RSAConference2015

San Francisco | April 20-24 | Moscone Center

CHANGE

Challenge today's security thinking

SESSION ID: CXO-T10

The CISO Reporting Project

Nicholas J. Percoco

Vice President, Strategic Services
Rapid7
@c7five

Trey Ford

Global Security Strategist
Rapid7
@treyford

Agenda

- Introductions
- Motivations for Research
- Boardroom Disciplines
- The Security Executive’s Challenges
- Research Results – 90 CISOs Point of View
- Affecting Change – Rapid7 Research Project

Introductions

- Nicholas J. Percoco, VP - Strategic Services
  - 18 years experience in information security
  - Leads Rapid7’s Program Development & Incident Response teams
  - Prior to Rapid7, built and ran SpiderLabs for almost 11 years
- Trey Ford, Global Security Strategist
  - Industry Advocate, Community Outreach, Spokesperson at Rapid7
  - Former GM at Black Hat, IR at Zynga, PM at McAfee, WhiteHat Security
  - Earned a gold star on a science project

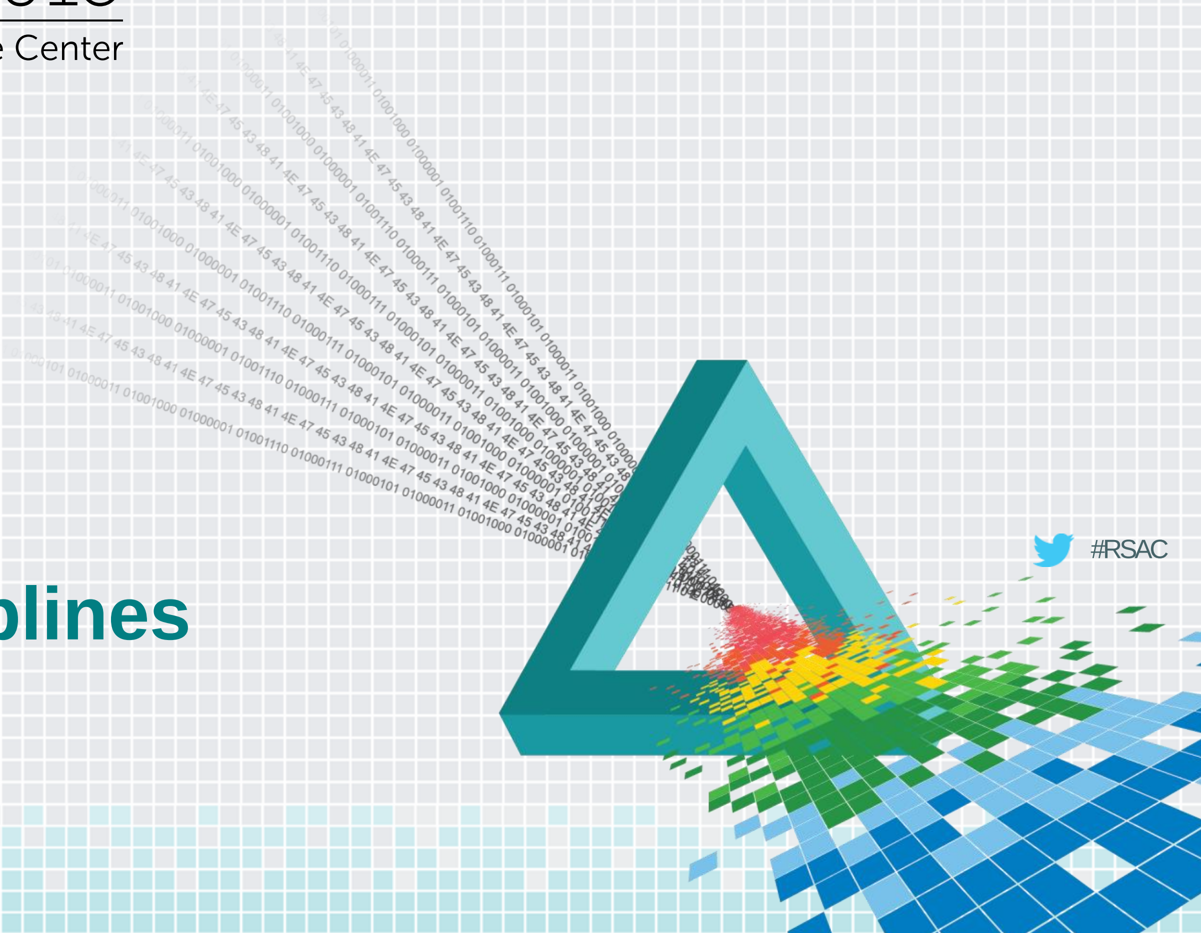
Motivation for this Research

- Most security professionals struggle with metrics and reporting
- Board level executives don’t often know what they need
- CISO’s often don’t know what Board members want
- No CISO playbook for metrics and reporting exists
- We want to change this by closer aligning security and business

RSA Conference2015

San Francisco | April 20-24 | Moscone Center

Boardroom Disciplines



#RSAC

Established Professions

- Medicine
- Law
- Engineering
- Accounting

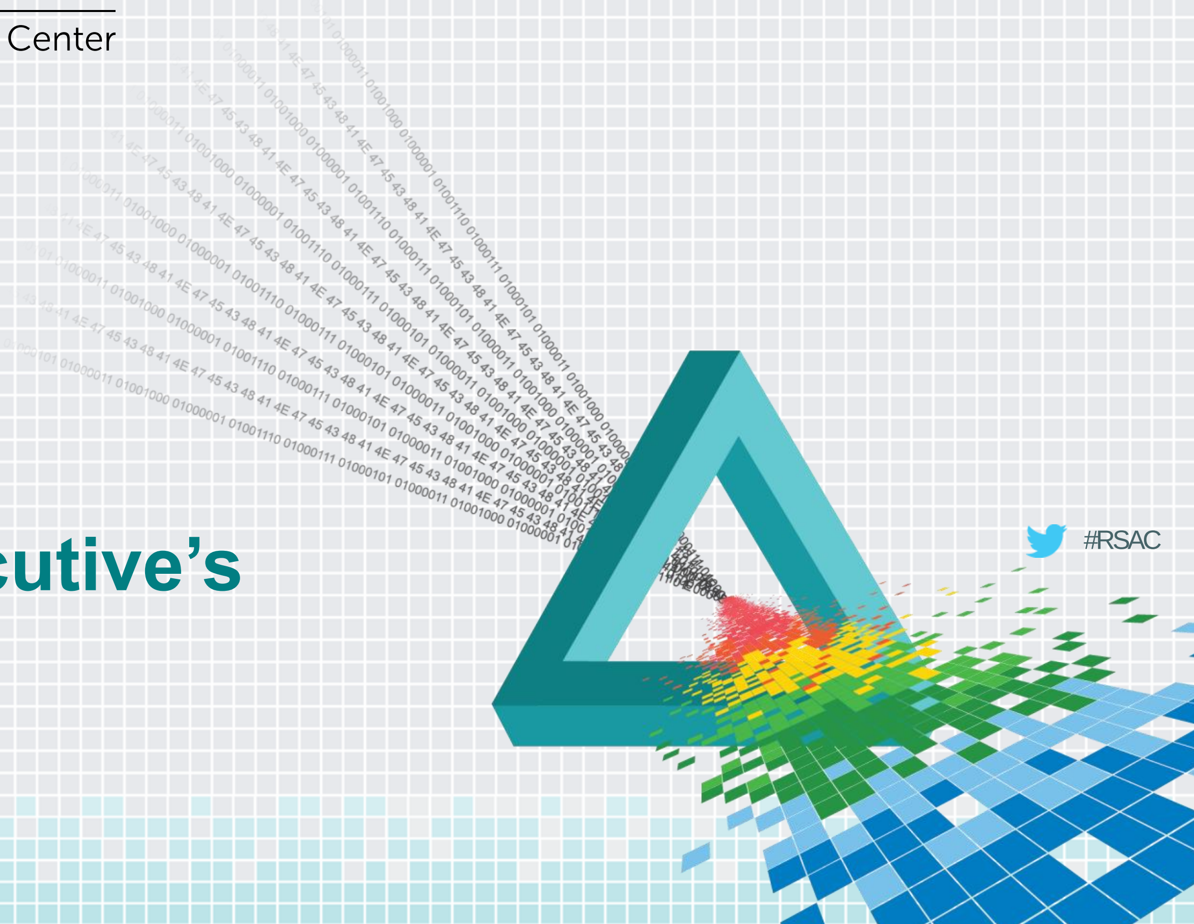
Boardroom Technology

NCR – 1884

IBM - 1911

RSAConference2015

San Francisco | April 20-24 | Moscone Center



#RSAC

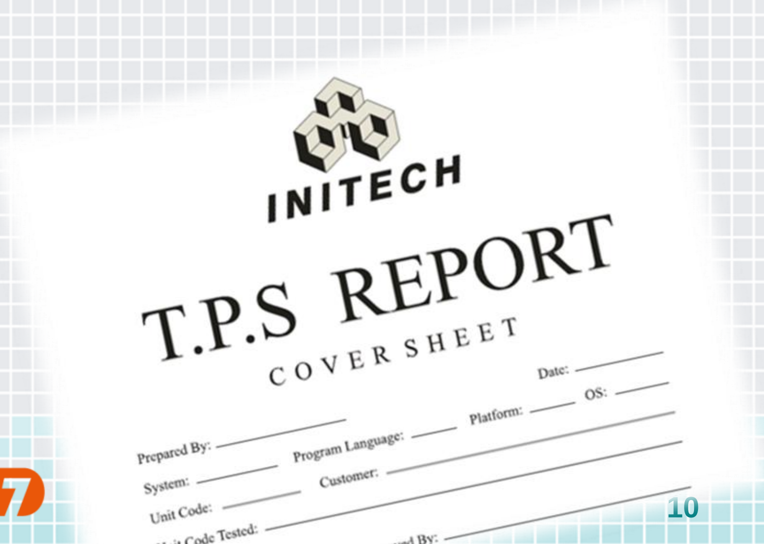
The Security Executive’s Challenges

Information Security

No Real ‘How To” Guide

Security Status Report

- Accounting has their GAAP
- Legal and Medicine has theirs
- What about Information Security?



INITECH

T.P.S REPORT

COVER SHEET

Date: ______

Prepared By: ______ Program Language: ______ Platform: ______ OS: ______

System: ______ Customer: ______

Unit Code: ______

Code Tested: ______ ed By: ______

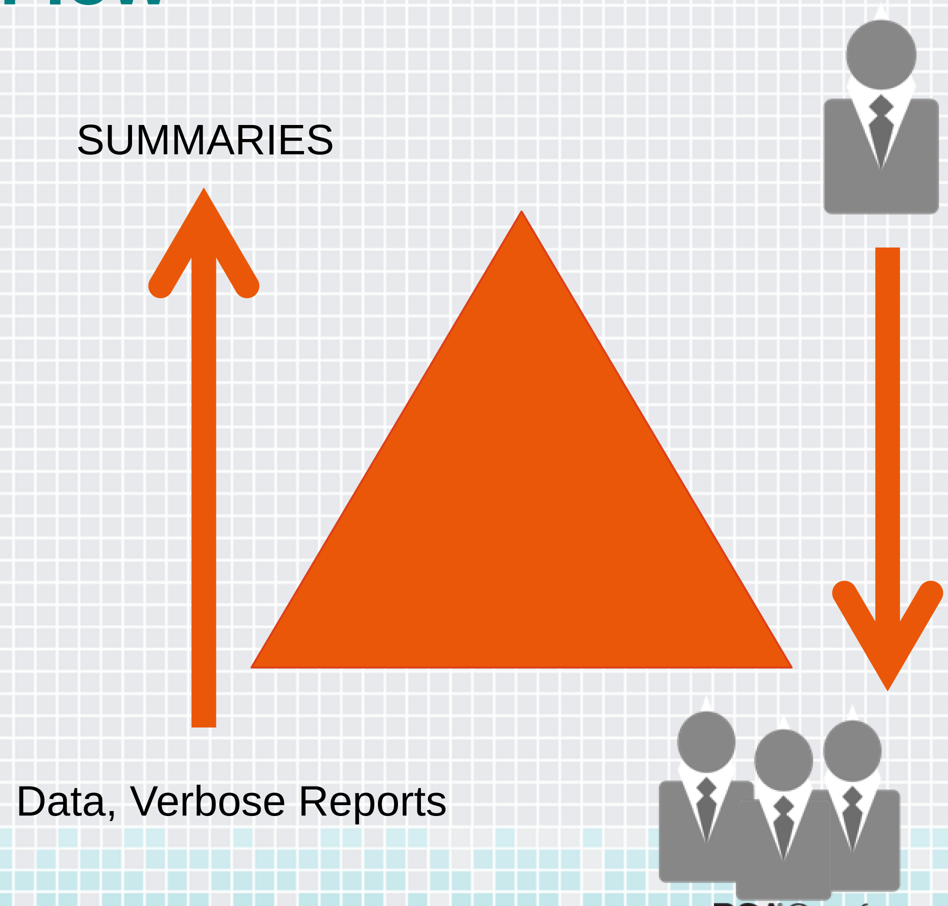
Communication Flow

WISDOM

KNOWLEDGE

INFORMATION

DATA

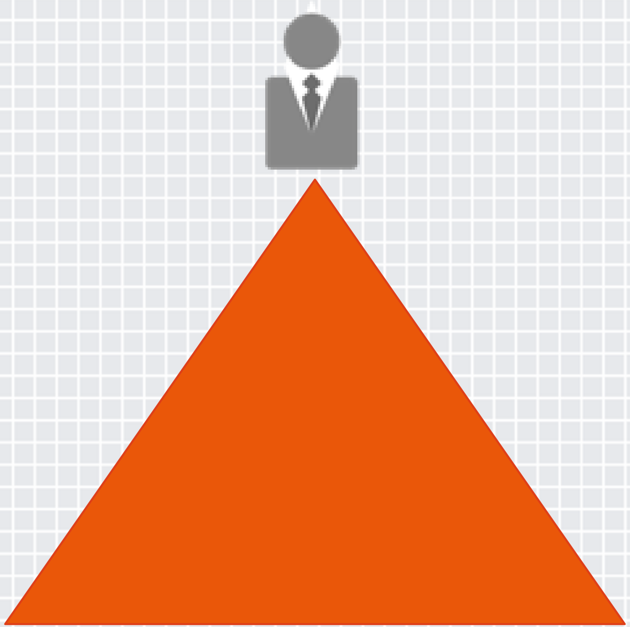


SUMMARIES

Data, Verbose Reports

Curse of Knowledge

- **Uncertainty at the Top**
  - Executives are Comfortable
  - Engineers are NOT Comfortable
- **The Secret**
  - Helping inform a point of view
  - The idea may be right or wrong



Vulnerability & External Audit Reports

BURY THEM!?!?!

Incidents Happen

- Unsafe to Discuss?
- Acknowledge bias:
  - Prevention vs. Response

Activating Incident Response

- Admitting Failure?
- Insurance Policy?

RSAConference2015

San Francisco | April 20-24 | Moscone Center

Research Results:
90 CISOs Point of View

#RSAC

Research Results: What We Already Knew

- All CISOs have to address 3 questions:
  - What do I need to know?
  - Why does it matter? / What do I care?
  - What do you need from me?

- This is both SIMPLE and HARD!

Research Results: Tenure

- 20% have been in the CISO role < 12 months.
- New focus by Board in Security changing their priorities
- 1/5 of CISOs are looking to validate their programs / guidance

Research Results: Area of Focus

- 15% report mostly on specific project status
- 20% are discussing Compliance Audits
- 25% are talking about Incident Response capabilities
- 49% are reporting on Vulnerability Management

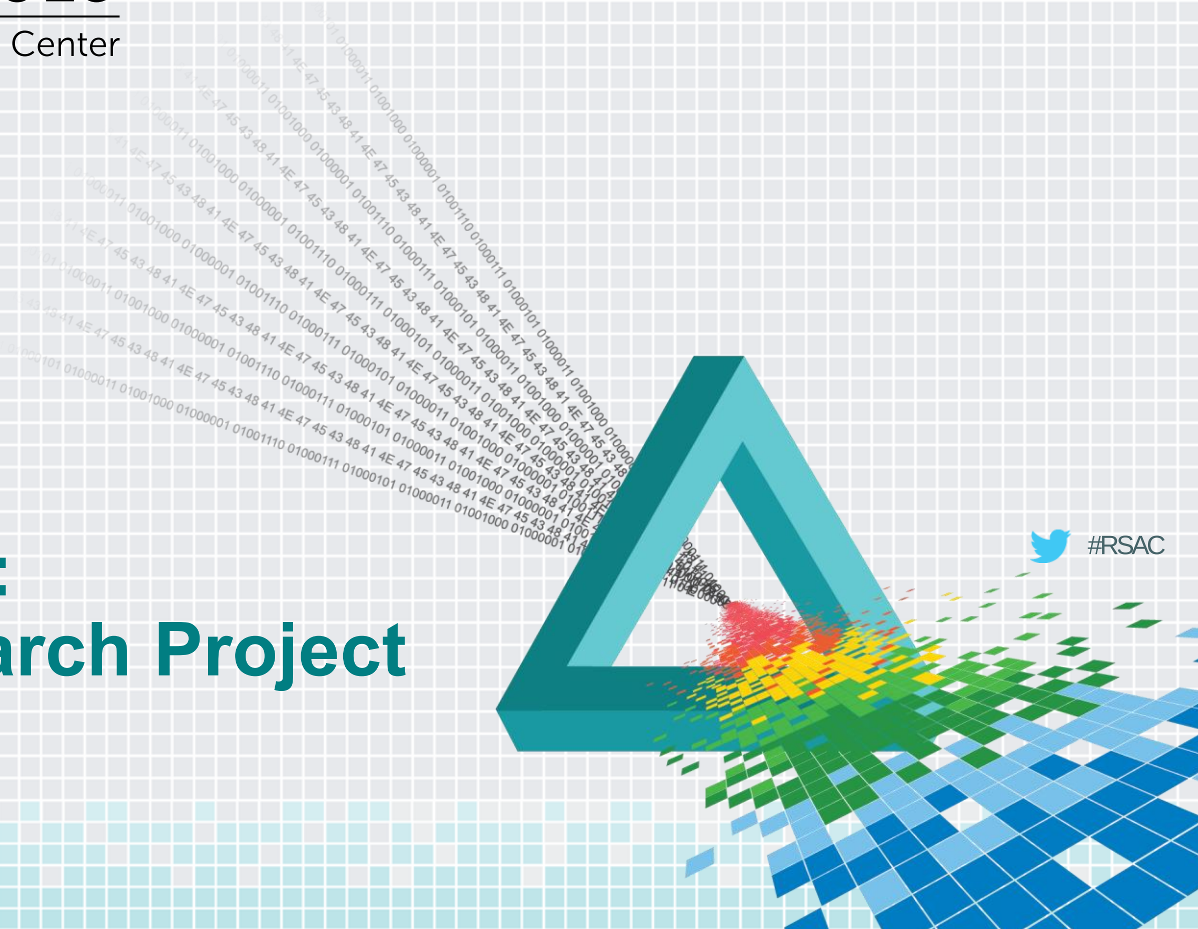
Research Results: Tangible & Obscure

- 6% report on “Volume of Spam Blocked”
- 12% report no metrics to their Board
- Also responded w/ “lost laptops/iPads” and “website blocking”
- Many CISOs grasp for topics to connect with their Boards

RSAConference2015

San Francisco | April 20-24 | Moscone Center

Affecting Change: Rapid7's Research Project



#RSAC

Affecting Change: Expanding the Survey

- A Quantitative and Qualitative Survey
- Need > 250 CISOs and Non-Security Executives
- Takes less than 15 minutes of someone’s time
- Results in an open source “Playbook” for CISOs
  - What should be reported? (Routine vs. Special Requests)
  - Mapping to Common Security Frameworks

Affecting Change: Take it Yourself / Contribute

- Please take 15 minutes to complete the survey TODAY

bit.ly/CISOSurvey2015

- Then, pass it along:
  - 2 security colleagues
  - 3 non-security colleagues!

How to Apply What You’ve Learned

- Today you should:
  - Take Rapid7’s CISO Reporting Survey
- In the next two week:
  - Evaluate what your teams are reporting
  - Think about how non-security executives will consume the results
  - Modify your metrics and report to focus more on business risk
- In the next 3 months:
  - Contact the consumers of your updated reports
  - Ask for feedback vs. previous months / years

RSAConference2015

San Francisco | April 20-24 | Moscone Center

CHANGE

Challenge today's security thinking

SESSION ID: CXO-T10

The CISO Reporting Project

Nicholas J. Percoco

Vice President, Strategic Services
Rapid7
@c7five

Trey Ford

Global Security Strategist
Rapid7
@treyford

#RSAC