

RSAC[®]Conference2015

San Francisco | April 20-24 | Moscone Center

SESSION ID: CXO-W01

IANIS Research - The 7 Factors of CISO Impact

Stan Dolberg

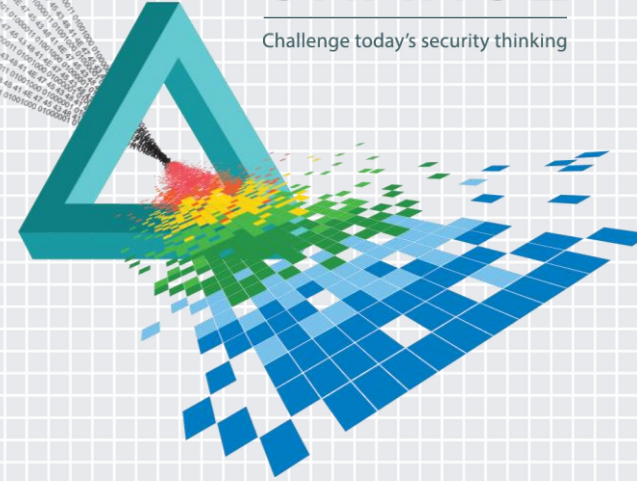
Head of Research
IANIS
@IANIS_Security

Phil Gardner

Co-Founder, Chief Executive Officer
IANIS
@IANIS_Security

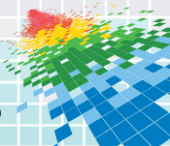
CHANGE

Challenge today's security thinking



“It is the mark of an educated mind to be able to entertain a thought without accepting it.”

Aristotle

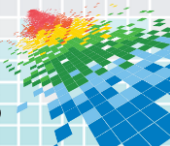
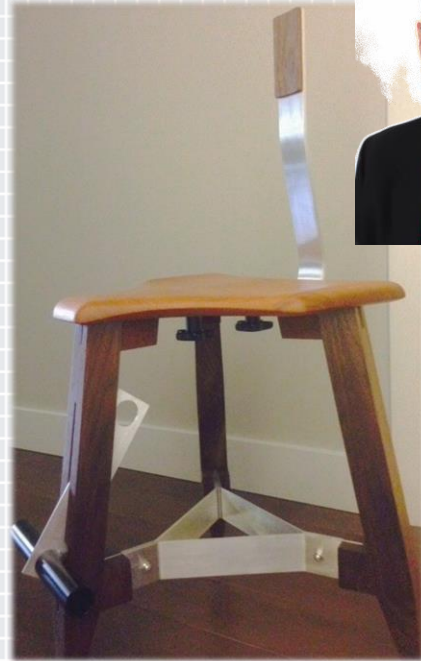




Phil



Stan

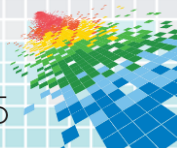


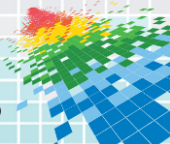
Institute for Applied Network Security

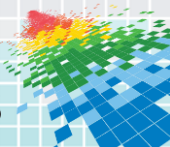
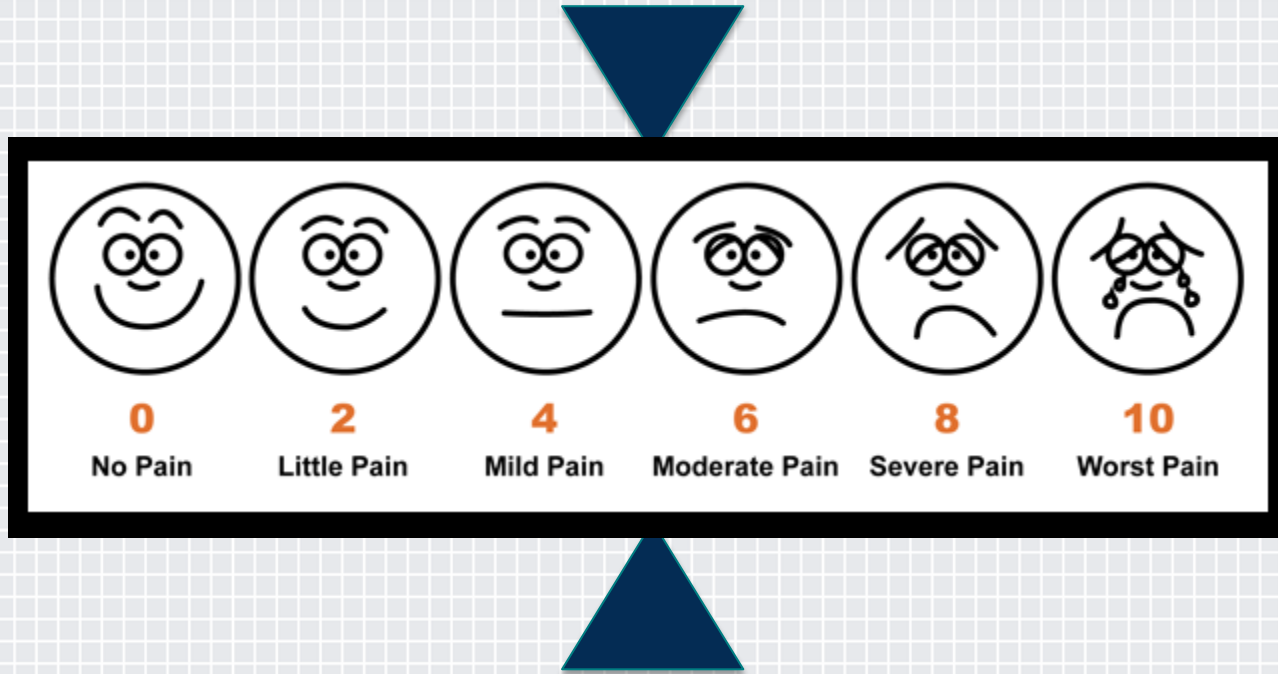


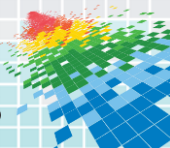
IANS

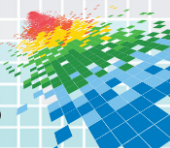
Helping information security
and IT risk professionals make
smarter decisions since 2001





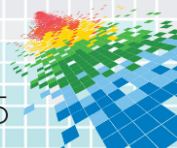


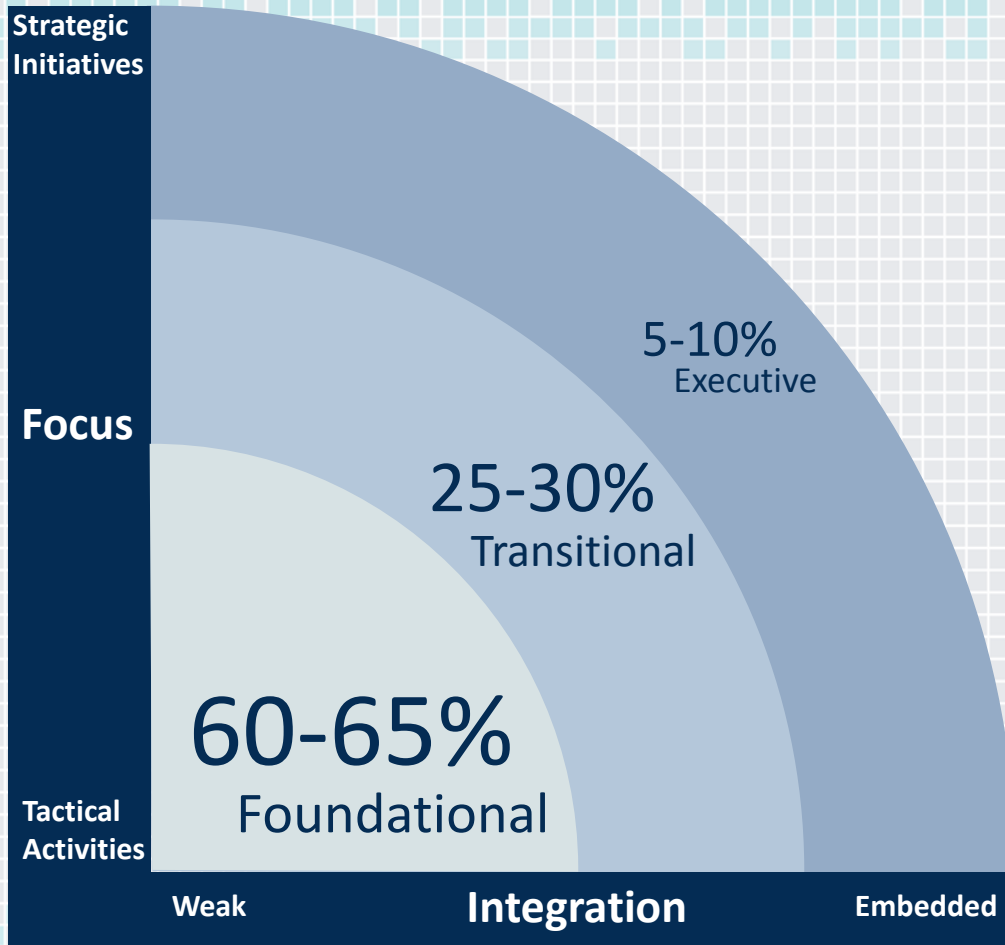




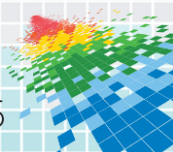


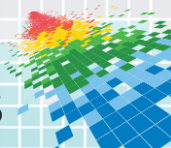
100+
FORTUNE 1000
CISOs

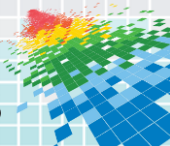


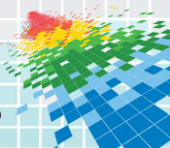
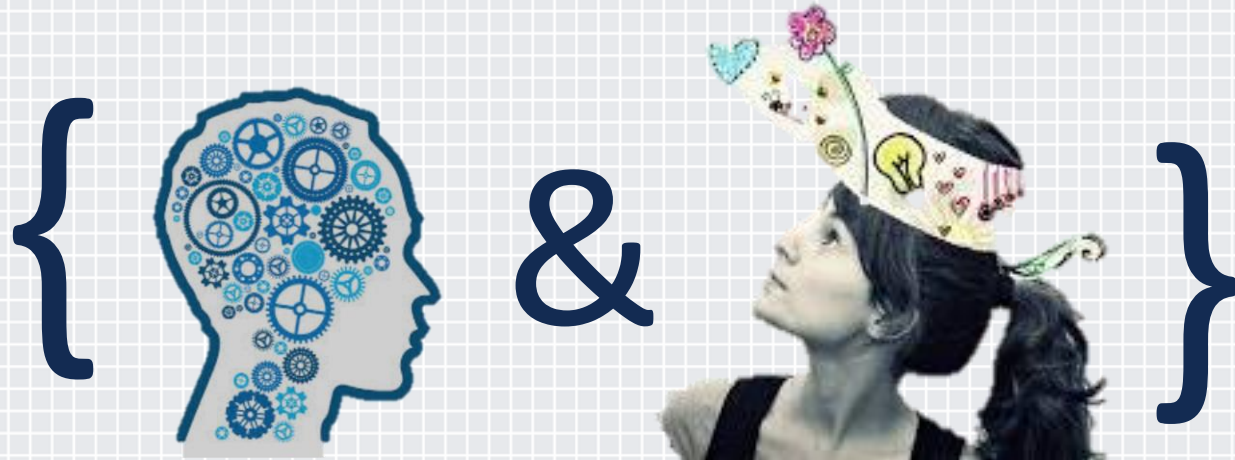


CISO Impact Quotient (CIQ)

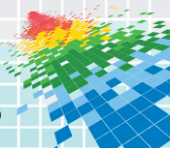




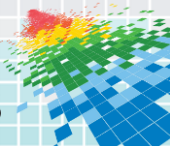




{ CISO Impact }

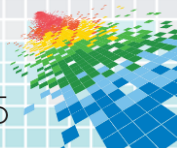


The 7 Factors of CISO Impact



CISO

THE PROMISE



THE PROMISE

... safeguard
information
assets across
space and
time

THE 'BUT'

... don't
control
most of the
resources

THE 'GOTTA'

... master
proactive
engagement
with the
business

Progress Starts with Assessment

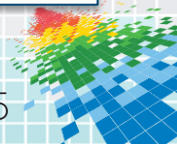
Information Security
Organizational Engagement

CISO Impact

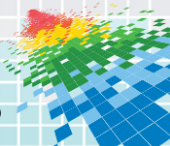
Technical Infrastructure
Information Security
Control Strength

Assessment Standards:

- ISO 27001
- NIST
- COBIT 5
- ...



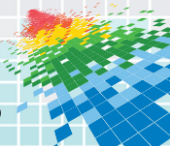
{CISO Impact}



CISO Impact Diagnostic



Over 400 Completes in 200 days
75% Fortune 1000
1000 Completes EOY 2015



Defense / Military

Public Sector / Non-Profit

Energy

Retail



Services

Finance

Health

Mfg

Transportation

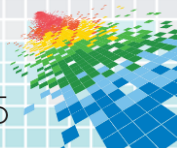
Technology

Telecom

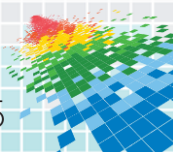
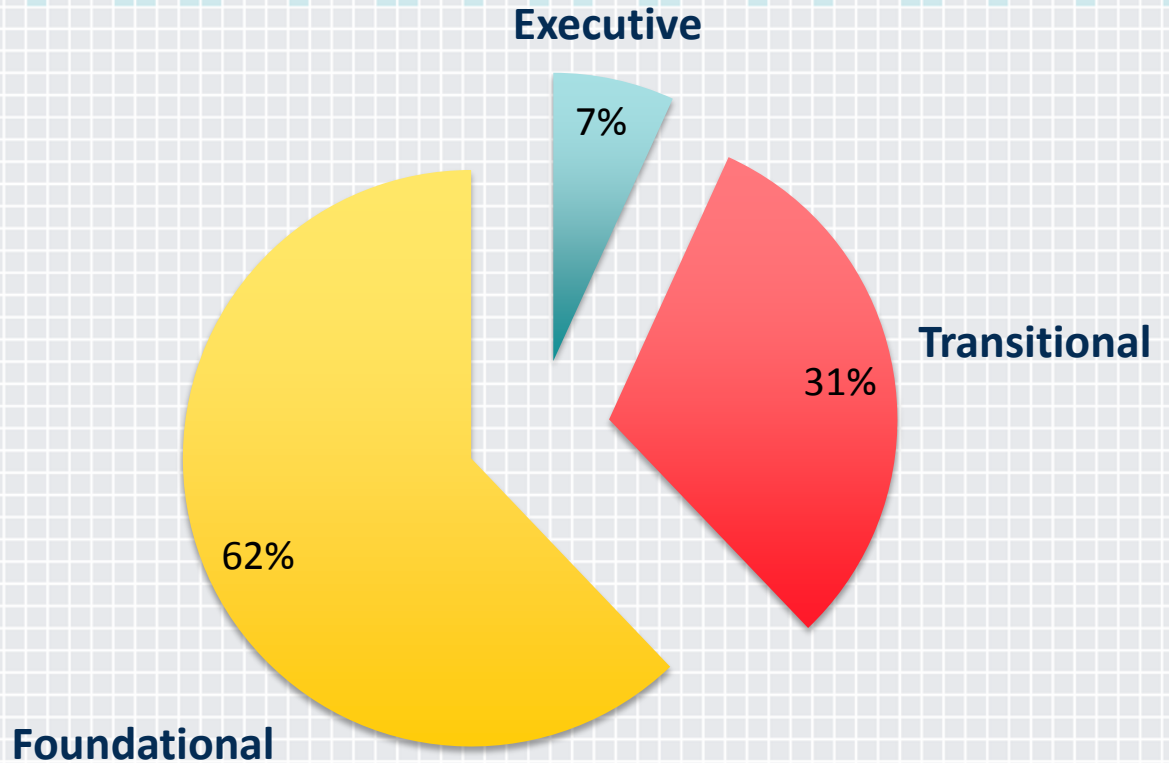
Healthcare

Manufacturing

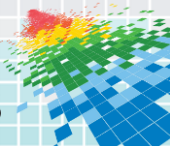
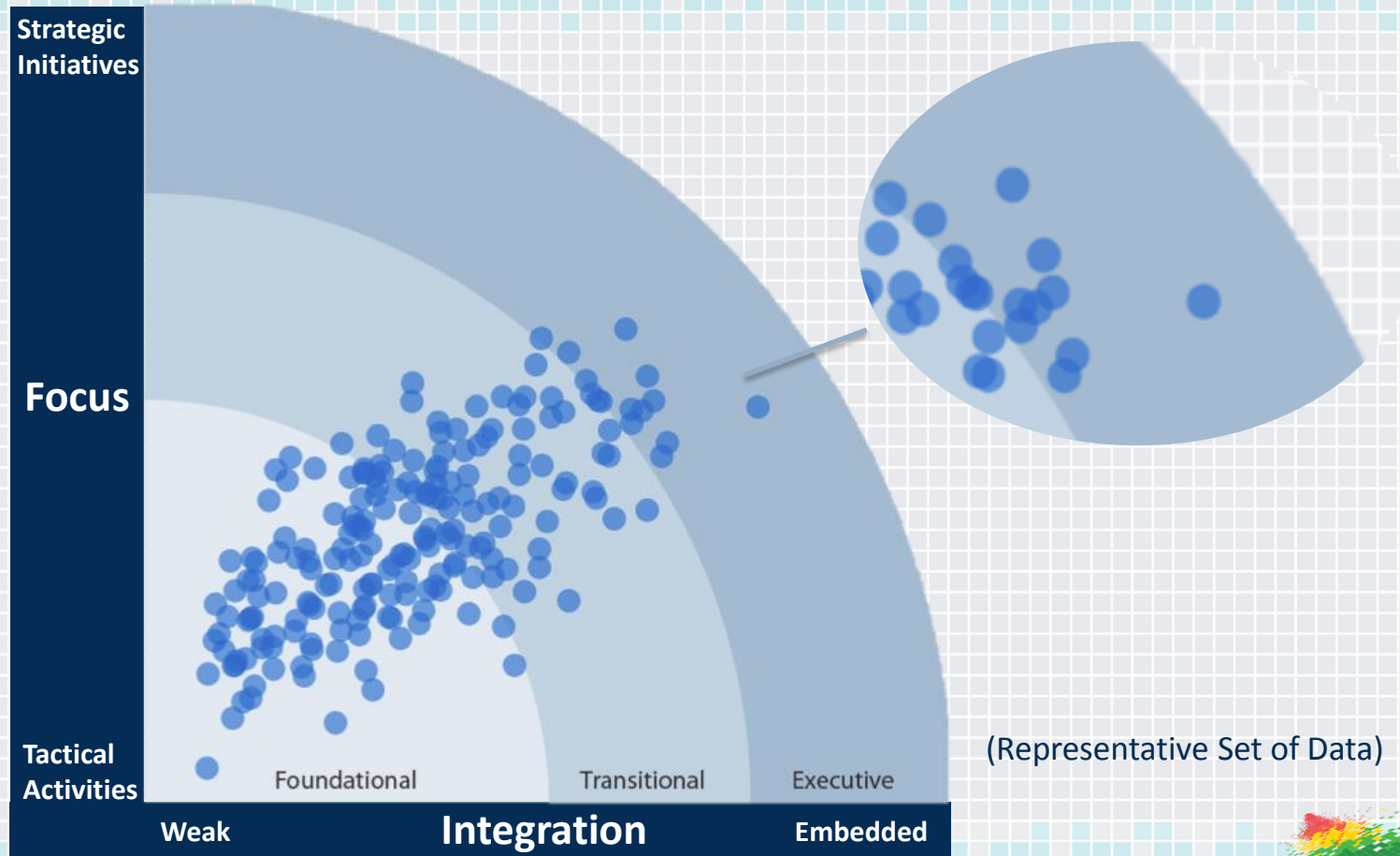
Financial Services



CISO Impact Data



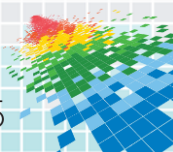
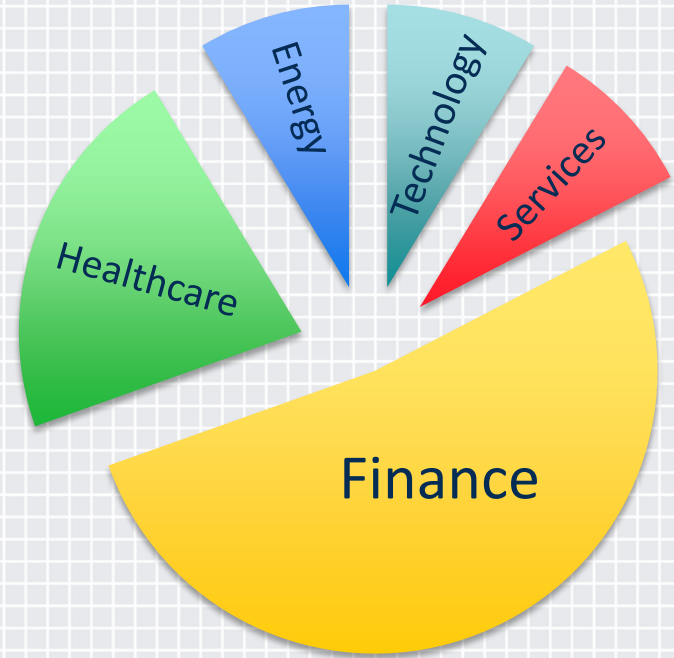
CISO Impact Quotient (CIQ)



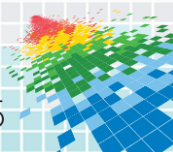
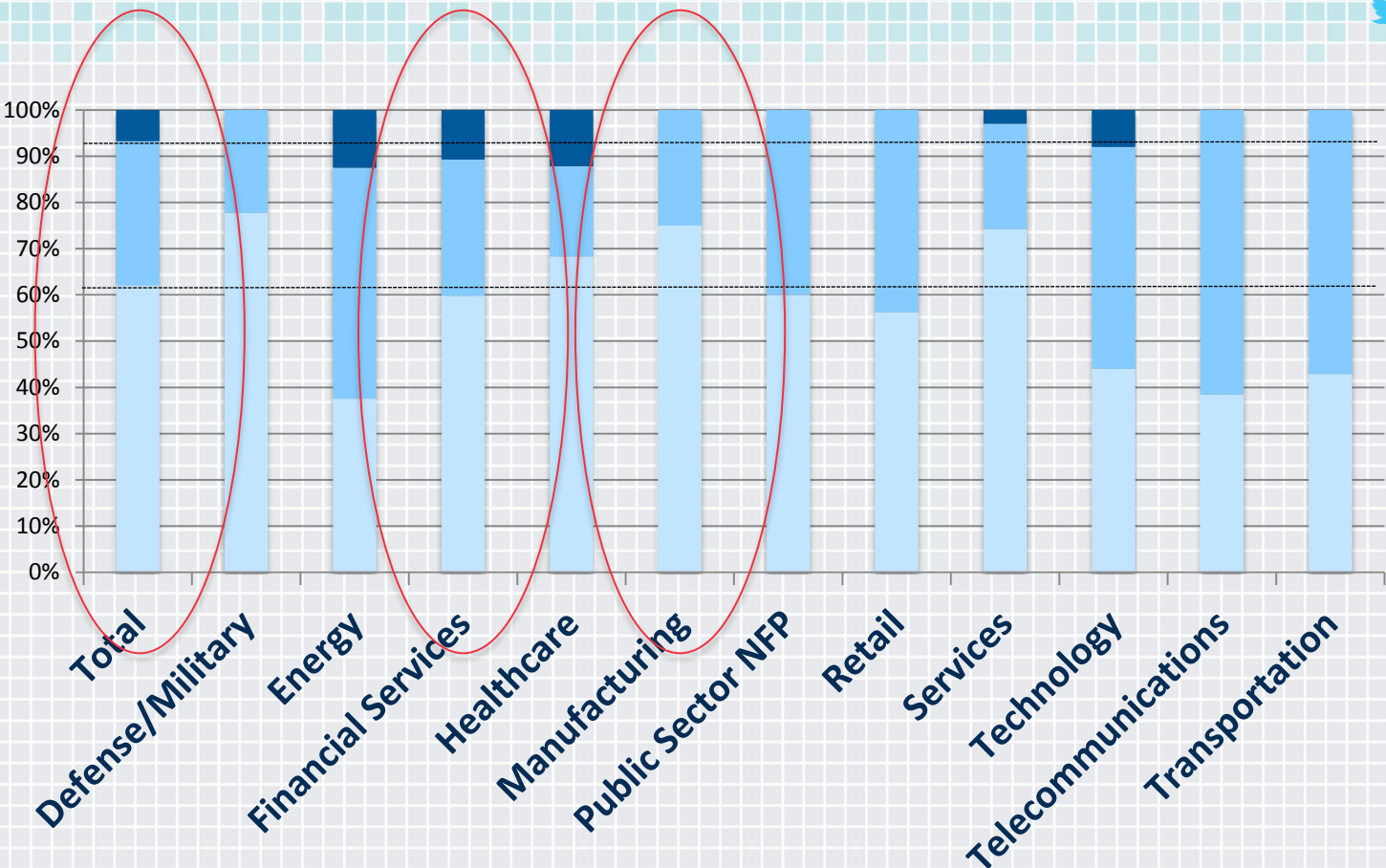
Breaking down the

7% of CISO Impact diagnostics that scored

Executive



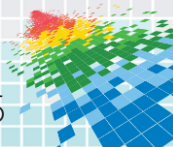
Executive
Transitional
Foundational



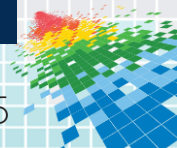
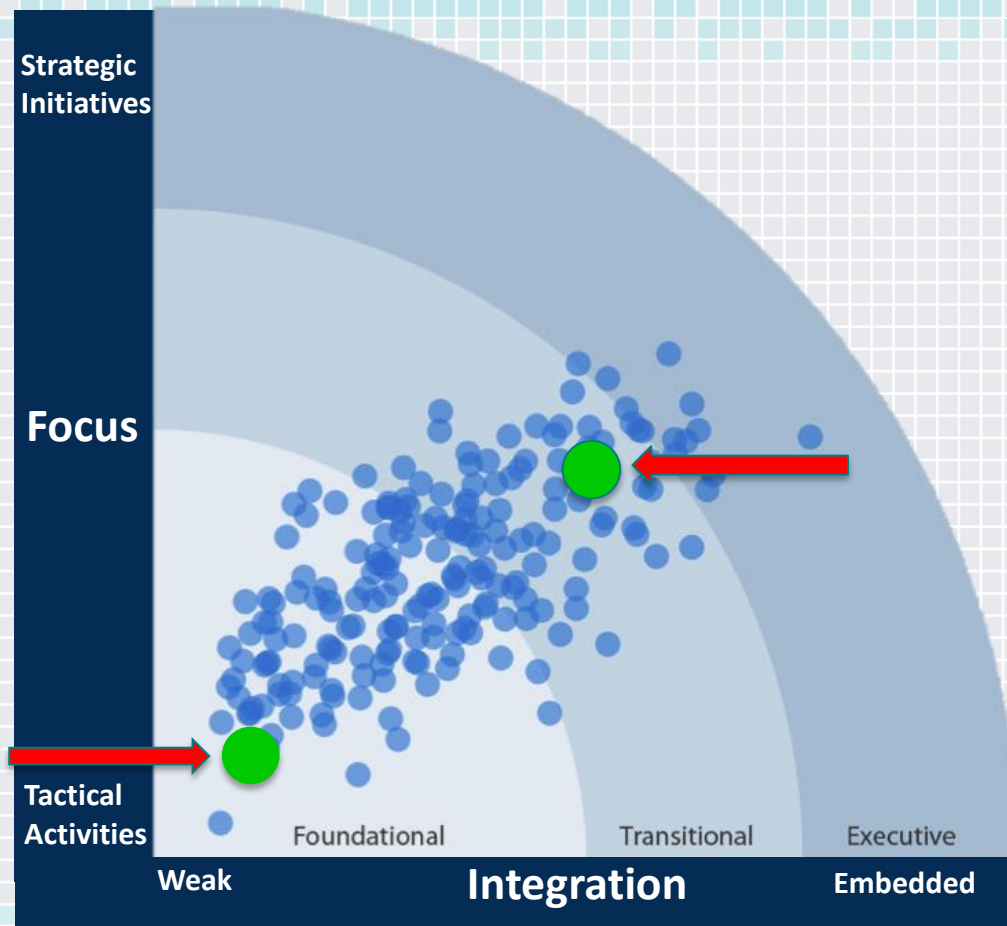
32% of respondents are
in **Financial Services...**

...yet **Financial Services** comprises

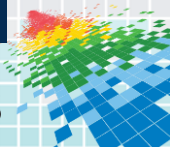
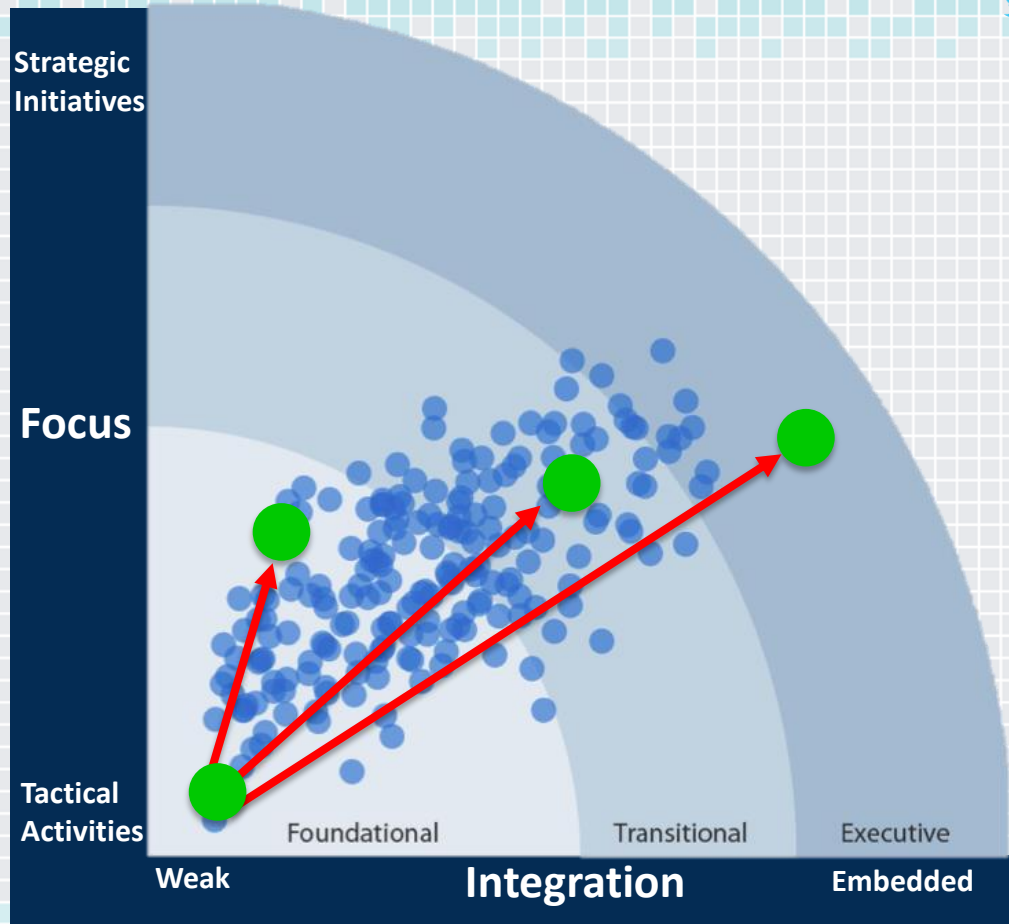
52% of **Executive CIQ**



What's Your CISO Impact Quotient (CIQ)?

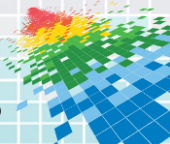


What's Your CIQ Goal?

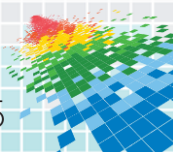
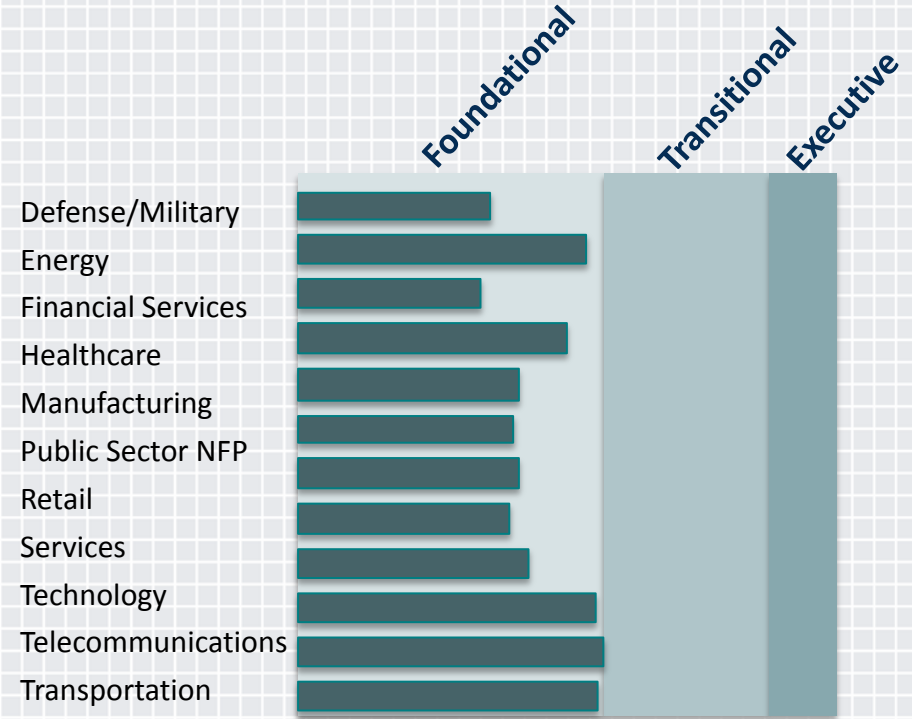


Factor 1: Gain Command of the Facts

- ✓ Acquire the data on information assets to support a company-specific risk profile
- ✓ Build a consensus with the business on what matters and on the impact of compromise
- ✓ Develop a robust planning tool including company and industry data to provide an outlook



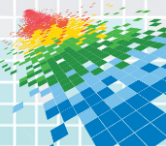
Who has Command of the Facts?



Factor 2: Get Business Leaders to Own Risk



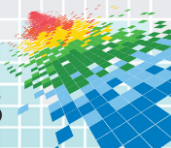
- ✓ Educate / advocate for the mind-shift that business owns InfoSec risk
- ✓ Build key alliances with the business to gain a foothold
- ✓ Run exercises, games, and simulations to make it personal
- ✓ Develop strong stewardship policies and follow-through tools



...walking the tightrope

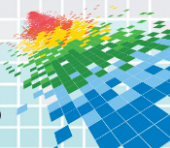


Alan Weber / AP

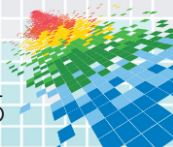


Factor 3: Embed into Key Processes

- ✓ Embed safe coding practices into software development processes
- ✓ Wire criteria into vendor due diligence
- ✓ Build consultations into new business initiatives
- ✓ Work your way to the front-end of mergers and acquisitions



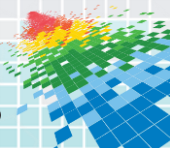
Technology
Manufacturing
Defense

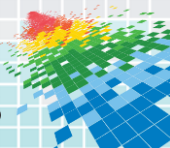


Factor 4: Run Infosec Like a Business



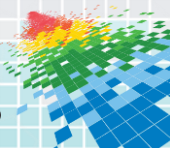
- ✓ Develop financial discipline to tie budgets to business impact
- ✓ Culture sophisticated resource management skills
- ✓ Build strong project management capabilities within InfoSec





Factor 5: Technical and Business-Capable Team

- ✓ Change the game with competency models that balance technical, business, and interpersonal skills
- ✓ Apply models & lay out career paths to retain those who can represent the CISO
- ✓ Invest in leadership and management development for the CISO and directs



Conflict resolution

Creative

Strong Communicator
& Listener

Humor

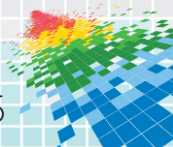


Positive


Story teller

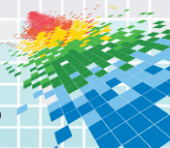
Collaboration

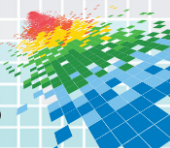
Able to execute



Factor 6: Communicate the value

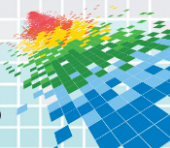
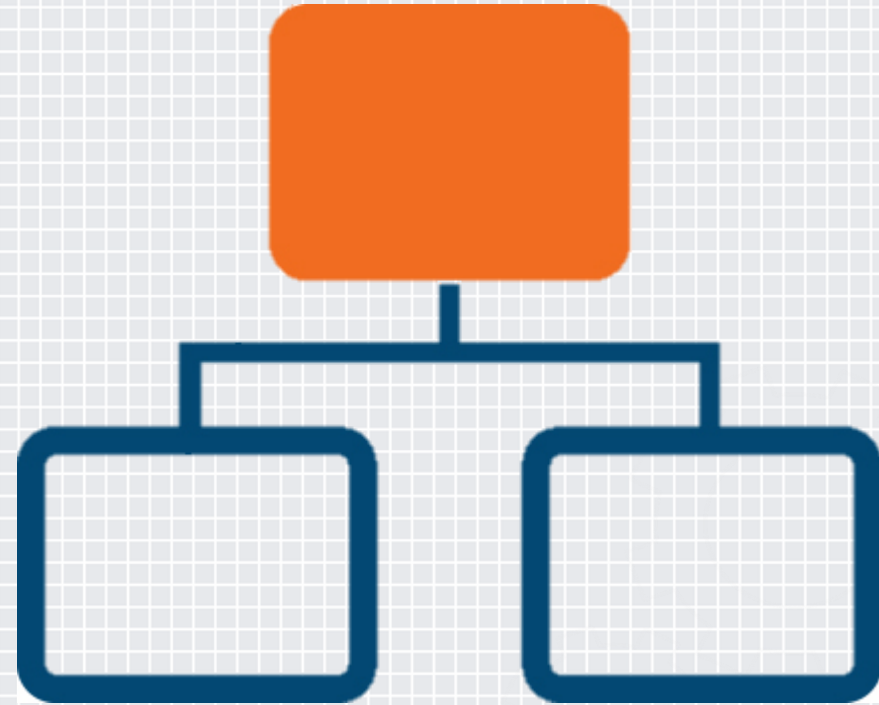
- 
- ✓ Build a value proposition for how InfoSec helps the company grow and win
 - ✓ Proactively and consistently communicate that value
 - ✓ Engage with stakeholders to learn how to express the value in terms with meaning to *them*





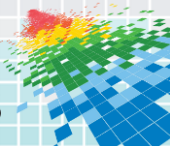
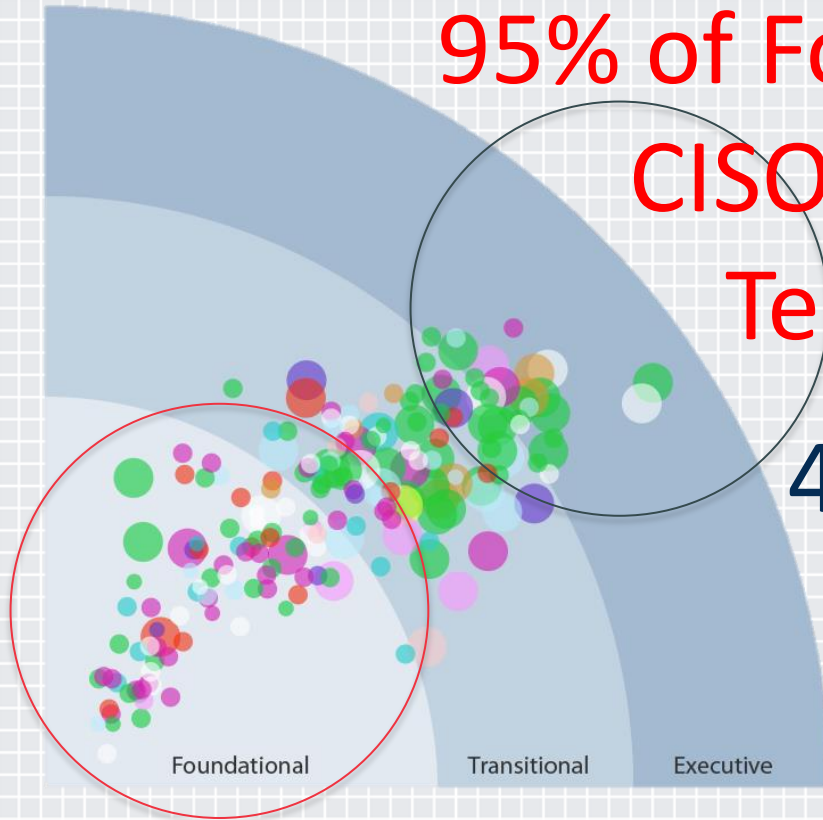
Factor 7: Organize for Success

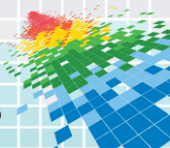
- ✓ How stretched thin is InfoSec between day to day ops and strategy / policy / architecture?
- ✓ CISO and BISO reporting? Technology?
- ✓ Dotted line reporting outside tech?
- ✓ Mechanisms that put CISO and team in direct contact with leaders?



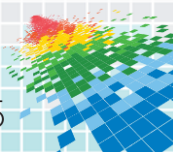
95% of Foundational
CISOs Report to
Technology

40% of Executive
CISOs Report
to Technology

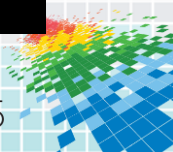
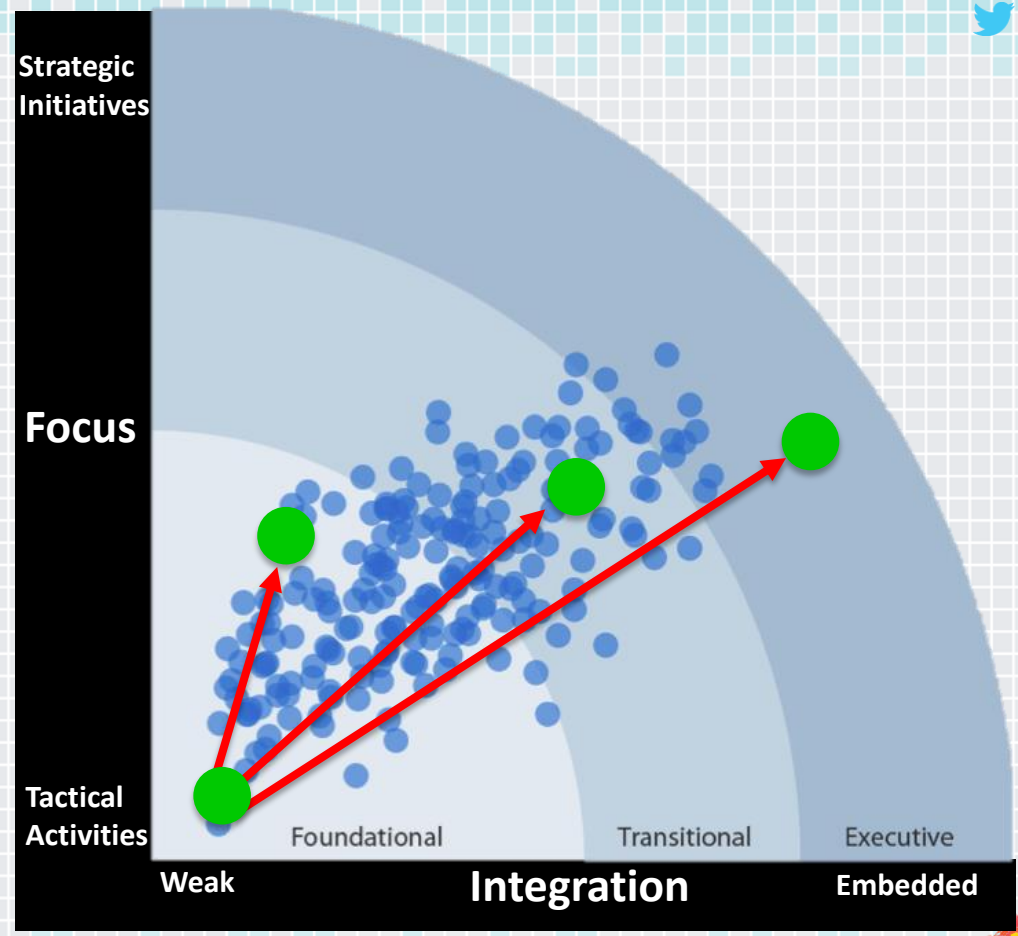




The 7 Factors of CISO Impact



What's Your CIQ Goal (now)?

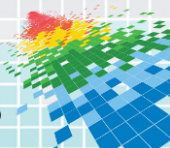


Take the CISO Impact Diagnostic

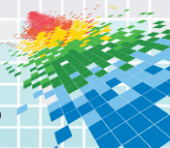
Embark on your CISO Impact Journey

- ◆ 25 questions / 20 minutes
- ◆ Get instant feedback on how you measure up in your industry
- ◆ Register to get an in-depth report

<https://rsa.iansresearch.com/>



<https://rsa.iansresearch.com/>



THANK YOU

Questions?

