

RSA® Conference 2015

San Francisco | April 20-24 | Moscone Center

SESSION ID: PROF-M05

The 50 Minute MBA for Information Security Professionals

James K. Adamson

Senior Consultant
OBS Global
@jameskadamson

Dr. Branden R. Williams

CTO, Cyber Security Solutions
First Data
@brandenwilliams

CHANGE

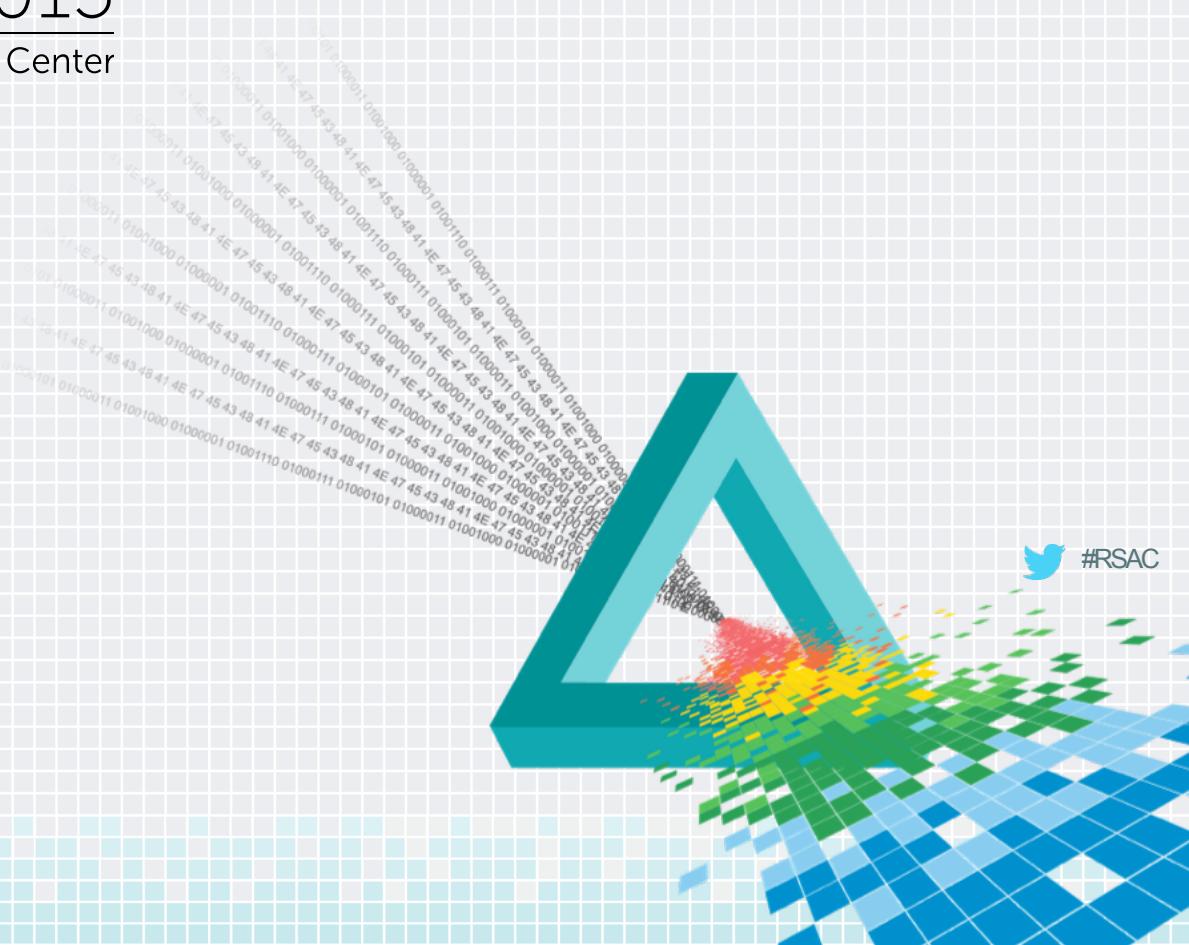
Challenge today's security thinking



RSA® Conference 2015

San Francisco | April 20-24 | Moscone Center

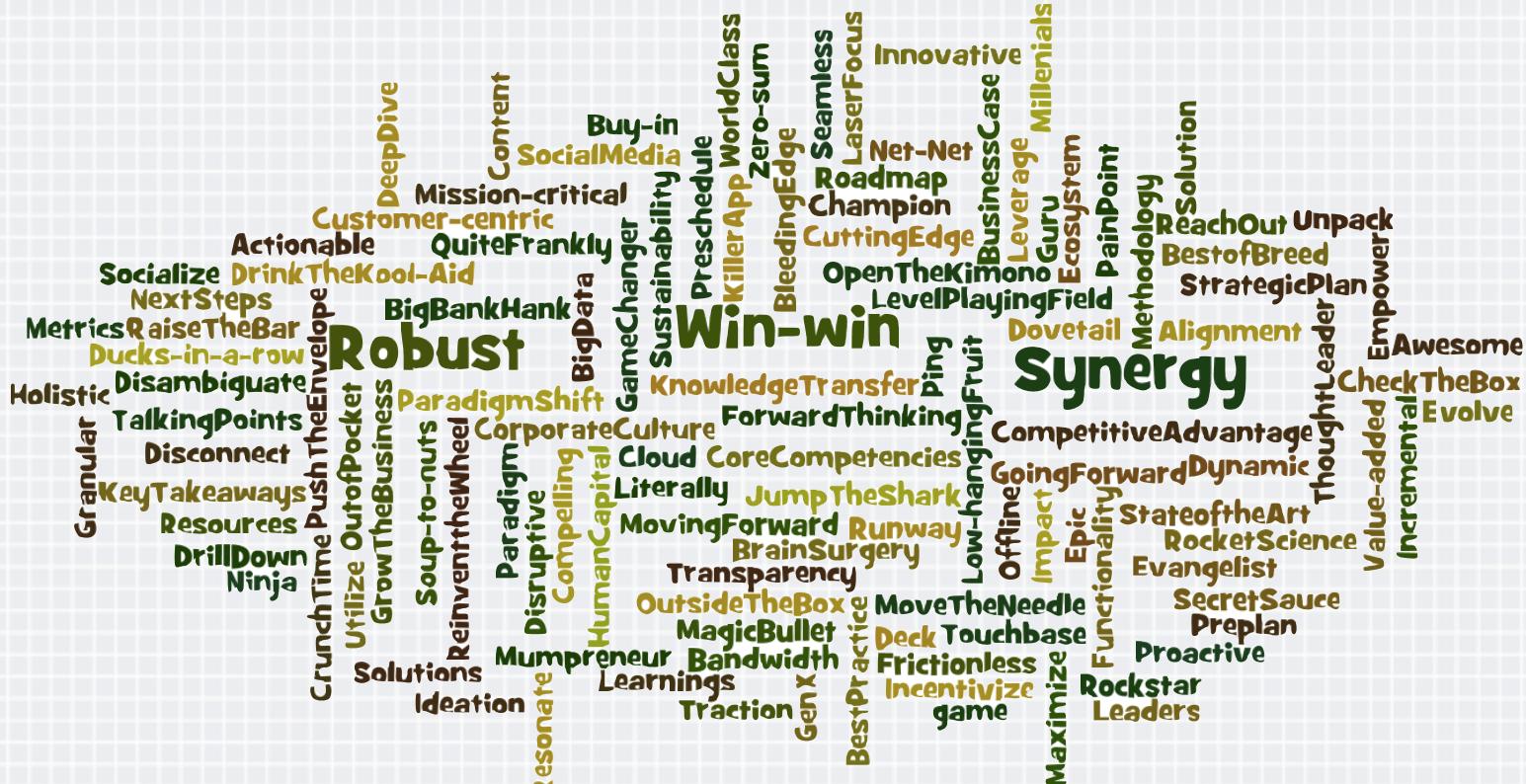
Overview



The Basement isn't for Security Anymore



Words we will try to avoid today



* Business terms (that are actually helpful) will be defined as we go along

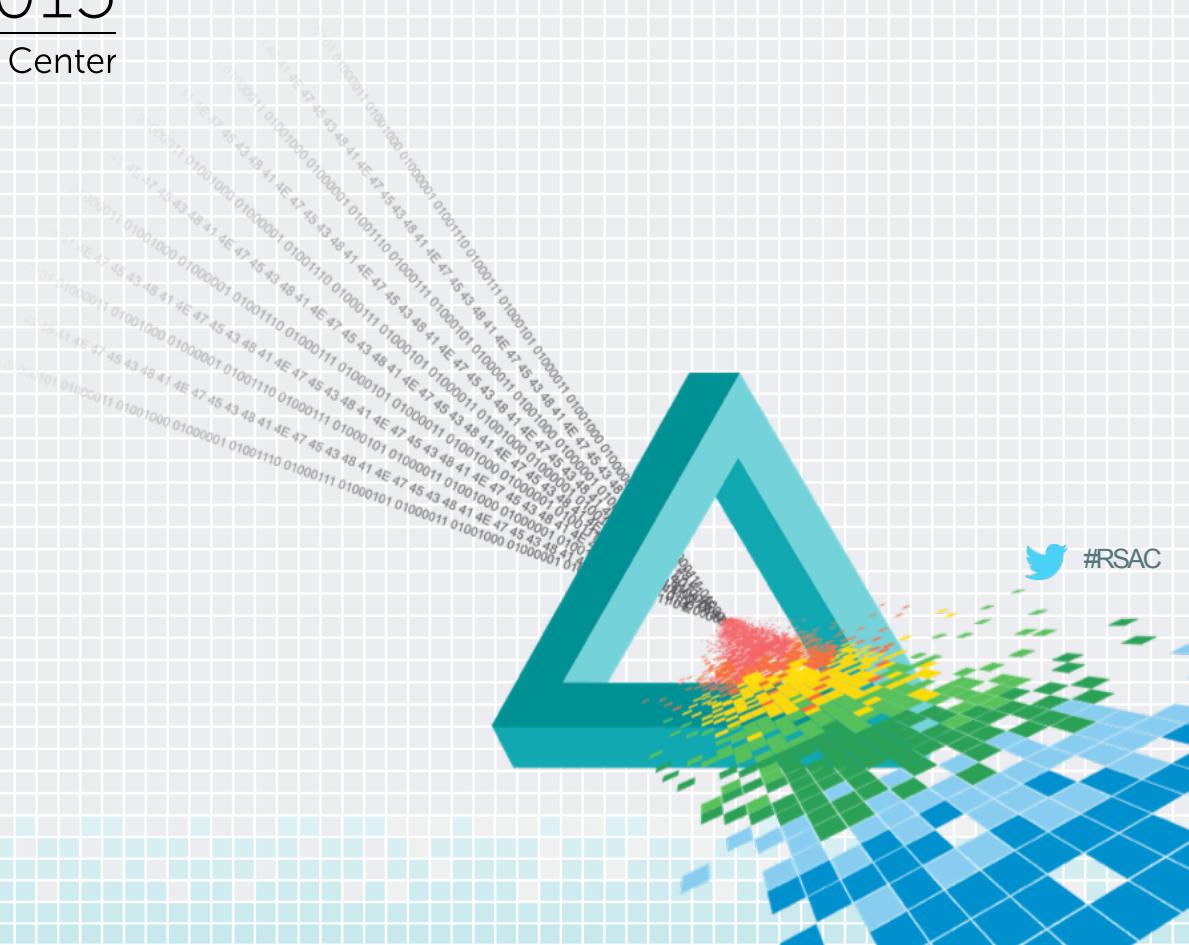
Quick note: Academics vs. Practitioners



RSA® Conference 2015

San Francisco | April 20-24 | Moscone Center

Our New Reality



#RSAC

Why should we care about the business?



More info on motivating others: <http://brando.ws/CS-Motivation>

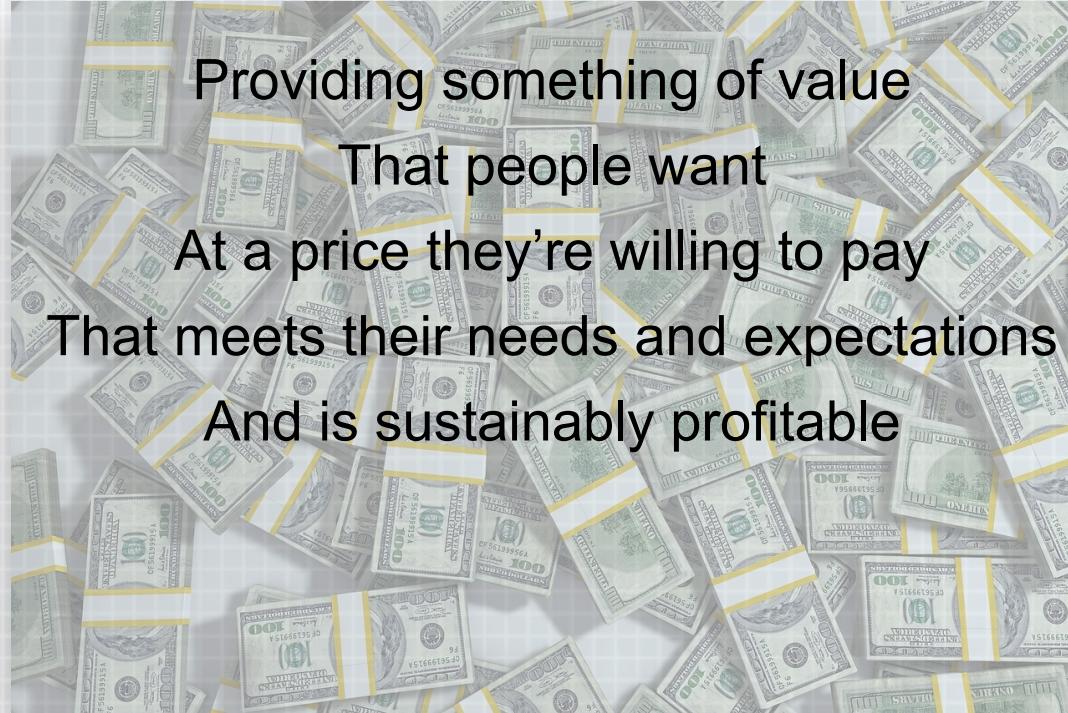


What's important to others in your company?

- ◆ You think security is important
- ◆ HR thinks people are important
- ◆ Finance thinks dollars are important
- ◆ Marketing thinks branding is important
- ◆ Sales thinks bookings are important
- ◆ IT thinks uptime is important
- ◆ CEO thinks his bonus is important (also maybe strategy)



What's ACTUALLY Important AS a business



How do you learn about business?



Typical Makeup of an MBA

- ◆ Covers the following areas:
 - ◆ Strategy & Innovation
 - ◆ Finance
 - ◆ Marketing
 - ◆ (Global) Operations
 - ◆ Data Analysis & Statistics
 - ◆ Leadership & Organizational Behavior
 - ◆ Specialization Classes
- ◆ Finishes with Capstone project



RSA® Conference 2015

San Francisco | April 20-24 | Moscone Center

Strategy & Innovation



What is Strategy (besides a buzzword)?

- ◆ Short and long term planning for the enterprise (Policy)
- ◆ Execution of the strategy—details (Procedure)
- ◆ Common elements in a strategy:
 - ◆ Vision statement / Elevator Pitch
 - ◆ What is our business model
 - ◆ What makes us different/better
 - ◆ What markets will we enter/divest
 - ◆ What products will we develop/shelve
 - ◆ What are the 3-5 year goals that we must manage to



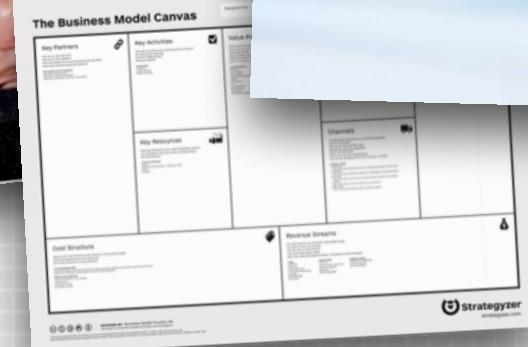
Strategy: Types and Tools

- ◆ Generic Corporate Strategies:
 - ◆ Low-Cost Provider
 - ◆ Broad Differentiation
 - ◆ Best-Cost Provider
 - ◆ Focused Low-Cost Provider
 - ◆ Focused Differentiation
- ◆ Tools:
 - ◆ Balanced Scorecard (Kaplan)
 - ◆ Business Model Canvas (Check the Resource Guide)

Thompson, A., Peteraf, M., Gamble, J., & Strickland, A. J. (2010). Crafting and executing strategy: The quest for competitive advantage (17th ed.). New York, NY: McGraw-Hill.

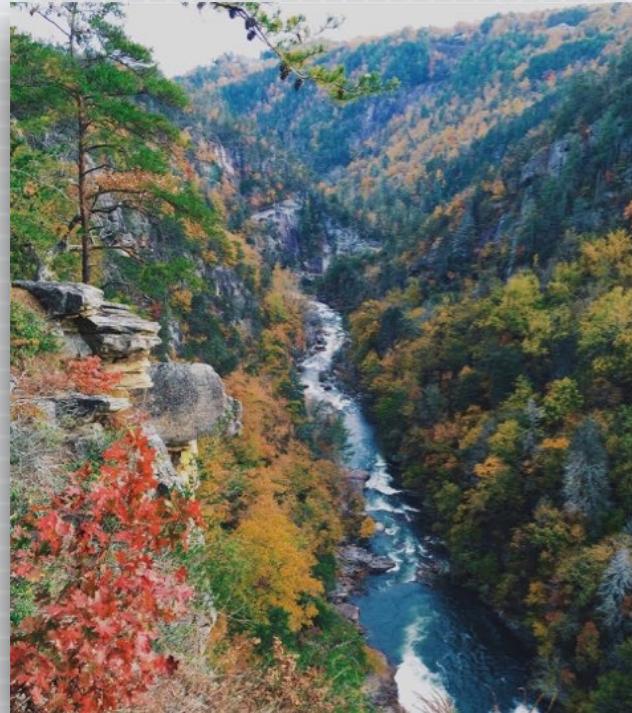


Strategy & Innovation Theories



Strategy (Translating to Security)

- ◆ Alignment is KEY!
- ◆ The strategy is the current in the center of the river...
- ◆ ... eddies on the edges cut into flow.
- ◆ How to leverage strategy:
 - ◆ Ensure your work aligns with corporate strategy
 - ◆ Be aware of future-looking statements (planning)
 - ◆ As a tool to clarify requests to the InfoSec group



RSA® Conference 2015

San Francisco | April 20-24 | Moscone Center

Finance



#RSAC

Finance

- ◆ Financial Accounting, Managerial Cost Accounting, Finance 101
- ◆ The basics:
 - ◆ Investors and owners expect to know where the money goes
 - ◆ “For every dollar I give you, I expect you to produce \$1.20.” (20%)
- ◆ How does this translate?
 - ◆ When you ask for \$\$\$ for a project, someone has to find a way to deliver return
 - ◆ Perhaps this is why security budget is so hard to come by?



Motivations of Finance People

- ◆ What are finance people asked to do?
 - ◆ Cut costs to maintain or improve margins
 - ◆ Raise funding via equity or debt
 - ◆ Assist in models for M&A
 - ◆ Balance demands of employees/managers/investors/customers
- ◆ What are finance people measured on?
 - ◆ Hitting targets
 - ◆ Improving financial positions
 - ◆ Providing investment funds



Finance (Translating to Security)

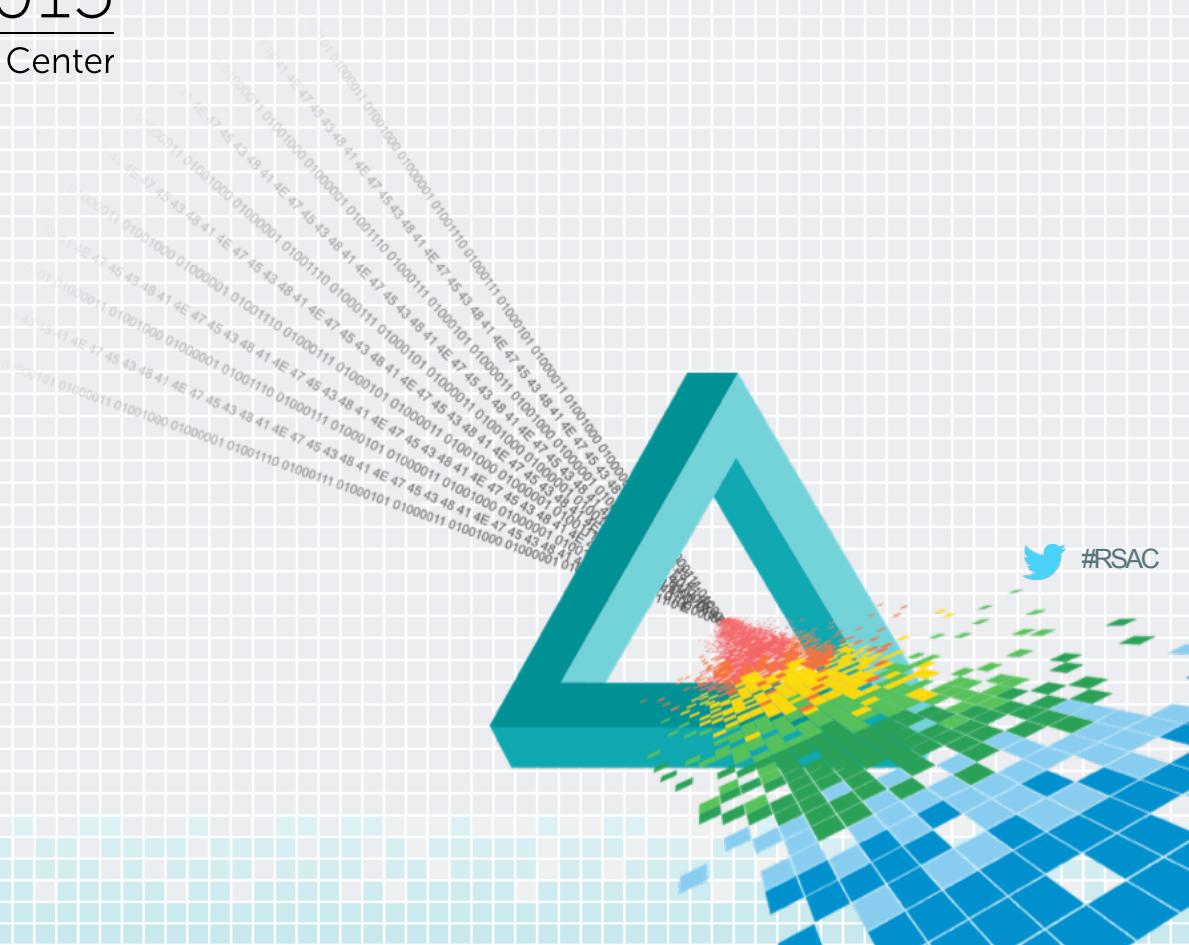
- ◆ Managers must balance revenue & expense requirements
- ◆ Risk management is critically important...
- ◆ ... and sometimes terribly done (see recent breaches!)
- ◆ Beating a dying horse time:
 - ◆ Align with the revenue side of the business
 - ◆ Be an enabler of business
 - ◆ Show how investments in security allow the business to make riskier decisions for better returns



RSA® Conference 2015

San Francisco | April 20-24 | Moscone Center

Marketing



Marketing

- ◆ In contrast to popular InfoSec tweets, these people have value
- ◆ If a business fails in the woods and no customers are around to hear...
- ◆ Get the right information to the right people the right way
- ◆ This could include tasks such as:
 - ◆ Promotion
 - ◆ Branding
 - ◆ Market segmentation
 - ◆ Sales support
 - ◆ PR



Motivations of Marketing People

- ◆ What are marketing people asked to do?
 - ◆ Expand positive brand awareness
 - ◆ Assist in market segmentation
 - ◆ Generate sales leads
 - ◆ Handle messaging and public relations
- ◆ What are marketing people measured on?
 - ◆ Exposure/Promotion
 - ◆ Qualified leads (quantity and quality)
 - ◆ Consistent messaging



Marketing (Translating to Security)

- ◆ Marketers care about propelling the business forward
- ◆ They take liberties with messaging...
- ◆ ... and sometimes we mock them.
- ◆ How to work with them:
 - ◆ Promote security as a customer initiative
 - ◆ Highlight how it differentiates you in the market
 - ◆ Enlist their help with internal education
 - ◆ Have them promote your initiative!



RSA® Conference 2015

San Francisco | April 20-24 | Moscone Center

(Global) Operations



#RSAC

(Global) Operations

- ◆ Executing on business strategy
- ◆ Includes processes that create and deliver the product:
 - ◆ Manufacturing/Developing
 - ◆ Supplying
 - ◆ Production
 - ◆ Distribution
- ◆ Increasingly includes managing activities in many places+countries
- ◆ This can be true of physical products or knowledge work



Motivations of (Global) Operations People

- ◆ What are operations people asked to do?
 - ◆ Convert materials and labor into goods and services
 - ◆ Do so efficiently to maximize profit
- ◆ What are operations people measured on?
 - ◆ Margin
 - ◆ Efficiency
 - ◆ Kaizen



(Global) Operations (Translating to Security)

- ◆ InfoSec is extremely relevant to operations groups
- ◆ Business chooses to open a facility in Manila
 - ◆ InfoSec needs to perform risk assessment
- ◆ Supply chains require info sharing and interconnectedness
 - ◆ Monitor what types of data can be shared with who and by what method
- ◆ Company starts to allow employees to work remotely every third Friday
 - ◆ Enable secure communications via corporate VPN with 2FA



Data Analysis & Statistics

- ◆ Data-based decision making
- ◆ Moving from qualitative to quantitative management
- ◆ Companies are collecting more data about more things
 - ◆ But they have to figure out what it means, or it's useless
- ◆ Technical tools have advanced this practice
 - ◆ Excel does a great job
 - ◆ SQL can do more
 - ◆ Python, R, SAS, SPSS do most



Data Analysis & Statistics (Translating to Security)

- ◆ Data here, data there
 - ◆ InfoSec should protect data
 - ◆ But groups now need to be able to access and use that information
 - ◆ Help implement new technologies that can make both happen
- ◆ Risk management
 - ◆ You can actually now explain to management, in their language, what your efforts will do to reduce corporate exposure to risk
- ◆ Advanced security analytics
 - ◆ Identify threats nearer to real time
 - ◆ Better than discovering you've been breached for 15 months



Leadership & Organizational Behavior

- ◆ People are weird.
- ◆ People know when they are being studied.
- ◆ People are great.
- ◆ People suck.
- ◆ Whether we like it or not, we have to work with people.
- ◆ This area of study has very rich literature with many studies:
 - ◆ Hawthorne Effect
 - ◆ Halo Effect
 - ◆ Bias



What do students learn here?

- ◆ Lots of soft skills here:
 - ◆ Interpersonal skills
 - ◆ Conflict resolution
 - ◆ Leadership skills
 - ◆ Communication
 - ◆ Collaboration
 - ◆ Relationship building
 - ◆ Negotiation
- ◆ All the stuff that technology pros scoff at but could be the most valuable skills in your tool belt



Ethics



or



Apply What You Have Learned Today

- ◆ Immediate actions
 - ◆ Identify the other groups in your business and the value they provide
 - ◆ Understand how individuals in these groups are rewarded (goals)
 - ◆ Locate and digest your business's strategy (and how it is executed)
- ◆ Actions to implement within 3 months of returning to the office
 - ◆ Put down the IT book, pick up a business book (See references)
 - ◆ Review of current InfoSec initiatives to check for alignment
 - ◆ Plan to align future security projects with business



RSA® Conference 2015

San Francisco | April 20-24 | Moscone Center



Questions?

@jameskadamson

@brandenwilliams

