead

1. Gaines, K. (2012). Leadership development. Leadership Excellence, 29(1), 9.
2. Tichy, N. (2012). Developing leaders. Leadership Excellence, 29(7), 5-6
3. Howard, A., & Wellins, R. S. (2010). Developing leaders. Leadership Excellence, 27(2), 20-21

# The leadership Process


Leader Traits and Skills

Leader Behavior

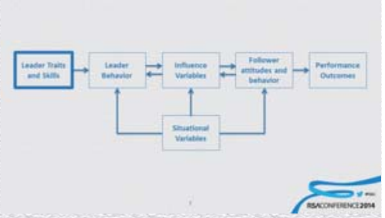
Influence Variables

Follower attitudes and behavior

Performance Outcomes

Situational Variables

Yukl, G. (2010). *Leadership in organizations* (7th ed.). Upper Saddle River, NJ. Pearson Prentice Hall



Leader Traits and Skills

Leader Behavior

Influence Variables

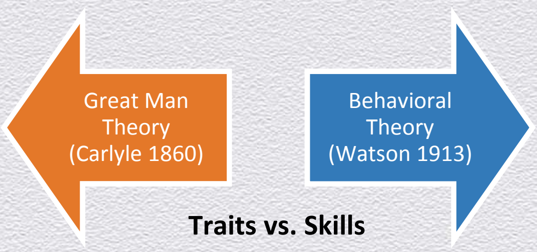
Follower attitudes and behavior

Performance Outcomes

Situational Variables

# Traits and Skills

- The traits vs skills argument has been debated for centuries
  - *If* traits are true then there isn't a lot we can do (aside from move people)
  - We can develop skills so focus here
- Traits or skills are reflected in behaviors
- Leadership styles can provide a taxonomy of skills and traits
- So traits and skills are interesting but ultimately behaviors matter

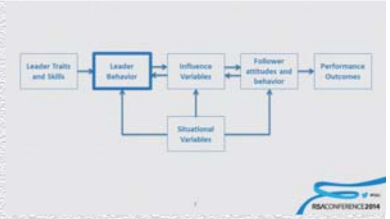


Great Man Theory (Carlyle 1860)

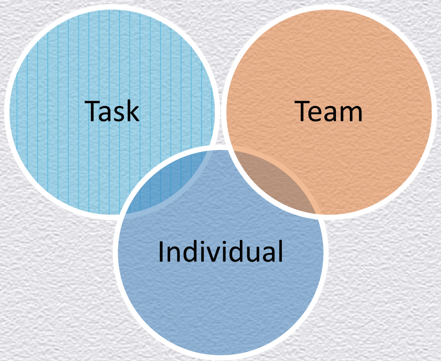
Behavioral Theory (Watson 1913)

Traits vs. Skills

# Leader Behavior

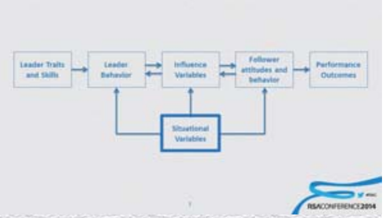


- Focus on what leaders actually DO
- Activities, behaviors, demands, opportunities, role conflicts
- Effective leader behavior
  - 15+ taxonomies
  - Most simplify complex social theory
  - Patterns rather than individual behaviors
  - Three prevalent categories are
    - Task focused
    - Individual (relationship) focused
    - Team focused



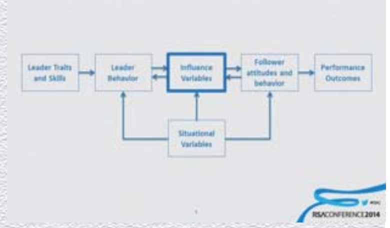
**Leadership Behavioral Categories**

# Some Situational Variables



- Nature of the organizational role and function of the participants
- Characteristics of the participants and stakeholders
- Organizational culture
- Nature of the problem
- Behavior modifiers
  - Situations can make certain behaviors more or less effective
  - Situational leadership wins the day here

# Influence Variables

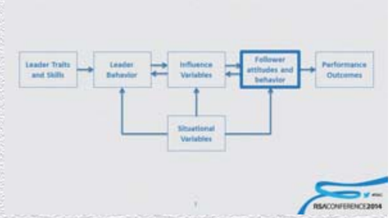


- Power Influence
  - Positional power
  - Personal power
- Participative Influence
  - Power sharing and empowerment
  - A key element in our leadership profile to develop our teams

| Positional Power | Personal Power |
|---|---|
| Legitimate Power | Referent Power |
| Reward Power | Expert Power |
| Coercive Power | |
| Information power | |
| Ecological Power | |

**Sources of Power**

# Impacting Follower Behavior

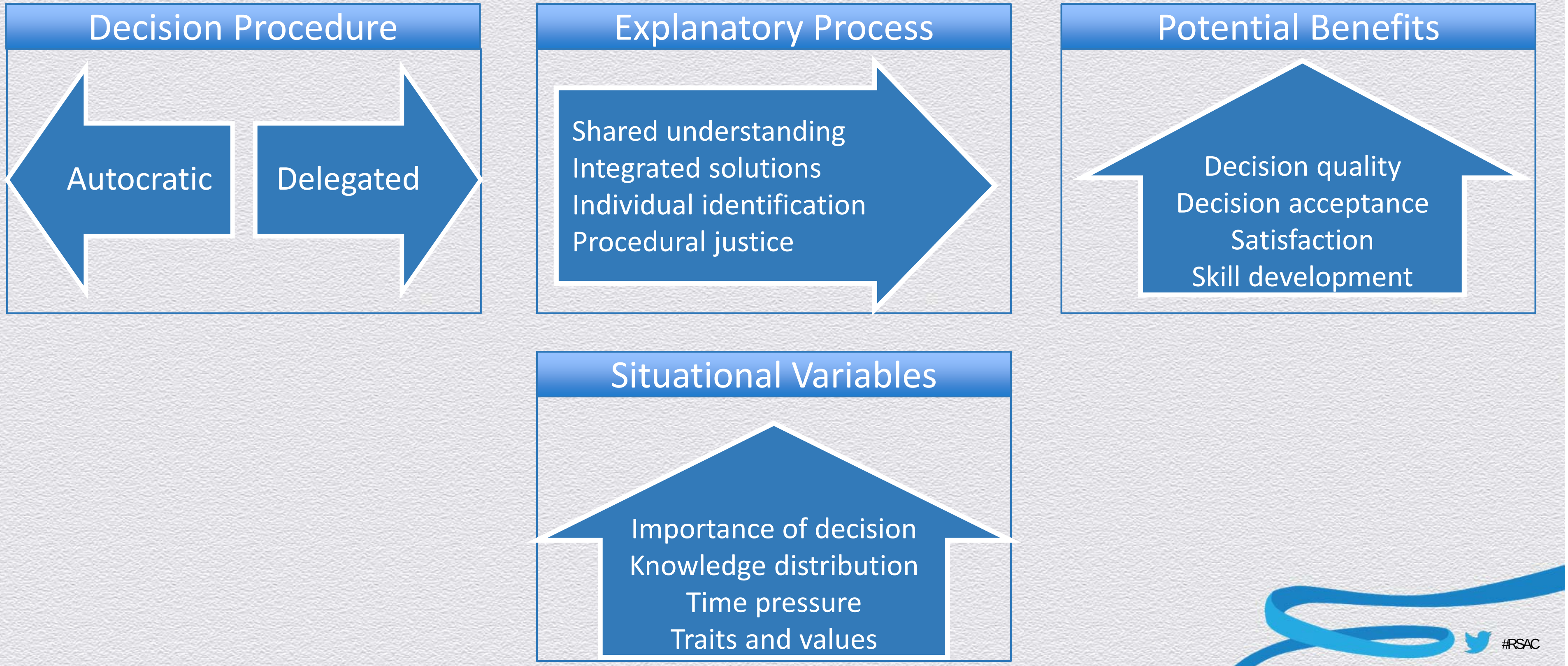


- Three levels of influence
  - Commitment, Compliance, Resistance
- Social exchange theory
  - Favor for a favor, mutual wins
  - Emphasis on personal power
- Contingency theory
  - You win I lose
  - Emphasis on positional power
- Efficacy factors into both theories

| Social | Contingency |
|---|---|
| Commitment ⇧ | Commitment ⇩ |
| Compliance ⇔ | Compliance ⇔ |
| Resistance ⇩ | Resistance ⇧ |

**Effect on behavior category**

# Simplified Participative Leadership Case



## Decision Procedure

Autocratic

Delegated

## Explanatory Process

Shared understanding
Integrated solutions
Individual identification
Procedural justice

## Potential Benefits

Decision quality
Decision acceptance
Satisfaction
Skill development

## Situational Variables

Importance of decision
Knowledge distribution
Time pressure
Traits and values

Adapted from Yukl, G. (2010). *Leadership in organizations* (7th ed.). Upper Saddle River, NJ. Pearson Prentice Hall

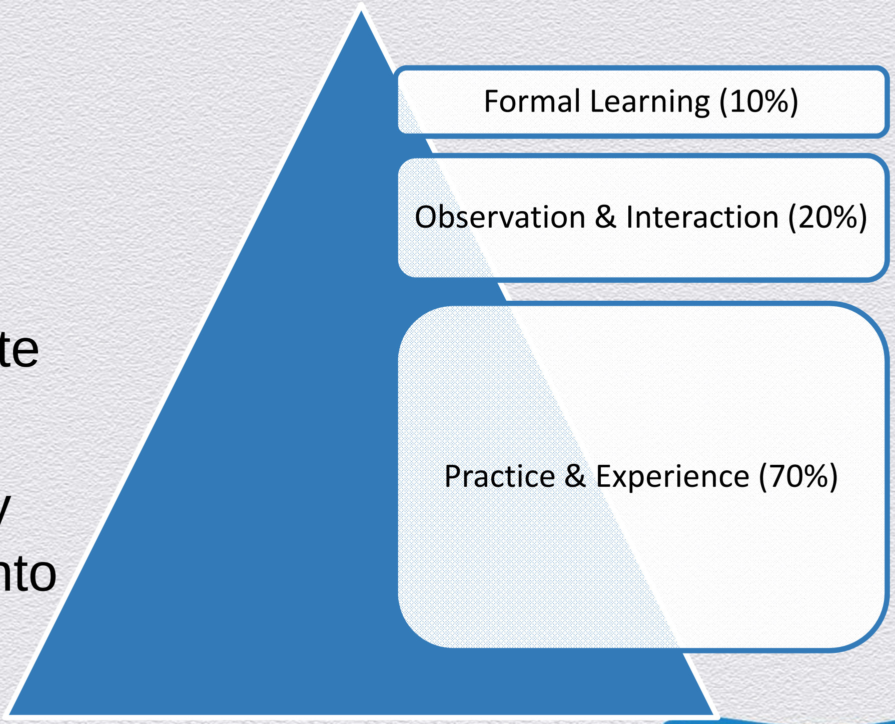
# The importance of delegation

| Reasons to delegate | | | | Reasons not to delegate |
|---|---|---|---|---|
| Develop subordinate skills and confidence | 97 | | 87 | Keep decisions involving confidential information |
| Enable subordinates to deal with problems quickly | 91 | | 76 | Keep tasks and decisions that are very important |
| Improve decisions by moving them close to the action | 89 | | 73 | Keep tasks and decisions central to your role |
| Increase subordinate commitment to a task | 89 | | 58 | Keep tasks for which mistakes are highly visible |
| Make the job more interesting for subordinates | 78 | | 51 | Keep tasks you can do better than subordinates |
| Reduce your workload to manage time better | 68 | | 43 | Keep tasks that are difficult to explain to subordinates |
| Satisfy superiors who want you to delegate more | 24 | | 39 | Keep tasks that are difficult to monitor |
| Get rid of tedious tasks you don’t want to do | 23 | | 24 | Keep tasks that are interesting and enjoyable |

Adapted from Yukl, G., & Fu, P. (1999). Determinants of delegation and consultation by managers. Journal of Organizational Behavior, 20, 219–232.

# Developing Leadership Skills

- How often do we take the easy way out and send people on courses?
- Are we exposing our future leaders to those that demonstrate good leadership?
- Are you taking every opportunity to allow your team to put skills into practice?



Formal Learning (10%)

Observation & Interaction (20%)

Practice & Experience (70%)

# Post training activities

- Discuss the training with the participant
    - Consider giving yourself a refresher by attending with them
- Provide opportunities to allow the participant to observe the skills in practice (especially in yourself)
- Give the person opportunities to practice their new skills
- Encourage good leadership behavior (and discourage bad)
- Embody leadership skills and values into performance appraisals
- Integrate leadership style and strategy into the organizational context.

# Takeaways

- Perform a self-assessment
  - Are you developing your leaders?
  - Are you developing your own leadership skills?
- If it doesn’t feel like a stretch you’re probably not doing enough
- Take mentoring and coaching opportunities
- Take an integrated approach
  - Formal, observation & interaction, practice and experience

RSA®CONFERENCE2014
FEBRUARY 24 – 28 | MOSCONE CENTER | SAN FRANCISCO

## Questions?

RSA®CONFERENCE2014

FEBRUARY 24 – 28 | MOSCONE CENTER | SAN FRANCISCO

Share.
Learn.
Secure.

Capitalizing on
Collective Intelligence

# Managing Third-Party Risk

SESSION ID: SEM-M02

Bruce Bonsall
BT US&C

Jeff Bardin
Treadstone 71

Evan Wheeler
Omgeo

Dave Notch
Intensity Analytics

Robert West
CipherCloud

RSA CONFERENCE 2014

FEBRUARY 24 – 28 | MOSCONE CENTER | SAN FRANCISCO

Share.
Learn.
Secure.

Capitalizing on
Collective Intelligence

# Stepping Inside the Board Room

SESSION ID: SEM-M02

Dennis Devlin

CISO, CPO and SVP of Privacy Practice
SAVANTURE
@DennisMDevlin

# First of all…

- DO NOT walk into a board room looking like the guy on the title slide!
  - DO wear a white shirt (it doesn’t show sweat) and use lots of deodorant
- Seriously, in the next 45 minutes we will decompose the process of preparing for, attending, and surviving a board of directors meeting
  - The presentation will include some real life examples and “war stories”
  - There will (hopefully) be time for questions and discussion at the end
- “There's nothing remarkable about it. All one has to do is hit the right keys at the right time and the instrument plays itself.” J. S. Bach

# Outline of Session

- An overview of 10 recommendations about:
  - Understanding your audience
  - Making it a team effort
  - Creating a compelling message
  - Presentation do’s and don'ts
  - Pre-game preparations
  - Post-game recap
- Some moments of truth
- Q&A

# 1. Know why you were invited

- Understand what's expected of you
  - You are attending the meeting at someone's request
  - Why were you invited to present?
  - What are they expecting to hear?
- Understand your audience
  - Research each board member and anticipate their questions
  - Study your website, annual report, investor relations, etc.

# What is a Board of Directors?

- A Board of Directors  is responsible for
  - protecting shareholders assets and ensuring reasonable ROI
  - assessing overall strategy and direction
  - hiring and firing the CEO
- A CEO is responsible for
  - overseeing day-to-day operation of the business
  - hiring all of the other employees
  - executing the strategy

# Board Members vs. Executives - Perspectives

- Board Members
  - Represent shareholders and bring perspectives from other companies
  - Rule 1. Did we increase shareholder value?
  - Rule 2. Did we protect our brand and increase market cap?
- Executives
  - Compensated with salary and incentive bonus
  - Rule 1. Did we make our numbers?
  - Rule 2. In all other cases refer to Rule 1.

# 2. Make it a team effort

- Your CEO, CFO, CMO, CIO, auditors, etc. have done this before
- They are colleagues and you are not here to compete with them
- You need to leverage what they know, and to help them look good
  - Ask them lots of questions and solicit guidance and counsel
  - Look at sample board presentations that others have done
  - Educate your colleagues about what you are doing in the process
  - Then they can become advocates and supporters vs. spectators

# 3. Create a compelling message

- Distill and sharpen your thoughts into a core message
- Focus on **what** you want them to hear and **why now**
- Less is always more when it comes to board presentations
- Use words that matter to the board, not words familiar to you

# CISOs are from Mars, Boards are from Venus

## Compelling to a CISO

- Migrate to next generation firewalls
- Use multi-factor authentication
- Minimize dwell time of APT's
- Harden virtualized server farm
- Reduce enterprise attack surfaces
- Deploy mobile device management

## Compelling to a Board Member

- Audit Committee or Entire Board?
- Manage and reduce enterprise risk
- Protect the brand and share price
- Grow revenues and reduce expenses
- Expand globally and grow market share
- Increase shareholder value and equity

# Make slides clear & accurate

- Slides must be condensed, relevant, and totally accurate
  - No more than 3-4 key points per slide
  - One mistake on a slide and your audience stops listening
  - Aside from presenting your slides speak when you’re spoken to and don’t improvise, editorialize or theorize – <u>nothing good will happen if you do</u>
- Think of your presentation like an iceberg
  - Your slides and everything you present are the part above the water
  - You need to have everything below the water in your head ready to confidently answer each and every question that is asked

# ***A REALLY BAD EXAMPLE*** of a Slide for a Board

- This year there were security breaches at a bunch of other companies
- Installing the latest IDS, IPS, DLP and UTM solutions will protect us better and may even provide a high ROI to the business someday
  - Failure to do so might put us at higher risk for a security incident or it might not
  - Our vendor will give us a significant discount if we purchase within 30 days
- If we install our recommended solution then we will be “state of the art”
  - Investing now might even save the company money in the long run
  - Please approve our $900K request ($600K capital + $200K annual operating)

# ***A BETTER EXAMPLE*** of a Slide for a Board

- Our 5 year strategic plan calls for a life cycle replacement of our core network security infrastructure in 2014
    - Our current infrastructure will no longer be supported by supplier in 2015
    - The replacement will require a budgeted capital investment of $600K and will reduce annual operating expense from $600K to $200K
    - The enhanced capabilities included in the upgrade will simplify our 2015 M&A plans and defer need for additional network security staff until 2016
- Do we have your approval to proceed?

# 5. Be clear about your "ask"

- If you are seeking an approval make it clear what you need
- Include all potential costs, all potential risks (of acting or not acting) and all potential benefits in terms that matter to the audience.
- Highlight any cost or complexity that you proposal is displacing
- Most of all try to demonstrate a "line of sight" between what you are proposing and the strategic goals of the organization
- Give your leadership what they need to help you make it happen

# CISO Insight from a Chief Financial Officer

- “Security is the only part of my organization where new investments never seem to displace old investments”
  - When we build a new factory the old one gets decommissioned
  - You always tell me that complexity is the enemy of security
  - But you add layers of incremental cost and complexity on what we have
  - How much is enough, how will we know if we’re spending too much?
- “If you don’t miss at least 10% of your flights you are spending too much time at the airport.” Bruce Schneier

# Sound Bites can help a Board help you Sell Security

- When executives repeat things they hear from you, things happen
  - “The risks are reputation, revenues, regulatory compliance”
  - “Our customers expect privacy, we must repect privacy”
  - “It’s about people, process, technology, in that order”
  - “We invest to protect, detect, react, in that order”
  - “ROI can mean Risk Of Incarceration”
  - “You can’t lose what you don’t have”
  - “Digital is forever unless you delete.”

# 6. Perfect practice makes perfect

- Find colleagues you have presented to the board and invite them to critique your presentation
- Take criticism and feedback constructively and don’t let your ego get in the way
- Find executive sponsor(s) who will be there with you (CIO, CTO, CFO, etc.) who can provide support if needed

# 7. Deliver your package early

- Boards need time to review materials ahead of time
- Boards never look kindly on material they receive at the last minute
- Once your slides are finalized review them with the CEO and other key executive sponsors BEFORE sending anything to the Board.
- Work with the team organizing the meeting to ensure that your materials are distributed as early as possible to the board
- And ensure that there are no typos, columns that don't add up, pie charts that exceed 100%, etc.

# 8. Sleep well and arrive early

- When you are as prepared as you can be stop worrying and get into your zone
  - Sleep well
  - Eat a good breakfast
  - Arrive early
  - Meet and greet attendees ahead of time if possible
  - Smile, be personable and exude composure and confidence

# 9. Read the room and adapt

- Be aware of how the board is responding to what you are saying
- If you see board members paging ahead in your presentation or looking at their watches consider pausing and asking for feedback
- Look for cues from your executive sponsor(s) (CIO, CTO, CFO, etc.)
- Stop and answer questions thoroughly when asked and commit to following up on questions if you don’t have an immediate answer
- Smile, be personable and exude composure and confidence
- Don’t be surprised if you are dismissed right after you present

# And Always Be Prepared… What If?

- What you would you do and what would you say if the Board or Audit Committee asked for a closed session with you and without the CEO and other key executives?
- As mentioned earlier in the presentation:
  - Maintain your composure and maintain eye contact
  - Speak when spoken to, and stick to facts and data vs. opinions
  - Don't improvise, editorialize or theorize, <u>nothing good will happen if you do</u>
  - Don't say anything to the Board that wouldn't say if the CEO were present

# 10.Follow up on action items

- Have a colleague take notes of any action items or questions that come up during your presentation
- Work with and through your executive sponsor(s) to formulate the answers and respond to the board in a timely fashion
- Ask for feedback from executive sponsor(s) and colleagues on what worked with your presentation, what didn’t work, and how you can improve for next time
- Savor that fact that you just survived your first “big league at bat”

# Board presentation moment of truth #1

- Early in my career (1970’s)
  - Board member:
    - Should we centralize or decentralize our data centers?
  - Me:
    - Sir, I try to take a middle of the road approach on that question.
  - Board member:
    - Young man, when try to you walk down the middle of the road you get hit by traffic in both directions.  Pick a side and be prepared to defend it.”

# Board presentation moment of truth #2

- Later in my career (1980’s)
  - Board member:
    - That was an excellent presentation of the voice and data network plan.
  - Me:
    - Thank you, sir.
  - Board member:
    - I have only one question. What you describe sounds great in practice, but how will it work in theory?

# Board presentation moment of truth #3

- Still later in my career (2000’s)
  - Board member:
    - Security should be centralized. Why did you decentralize your program?
  - Me:
    - Sir, we federated security to make it consistent with our culture and the way we manage other corporate functions. It increases buy-in from business unit CEO’s. It simplifies acquisitions and divestitures. It puts the cost of security into individual business unit P&L’s. And our businesses have different risks.
  - Board member:
    - Excellent points. Please carry on with your presentation.

# In summary – the 10 recommendations

**Preparation**

1. Know why you were invited
2. Make it a team effort
3. Create a compelling message
4. Make slides clear & accurate
5. Be clear about your “ask”

**Delivery**

6. Perfect practice makes perfect
7. Deliver your package early
8. Sleep well and be early
9. Read the room and adapt
10. Follow up on action items

What you need to show.

What you need to know.

And in conclusion…

# There is never enough time.  Thank you for yours.

- **Dennis Devlin**

  CISO, CPO and SVP of Privacy Practice
  **SAVANTURE**
  dennis.devlin@savanture.com

  Don’t be flattered if you are invited.
  Be flattered if you are invited back.