RSAConference2015

San Francisco | April 20-24 | Moscone Center

CHANGE

Challenge today's security thinking

SESSION ID: CXO-W01

IANS Research - The 7 Factors of CISO Impact

Stan Dolberg

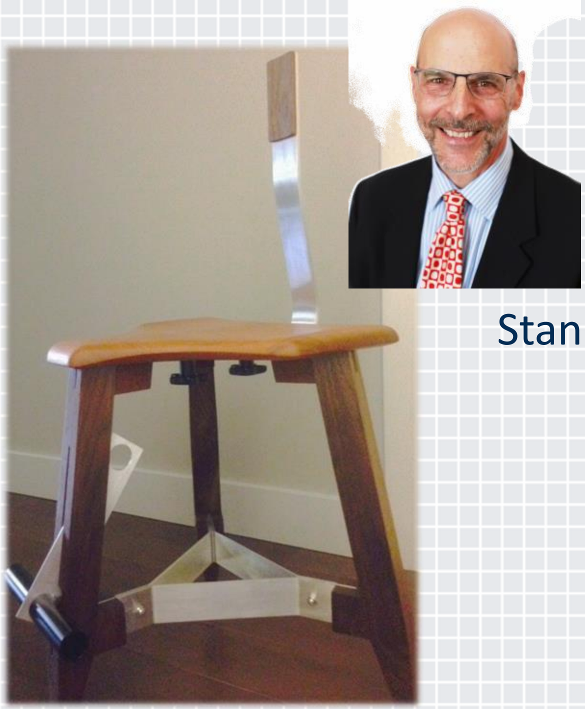
Head of Research
IANS
@IANS_Security

Phil Gardner

Co-Founder, Chief Executive Officer
IANS
@IANS_Security

#RSAC

Phil

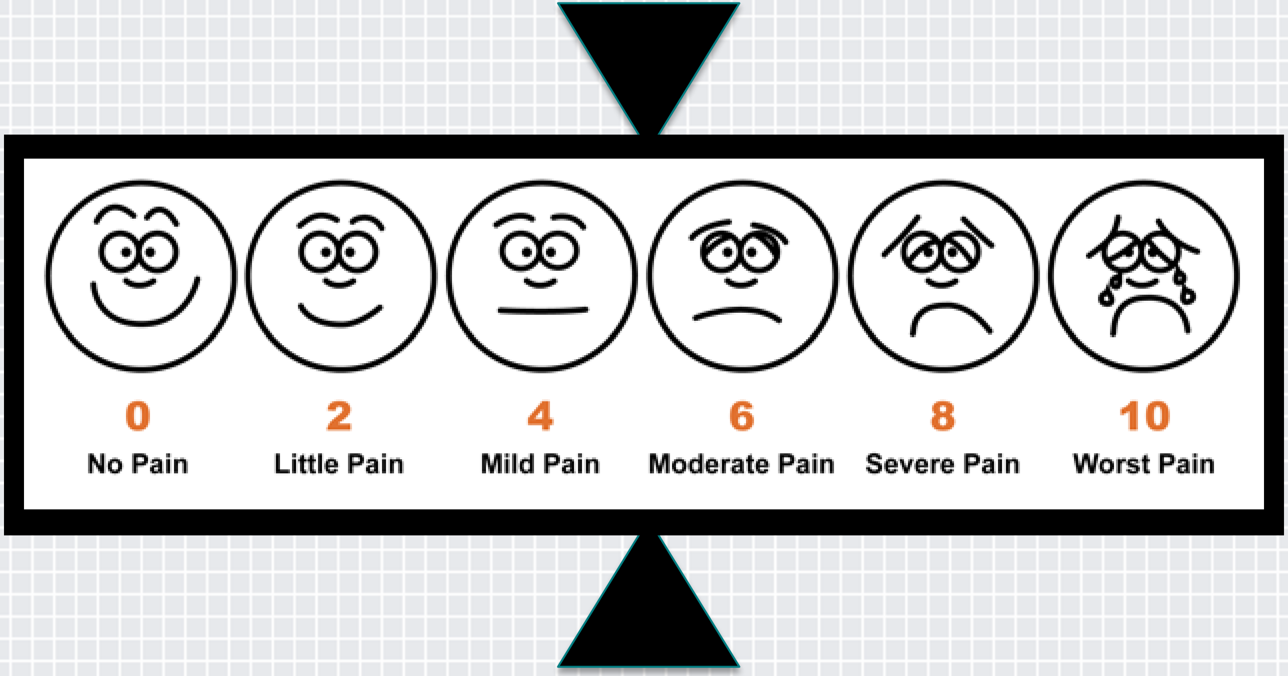


Stan

Institute for Applied Network Security

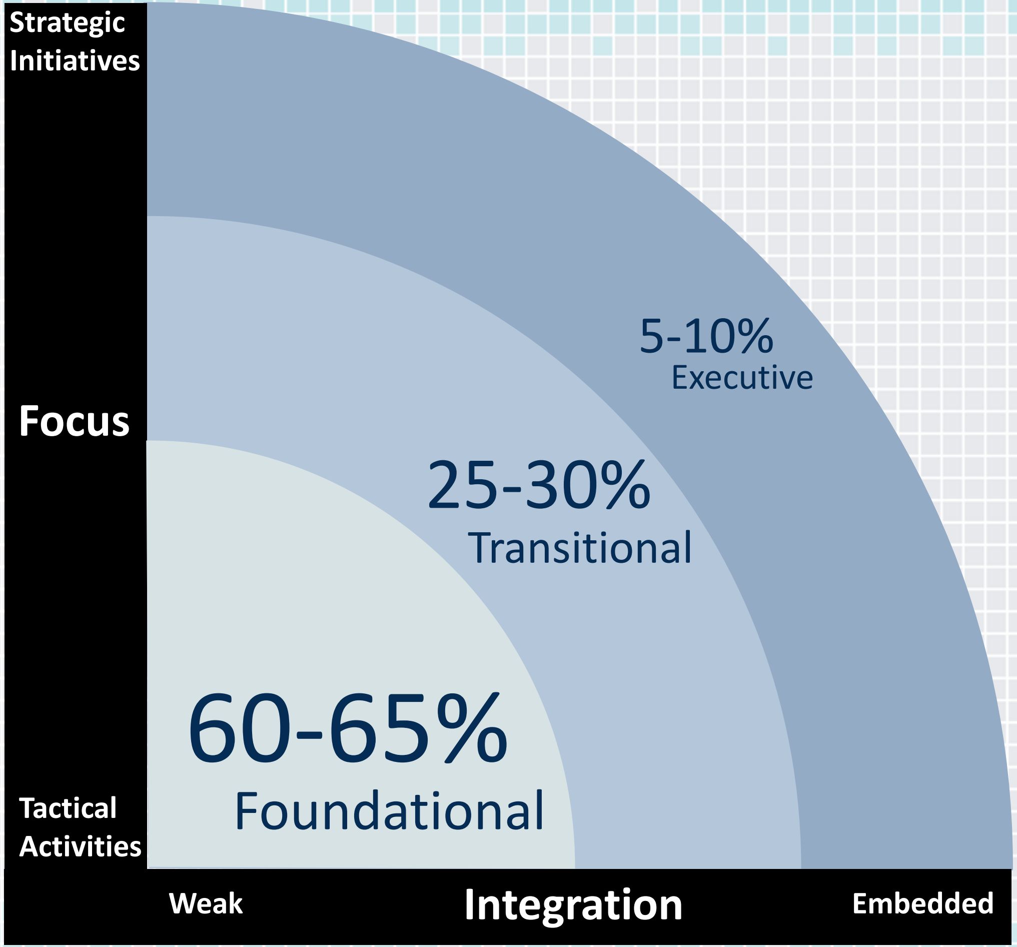
IANS

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


0
No Pain
2
Little Pain
4
Mild Pain
6
Moderate Pain
8
Severe Pain
10
Worst Pain

?

100+
FORTUNE 1000
CISOs


Strategic Initiatives
Focus
Tactical Activities
5-10%
Executive
25-30%
Transitional
60-65%
Foundational
Weak
Integration
Embedded

!

{ & }

{ CISO Impact }

The 7 Factors of CISO Impact

CISO

THE PROMISE

▲

THE 'GOTTA'

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

CISO Impact!

How does progress begin? 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

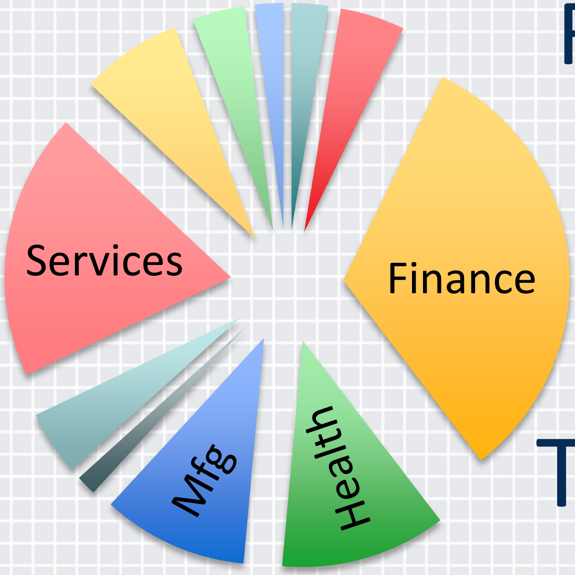
1000 Completes EOY 2015

Defense / Military

Public Sector / Non-Profit

Retail

Energy



Services

Financial Services

Technology

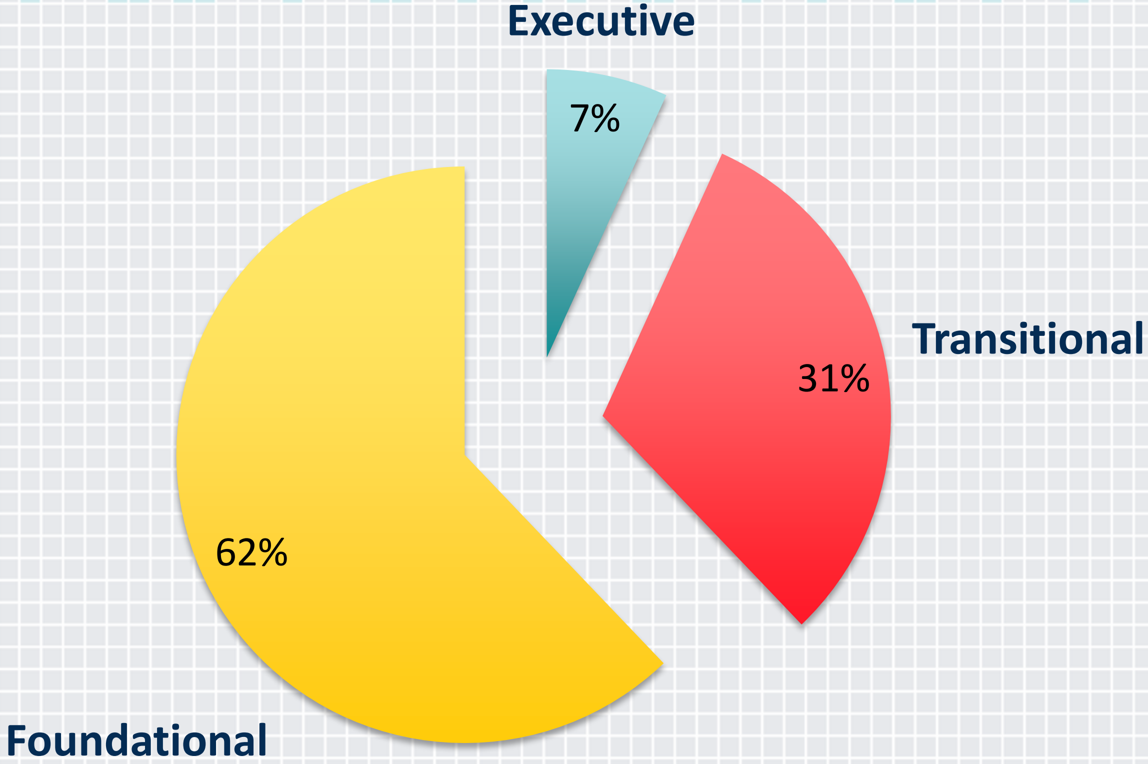
Healthcare

Manufacturing

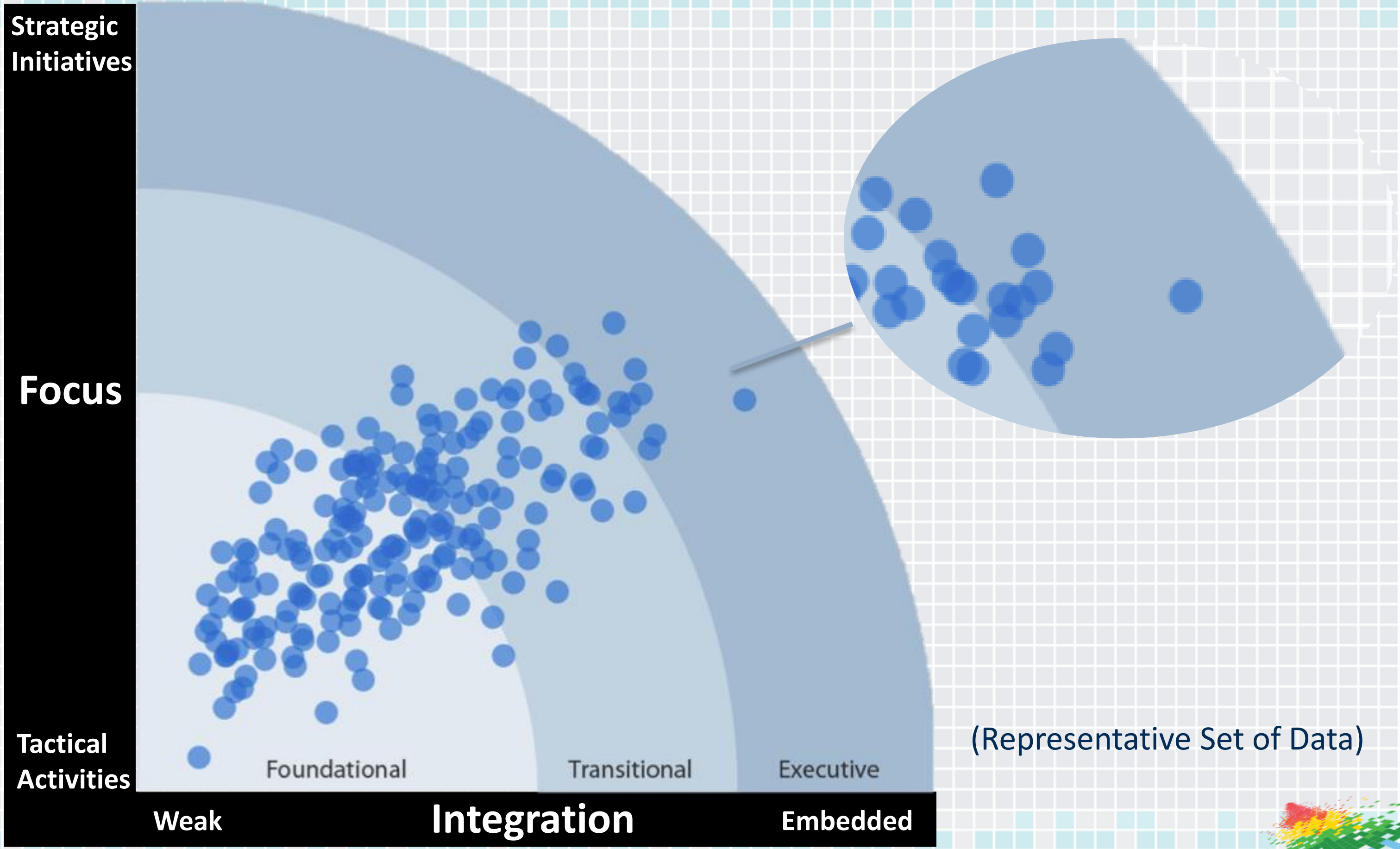
Transportation

Telecom

CISO Impact Data



CISO Impact Quotient (CIQ)

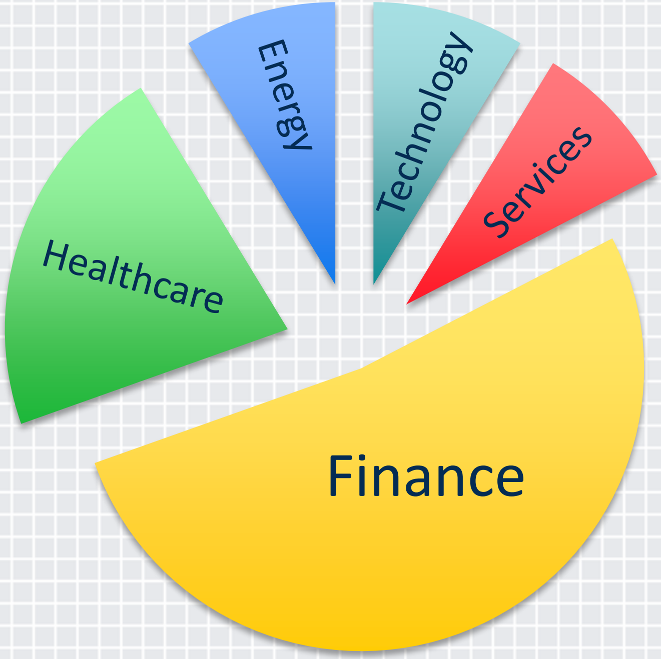


(Representative Set of Data)

Breaking down the

7% of CISO Impact diagnostics that scored

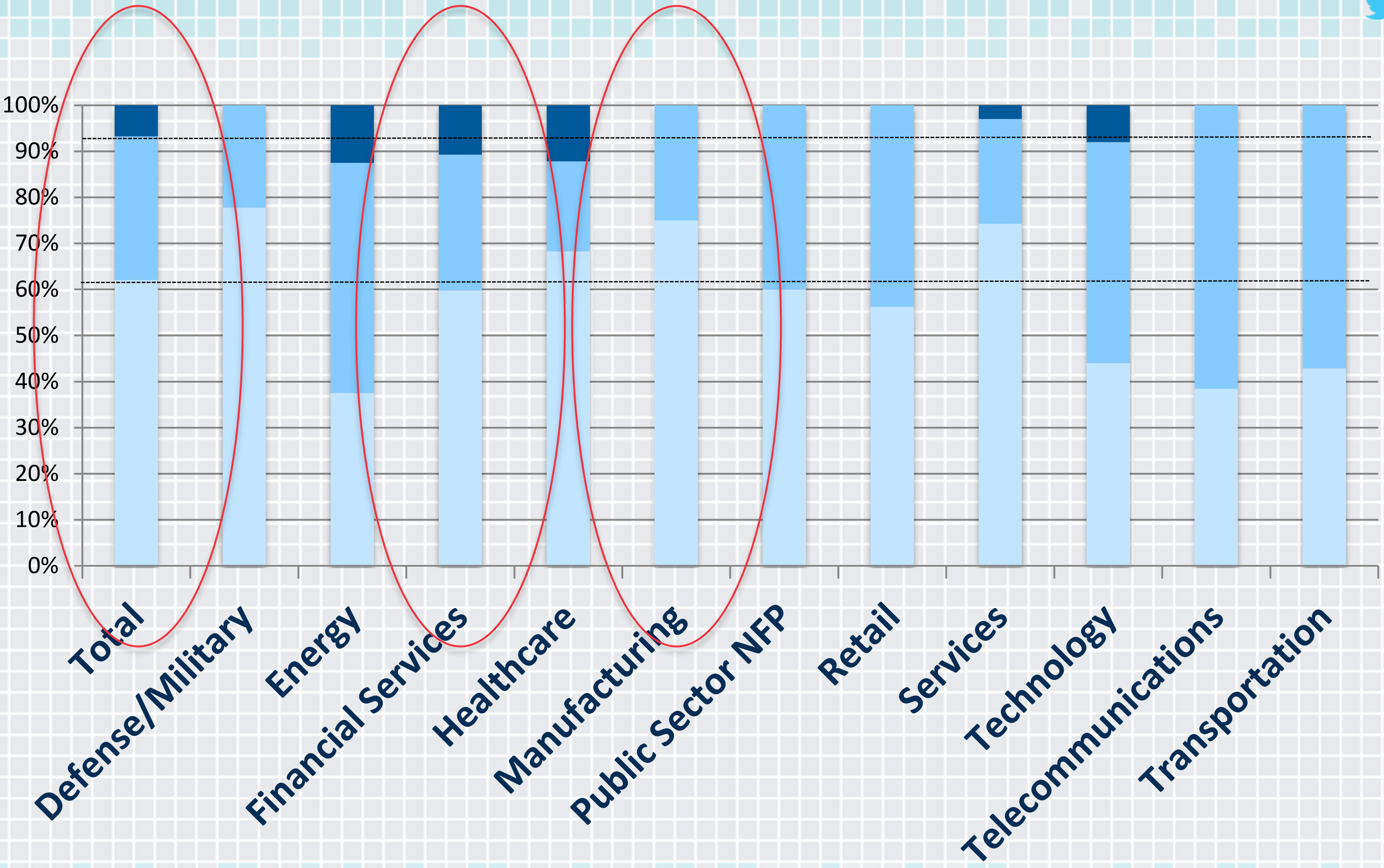
Executive



Executive

Transitional

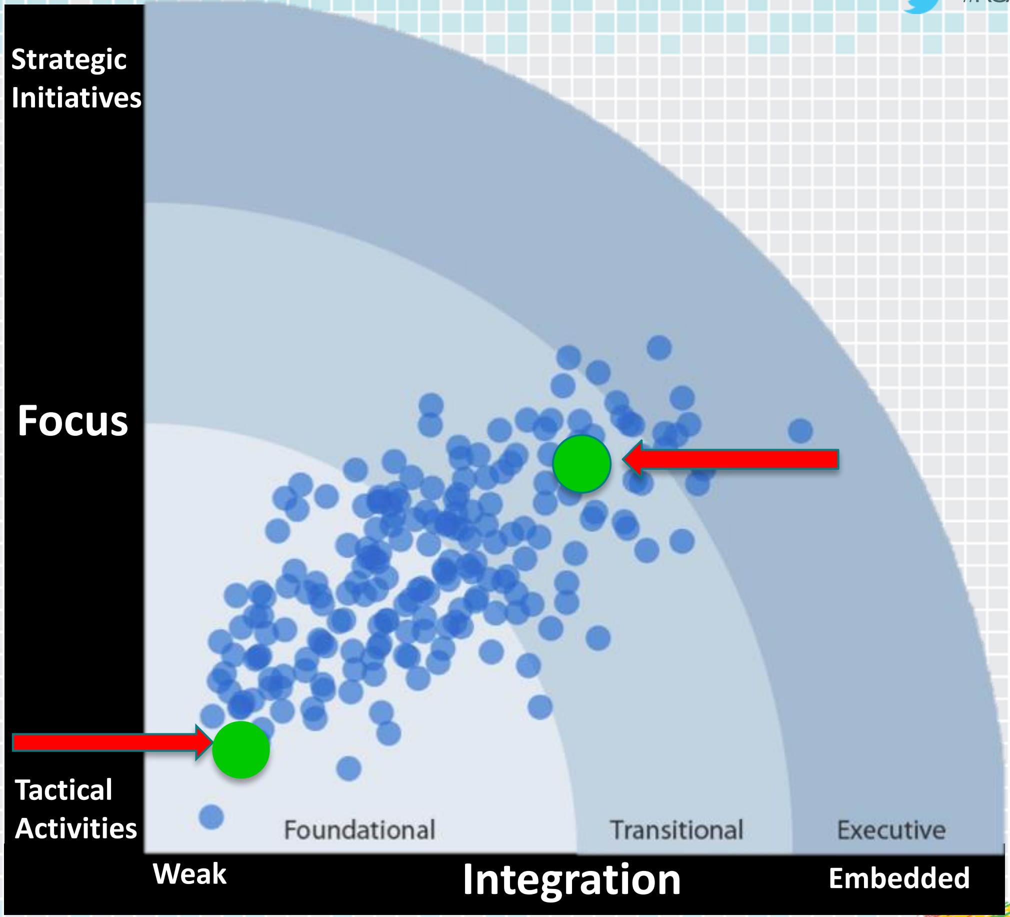
Foundational



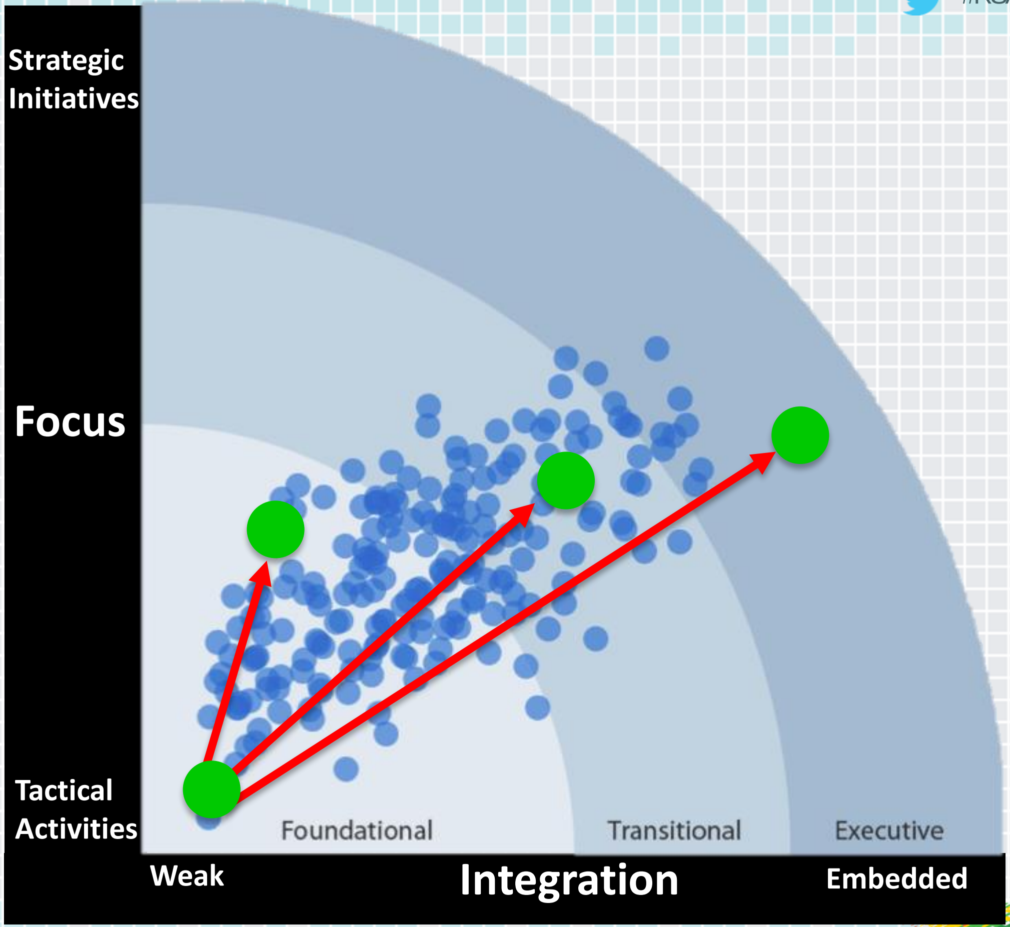
32% of respondents identify as **Financial Services…**

…yet Financial Services comprises **52%** **of Executive CIQ**

What's Your CISO Impact Quotient (CIQ)?



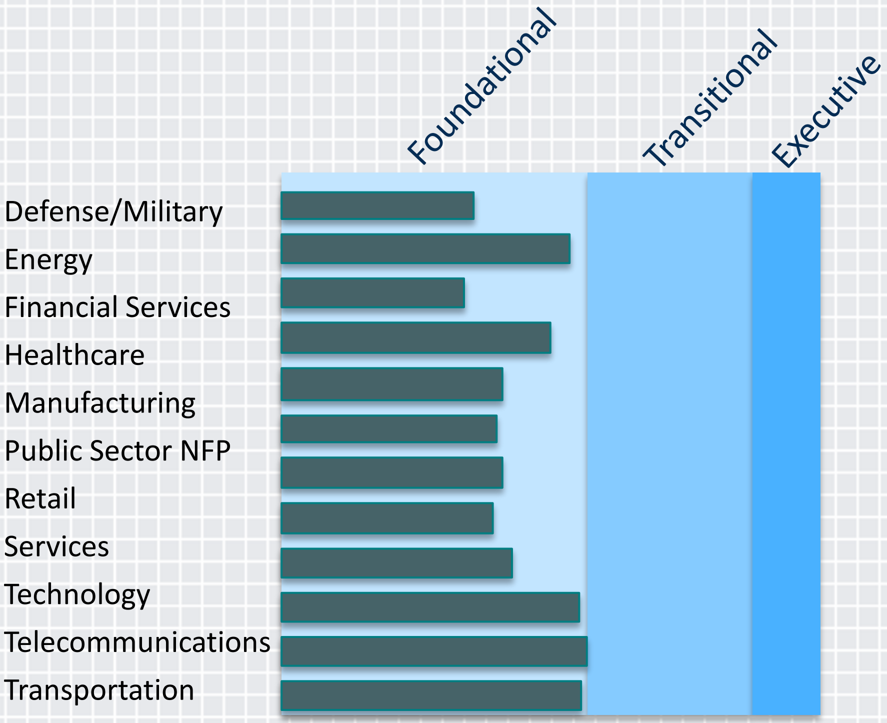
What's Your CIQ Goal?



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

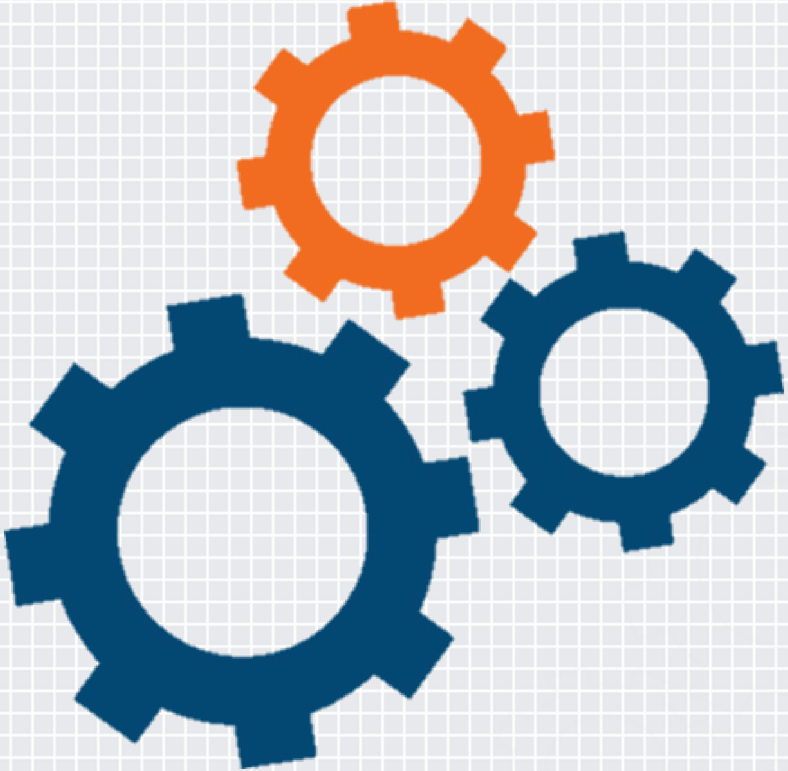
- ✓ Educate / advocate for the mind-shift that business owns InfoSec risk
- ✓ Build key alliances with the business to gain a foothold
- ✓ Run exercises, games, and simulations to make it personal
- ✓ Strong stewardship policy and follow-through tools

Alan Welner / AP

Man on Wire

Factor 3: Embed into Key Processes

- ✓ Embed safe coding practices into software development processes
- ✓ Wire criteria into vendor due diligence
- ✓ Build gates and 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 build budgets tied 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

Creativity

Strong communications / Listening Skills - People who can “see gray” - ambiguity

Conflict resolution

Positive

Humor

Context – the ability to be a story teller

Collaboration

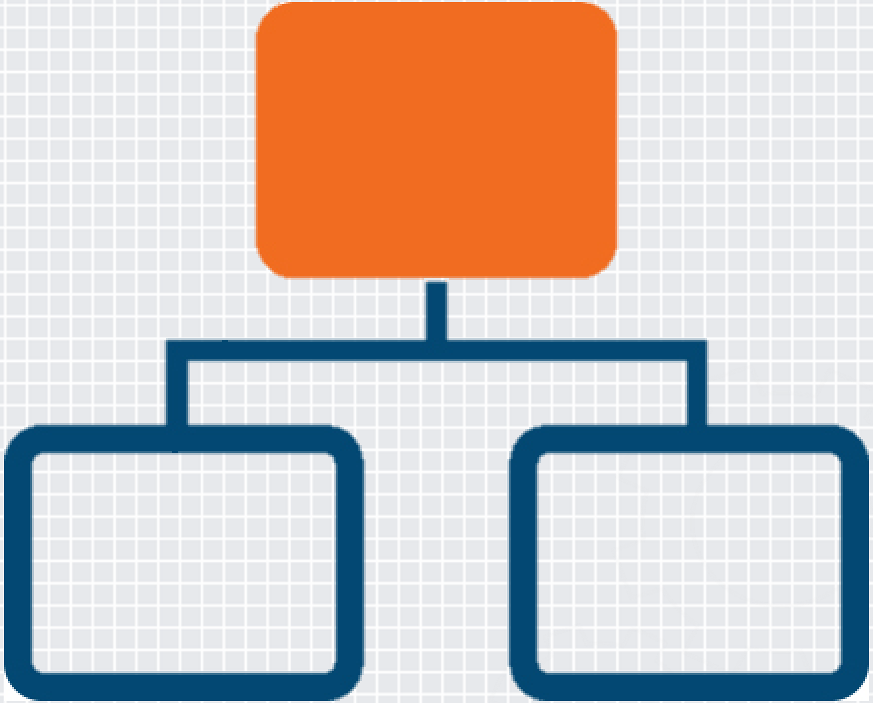
Ability to execute

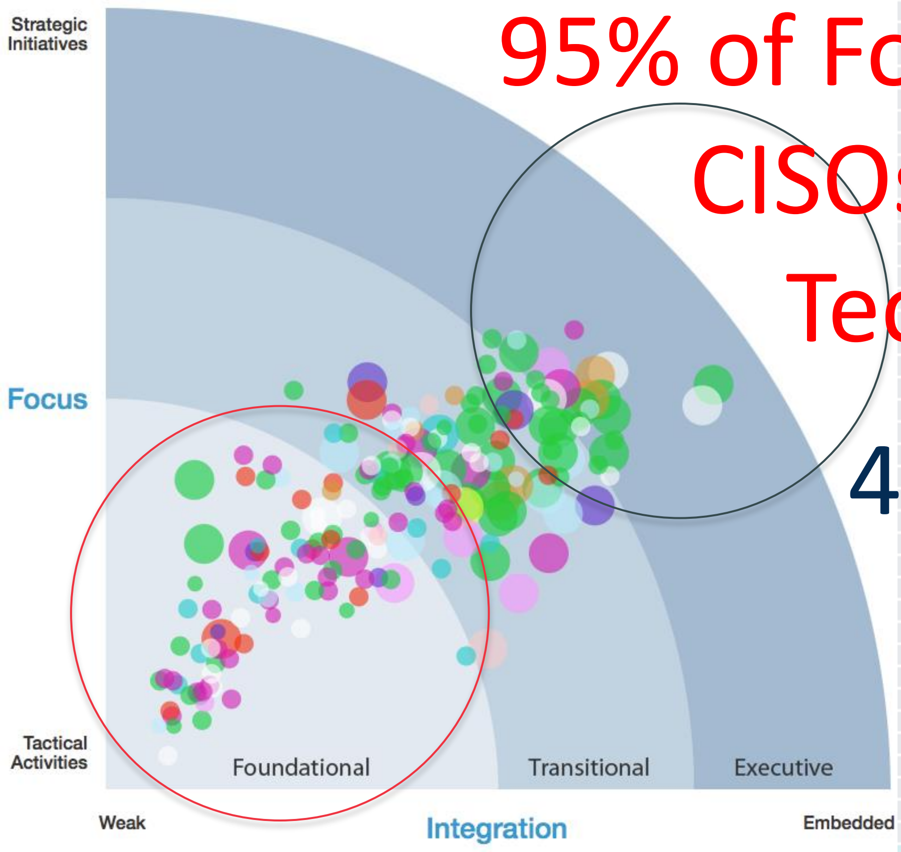
Factor 6: Communicate the value

- ✓ 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 that have 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? Tech?
- ✓ 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

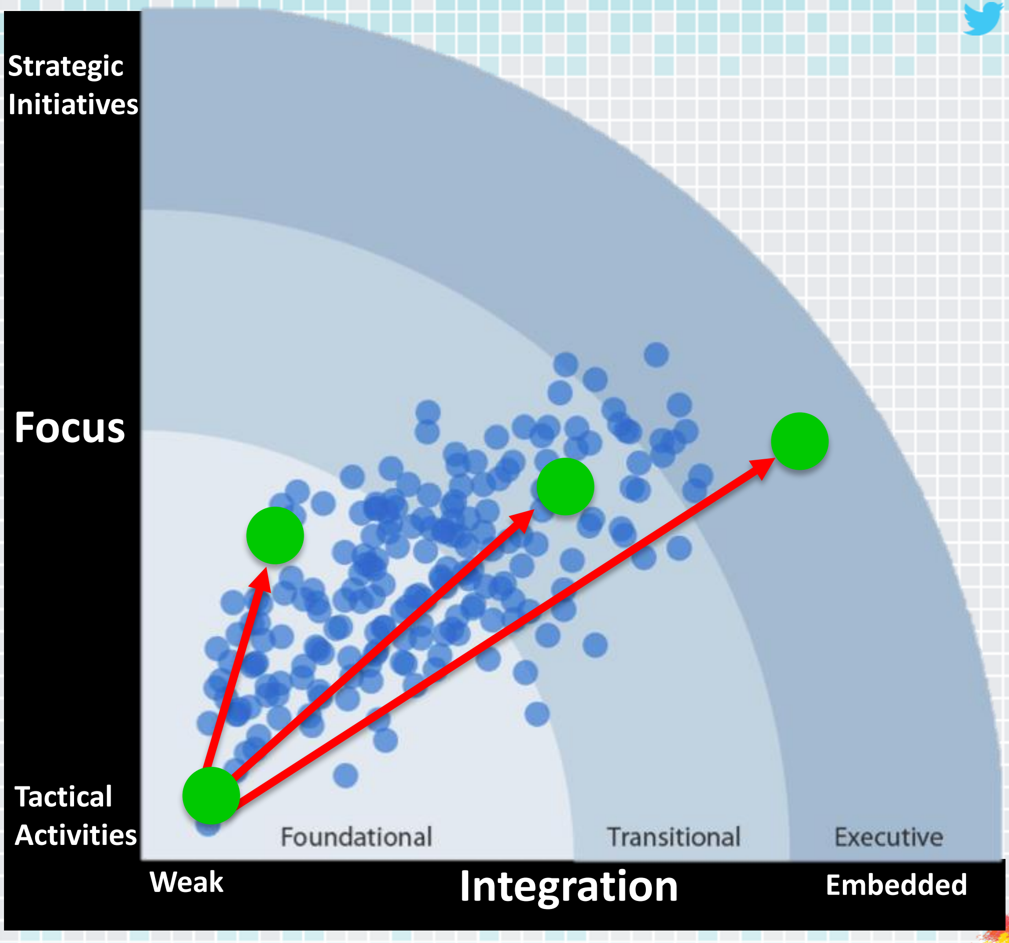
{

&

}

The 7 Factors of CISO Impact

What's Your CIQ Goal?



Embark on Your CISO Impact Journey

Take the CISO Impact Diagnostic

- 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/

In their own words:

[CISO Impact]… "tells me how to engage the organization around how/where the decision is made."

"I think it's pure gold to have the CISO Impact Diagnostic taken by my C-Level execs."

"This will help me grow my position and professional development so that I can have a greater impact."

"I am continually asked by the board: 'How do we compare to our peers'?"

"… we expected to be above the norm in everything, because we actually have budget to fund resources. But this showed we still have gaps…"

"This answers the question of where should I be investing on this team?"

THANK YOU