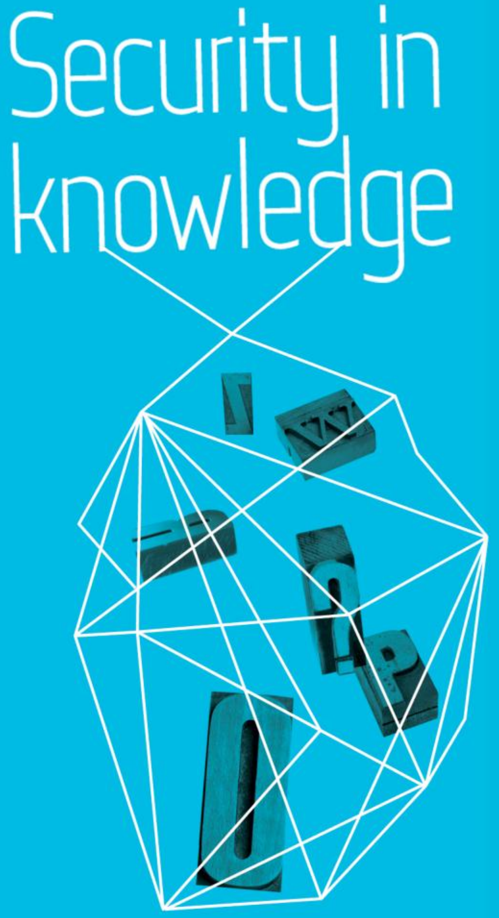
RSACONFERENCE2013

Managing Security Risk: The CSO Panel



Moderator:

Gary McGraw
Cigital

Panelists:

Eric Grosse
Google

Gary Warzala
Visa

Howard Schmidt
Former Presidential Cyber-coordinator

Jason Witty
USBank

cigital

IEEE SECURITY & PRIVACY

Session ID: CISO-W25

Session Classification: Advanced

PANEL FORMAT

- Introductions
- What does a CSO do all day? (one slide each)
- Six central questions
- Open discussion

RSA CONFERENCE 2013

WHAT DOES A CSO DO ALL DAY?

cigital

IEEE SECURITY & PRIVACY

WHAT DOES A CSO DO?

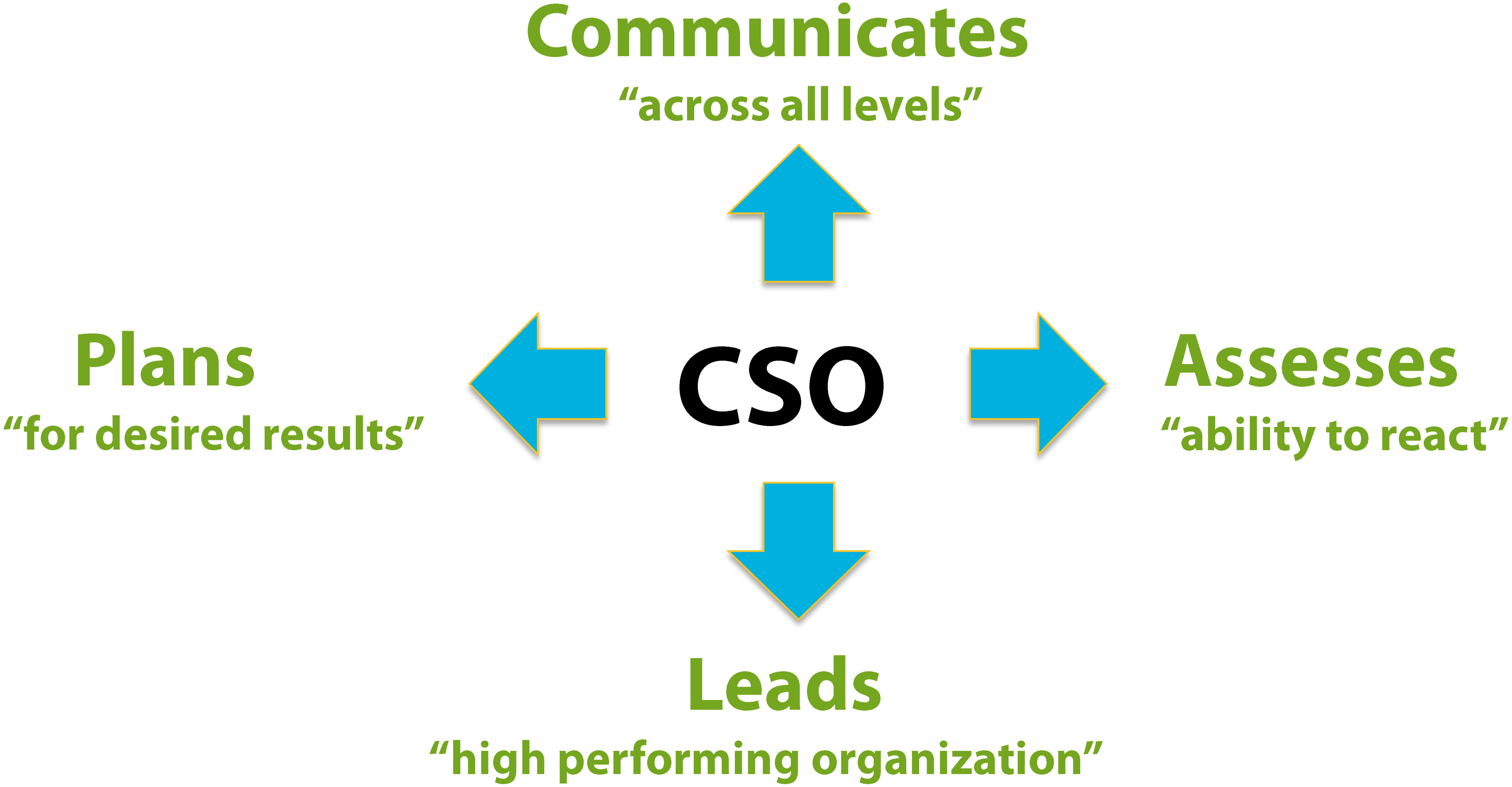
I think about, and fix where I can by:

- hiring and retaining the right people, and deploying them in the right roles
- learning about who may attack and how those attacks can be disrupted
- identifying our important assets and verifying the proper access controls
- making our users and developers lives easier, subject to the previous points

WHAT DOES A CSO DO?

- Review various information security news sources
- Oversee policy development
- Oversee audit process, results and remediation actions
- Work with biz units to develop security processes to meet their needs.
- Work with biz executives to evangelize information security
- Interact with IT-ISAC, US CERT and relevant external sources

WHAT DOES A CSO DO?



Communicates

"across all levels"

Plans

"for desired results"

CSO

Assesses

"ability to react"

Leads

"high performing organization"

WHAT DOES A CSO DO?

- Protect & enhance revenue
- Provide board accountability
- Digest intelligence
- Set direction / change it
- Remove road-blocks
- Drive execution
- Mentor managers to become leaders

SIX DRIVING QUESTIONS

#1: MEASURING RISK

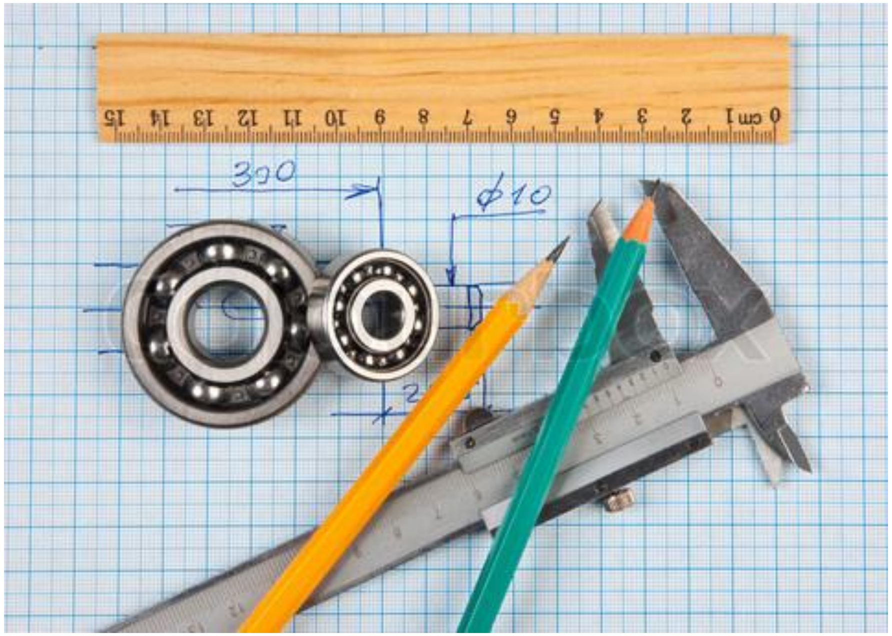
- How do you measure risk? Should risk management be driven by compliance? Technology? Audit? Vulnerabilities discovered in the field?

#2: BUSINESS INTERACTION

- How should the security function interact with business executives? Should the Board care? The CEO? Shareholders?

#3: TOOLS

- What tools do CSOs find useful in their own work? Are dashboards real? Do you have to build your own?



#4: PEOPLE

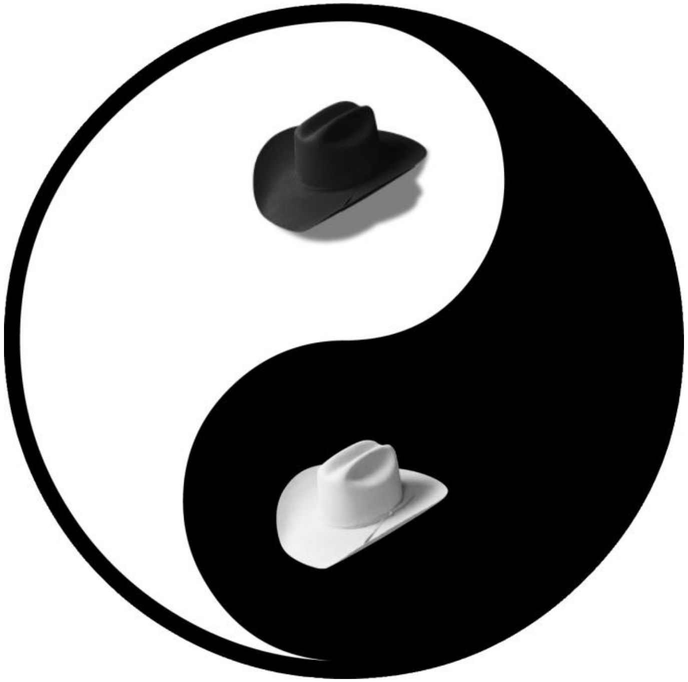
- How do you find and retain good security people?

#5: ROSI

- How do you figure out what levels of investment to make in securing the enterprise? Is return on security investment real or nonsense? How do you measure return?

#6: BUILDING SECURITY IN

- Should a CSO care about software security and building security in? How does a huge enterprise embrace security in development?



AUDIENCE QUESTIONS