Security in knowledge

PLAYING THE GAME OF THRONES: ENSURING THE CISO's ROLE AT THE KING'S TABLE

Thom Langford (@thomlangford)

Sapient

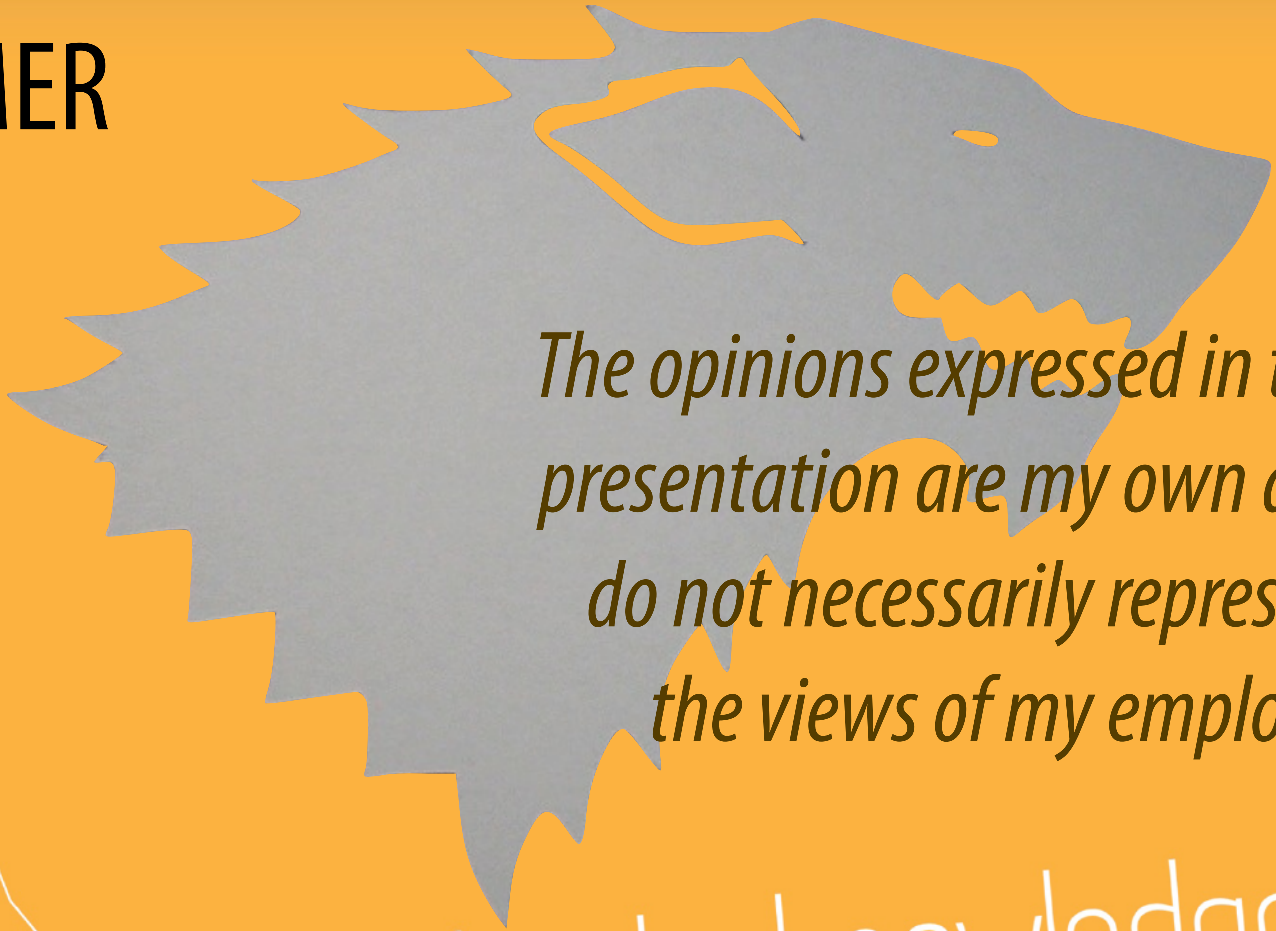
RSACONFERENCE
EUROPE 2013

#RSAC

Session ID: GRC-R08

Session Classification: Intermediate

DISCLAIMER



The opinions expressed in this presentation are my own and do not necessarily represent the views of my employer

Security in knowledge

#RSAC @thomlangford

WHY ARE WE HERE?

Security in knowledge

BECAUSE WE DON'T OWN A PAIR OF THESE

rose-tinted security:
budget love

Source (i)

IN THE GAME OF THRONES...

A QUESTION OF DEFINITION

Security in knowledge

#RSAC @thomlangford

RSA CONFERENCE EUROPE 2013

WHO ARE WE TALKING ABOUT?

Head of Security

Chief Information

I.T. Security

CISO

Business Continuity

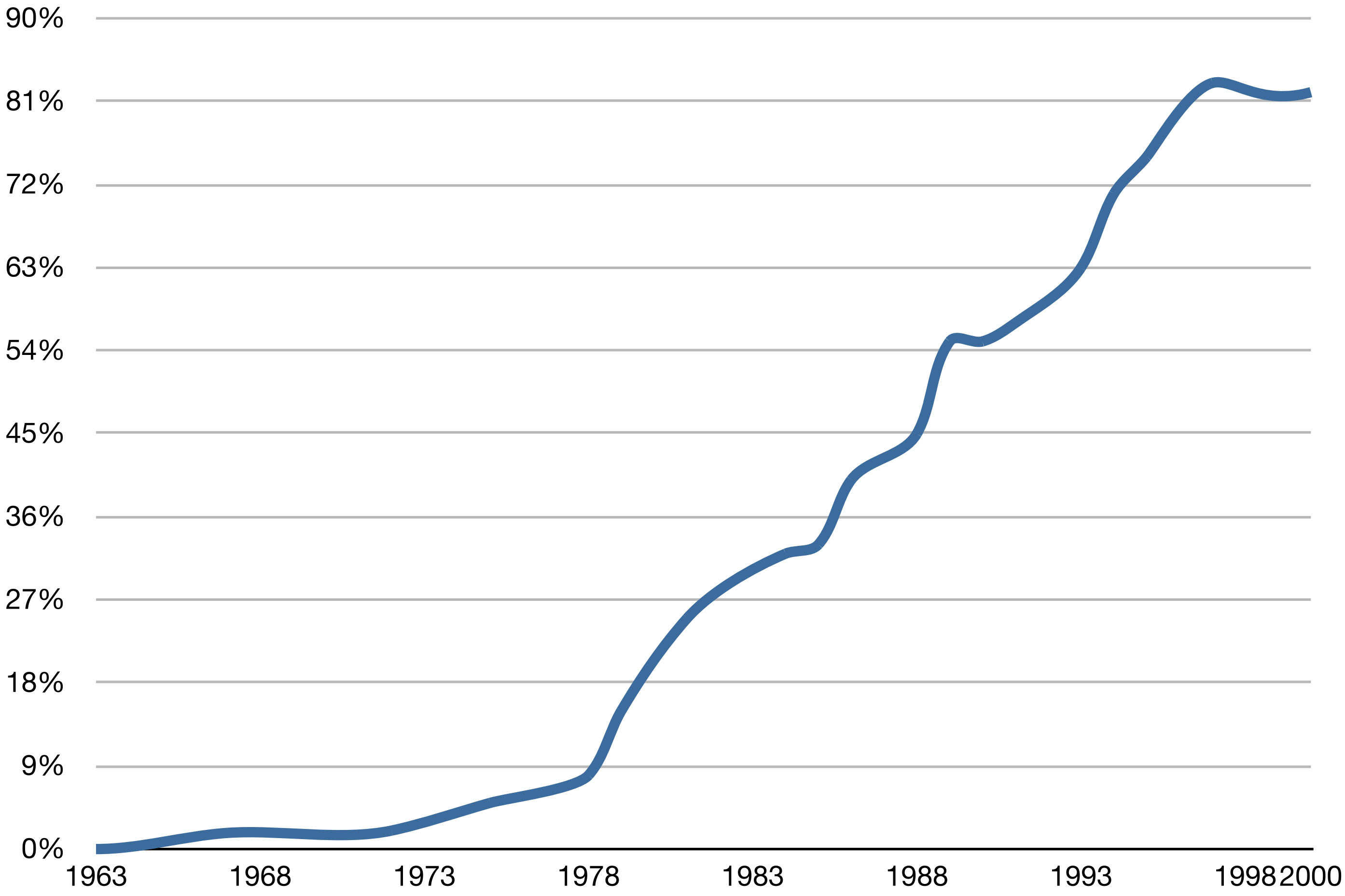
[illegible]

REFERENCE POINTS

Security in knowledge

THE RISE OF THE CFO

Prevalence of CFO Position, 1963-2000



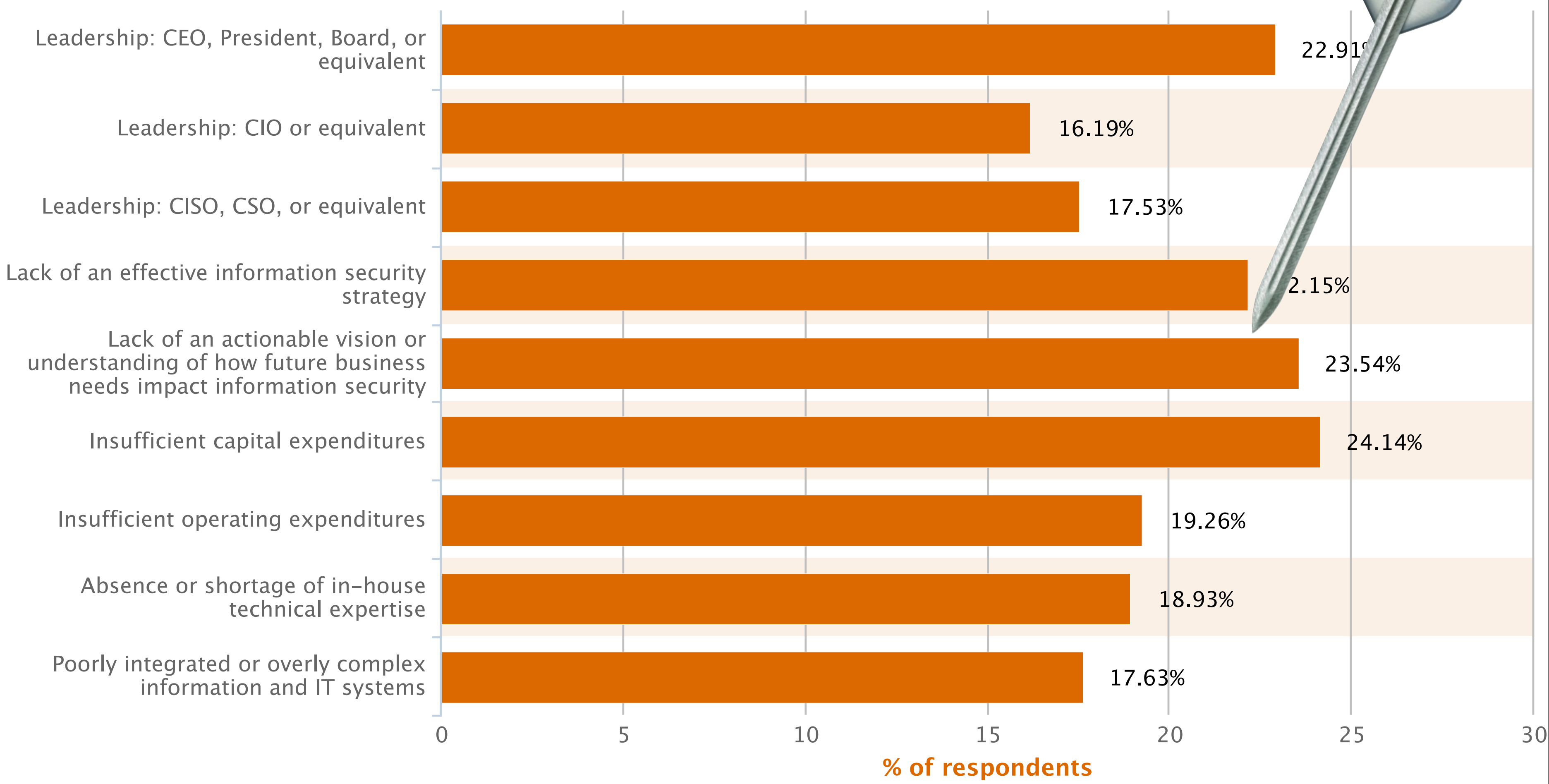
Source (Princeton University, ii)

RSA CONFERENCE EUROPE 2013

#RSAC

@thomlangford

THE RISE OF THE CISO?

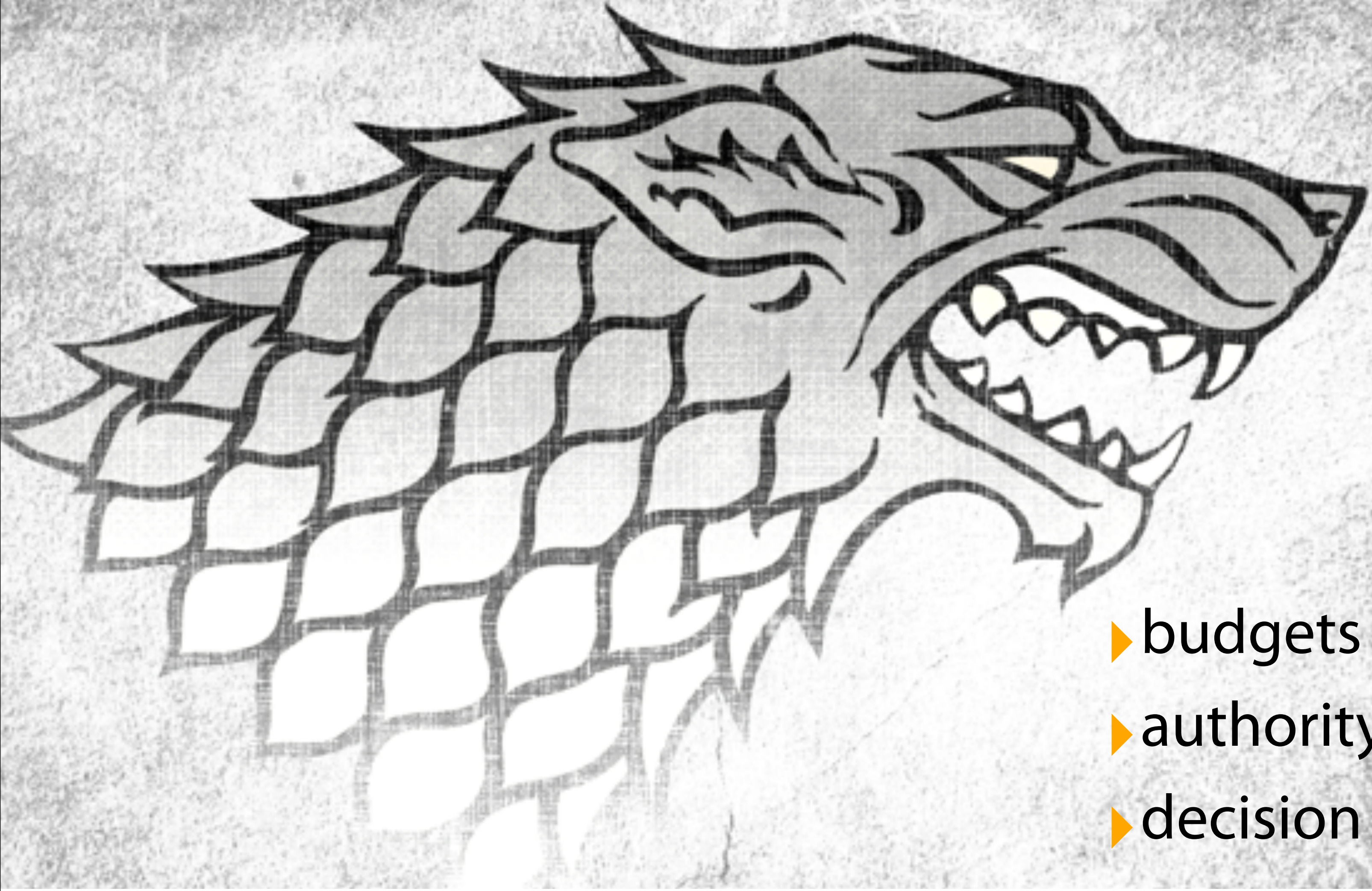


- Source (PwC, iii)

THE EVOLUTION OF THE CISO

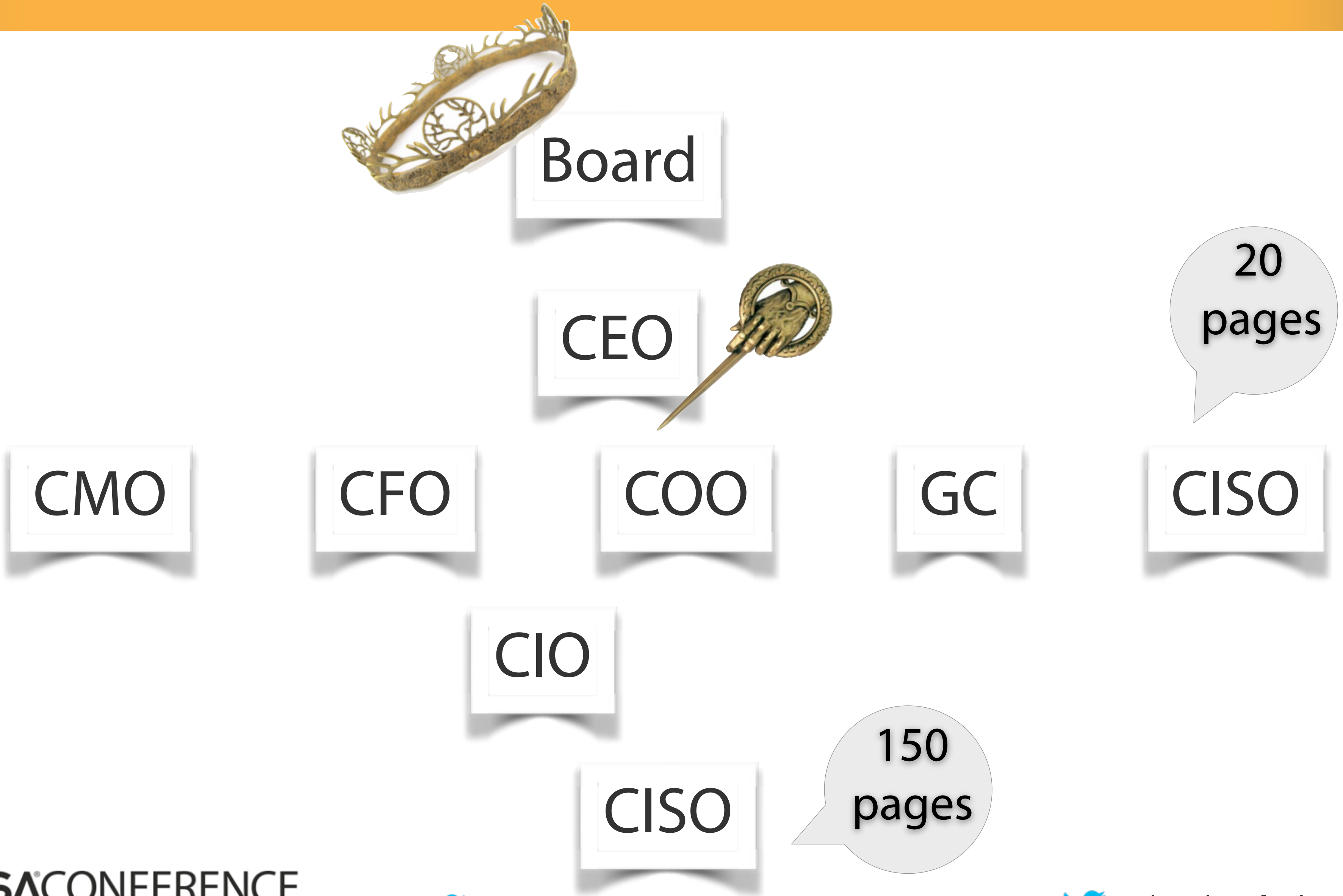
- Organisational Influencers
- Enterprise Protectors
- Responders
- The IT Guy

A QUESTION OF TEETH?



- budgets
- authority
- decision making

THE VIEW FROM HALFWAY UP



Board

CEO

20 pages

CMO

CFO

COO

GC

CISO

CIO

CISO

150 pages

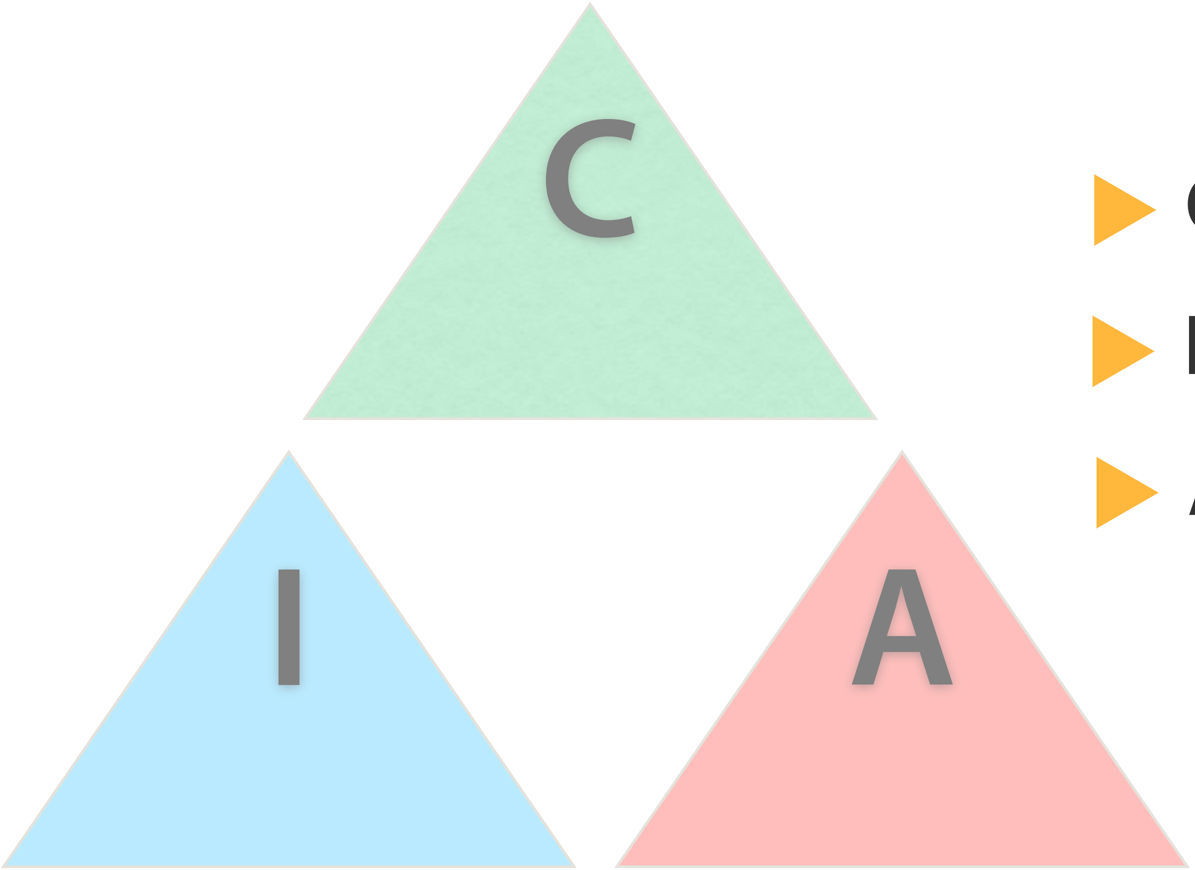
WHAT HAS HELPED

- Source (iv)

GAINING THE KING'S TRUST

Security in knowledge

RE-INTERPRET YOUR CIA TRIANGLE



- Confidentiality
- Integrity
- Availability

CIA REINTERPRETED

I

- Trust the ***integrity*** of the data you are gathering

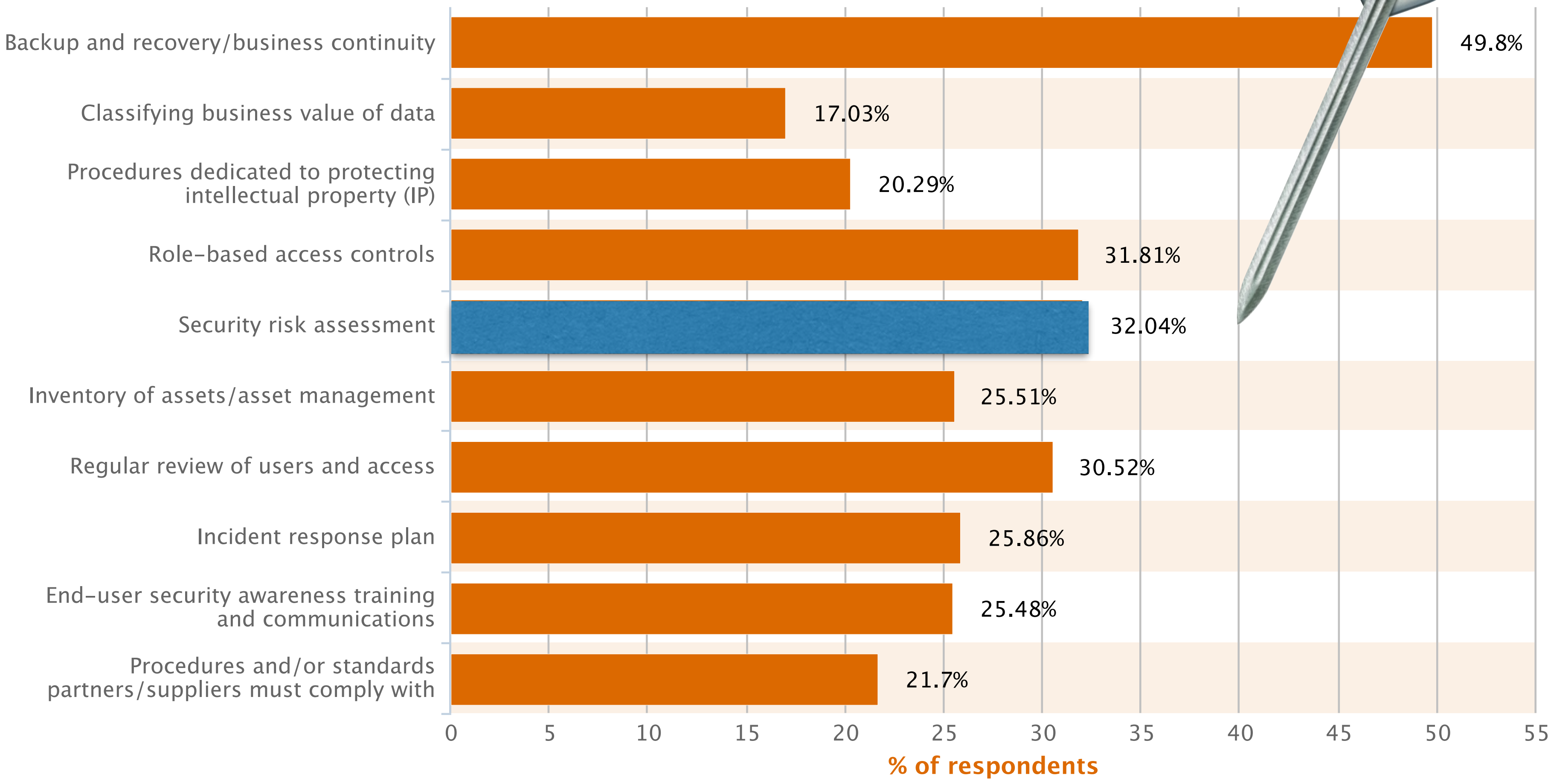
A

- Make your data ***available*** in a way that makes sense to the business

C

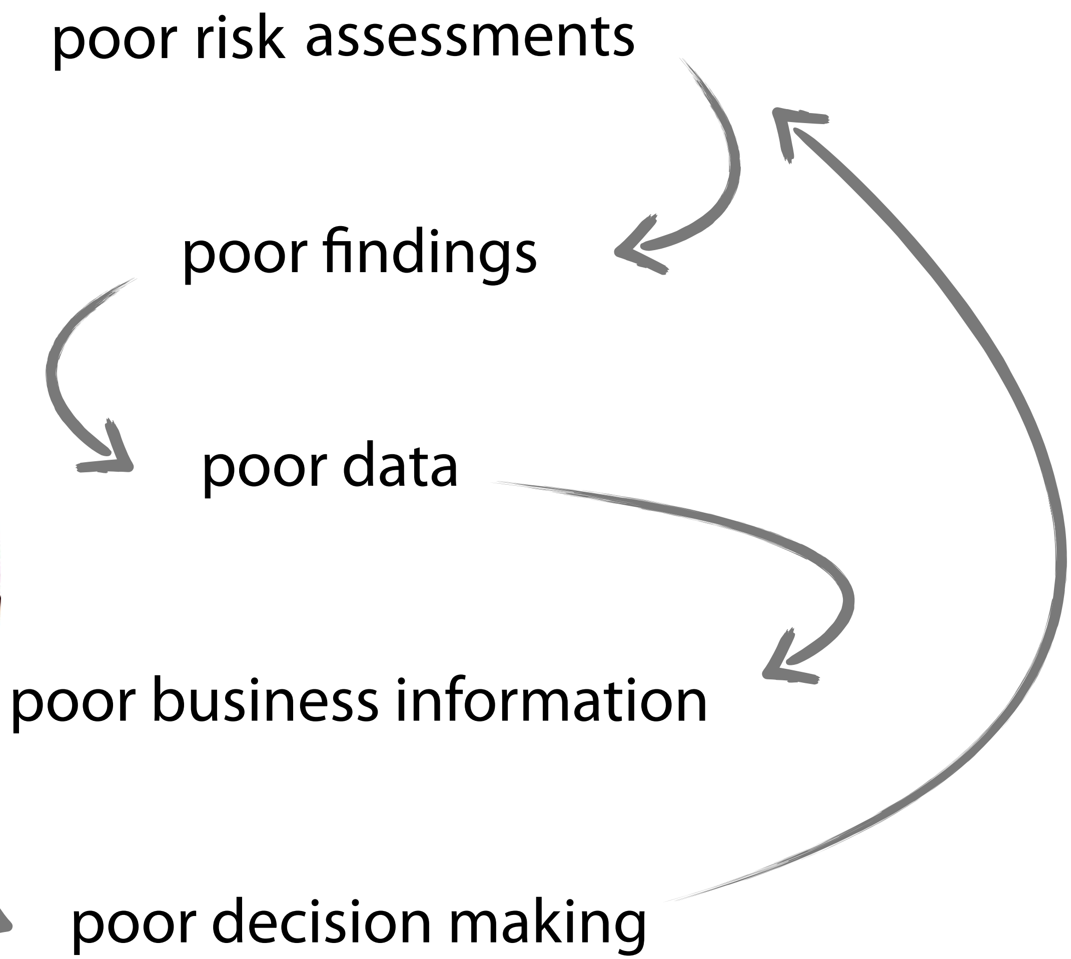
- Gain the ***confidence*** of your business

INTEGRITY (1)



Source (PwC, iii)

INTEGRITY (2)



poor risk assessments

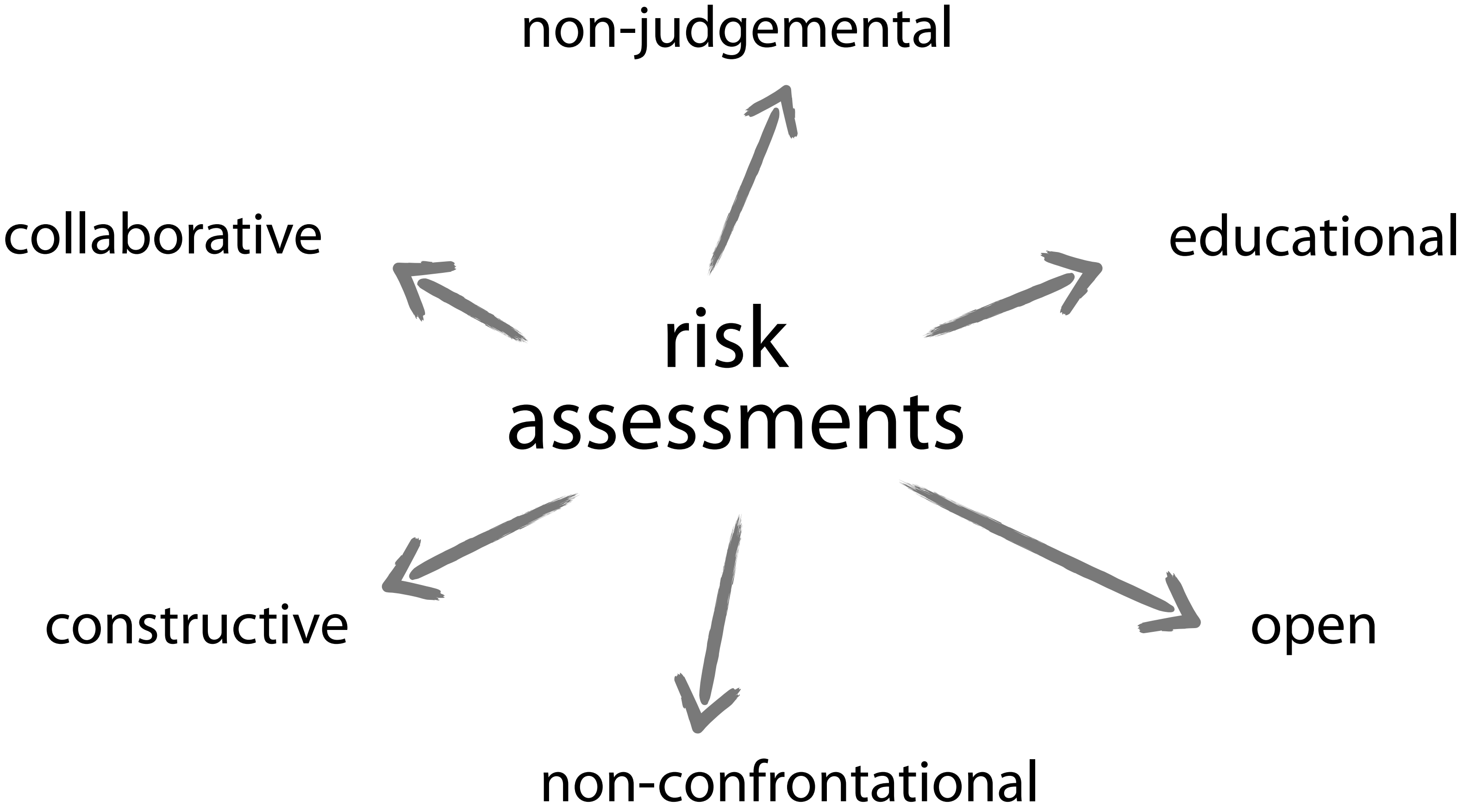
poor findings

poor data

poor business information

poor decision making

INTEGRITY (3)



risk assessments

non-judgemental

educational

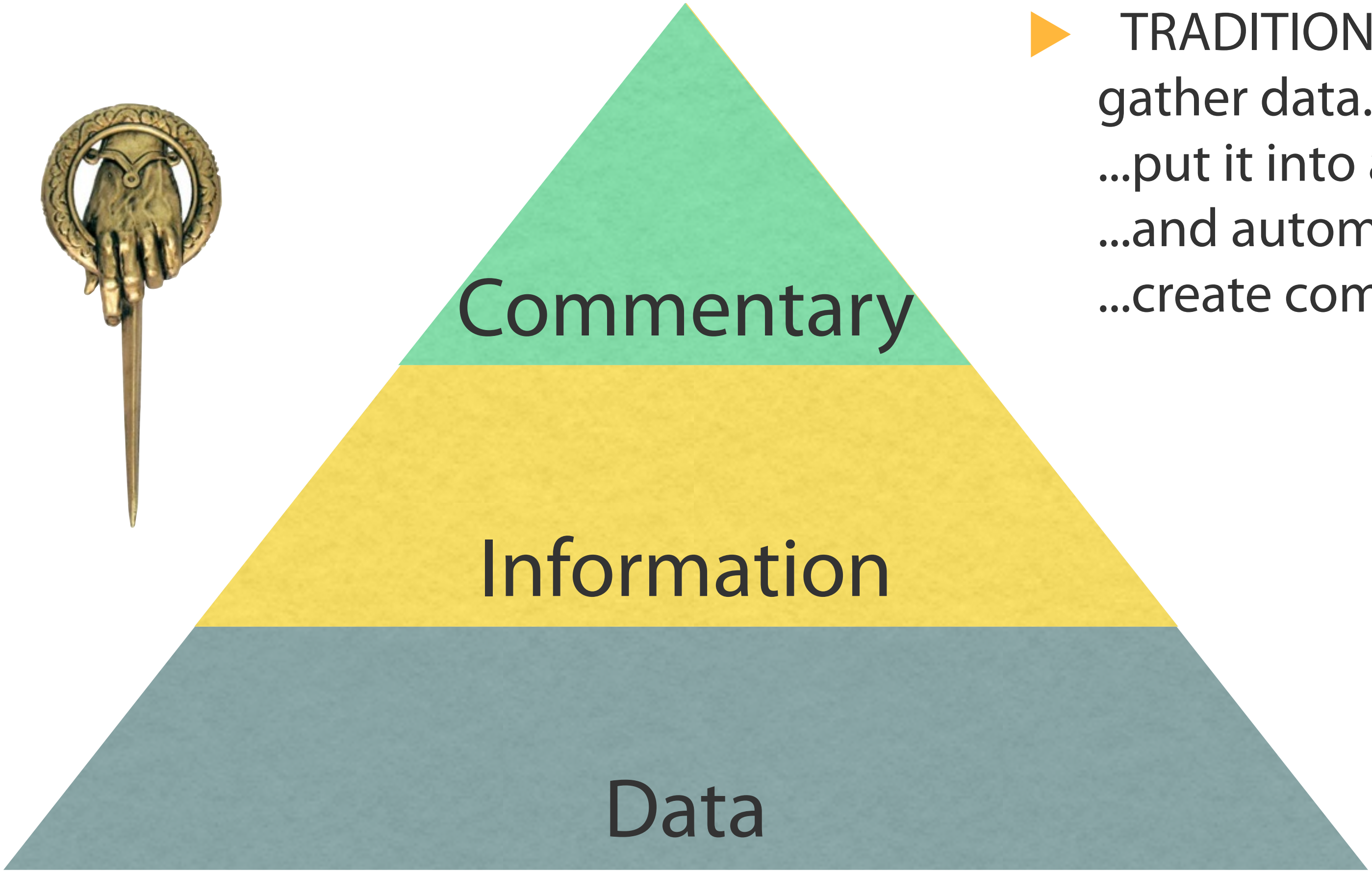
open

non-confrontational

constructive

collaborative

AVAILABILITY (1)



- TRADITIONAL VIEW

gather data...
...put it into a report...
...and automagically...
...create commentary!

AVAILABILITY (2)

- Business Intelligence ≠ Quality & Coverage
- This is not panning for gold
- Need to start with an idea

AVAILABILITY (3)

What is the business belief?

"There has been an increase in security costs over the last two years"

Establish a hypotheses:

"This is tied to BYOD and WFH"

AVAILABILITY (4)

- Identify data needed to support the hypotheses

Staff records, onboarding training, personal devices, industry increases, access control records, hiring practises, remote access records, security training records, etc..

AVAILABILITY (5)

- Establish correlations

"WFH + BYOD + Remote Access + start date before 2010 + OS=increased costs"

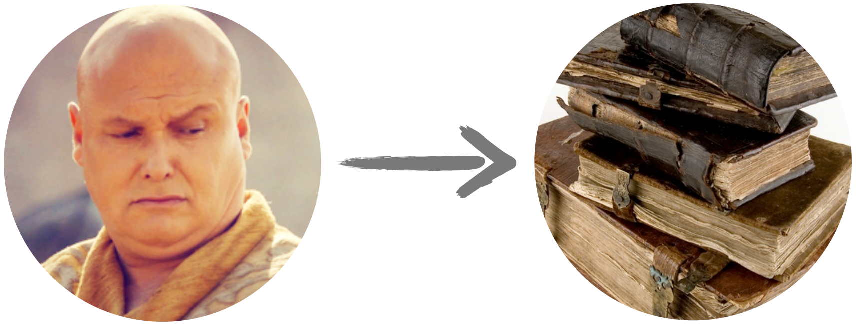
AVAILABILITY (6)

- Functional requirements
  - Use cases
  - What can I do with the data?
- Non-functional requirements
  - Location of data
  - Volume of data
  - Performance/KPI's

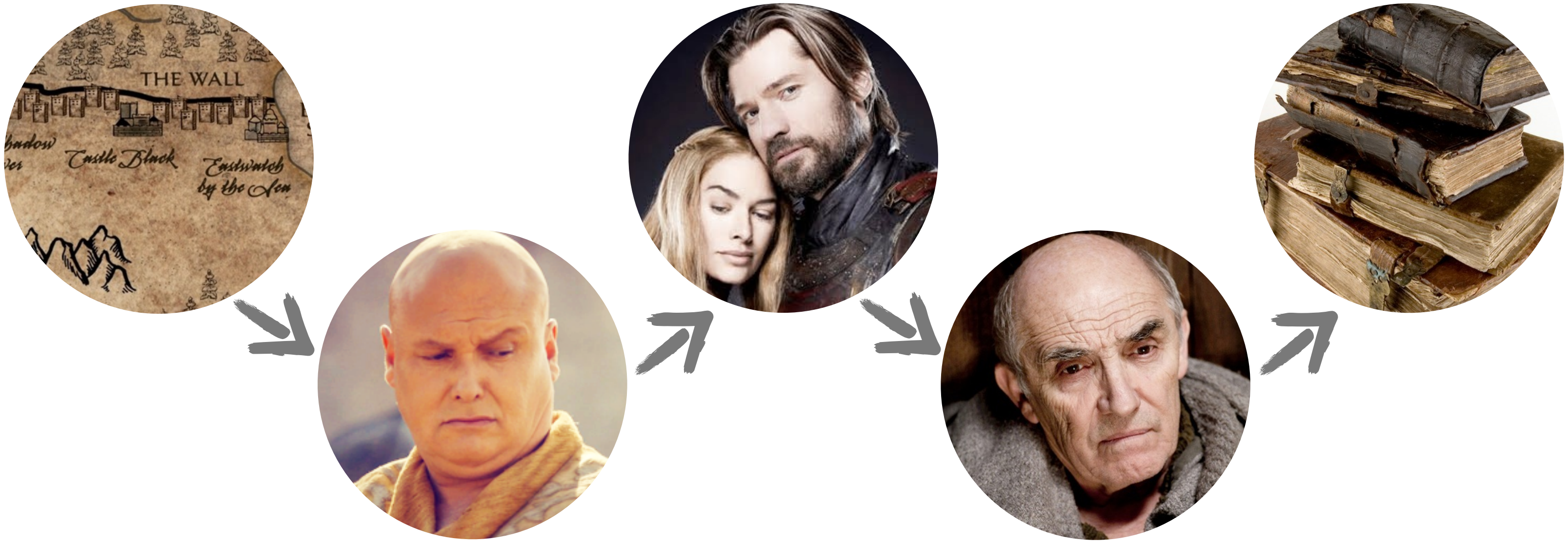
AVAILABILITY (7)

- Build your report
- Format it to your audience

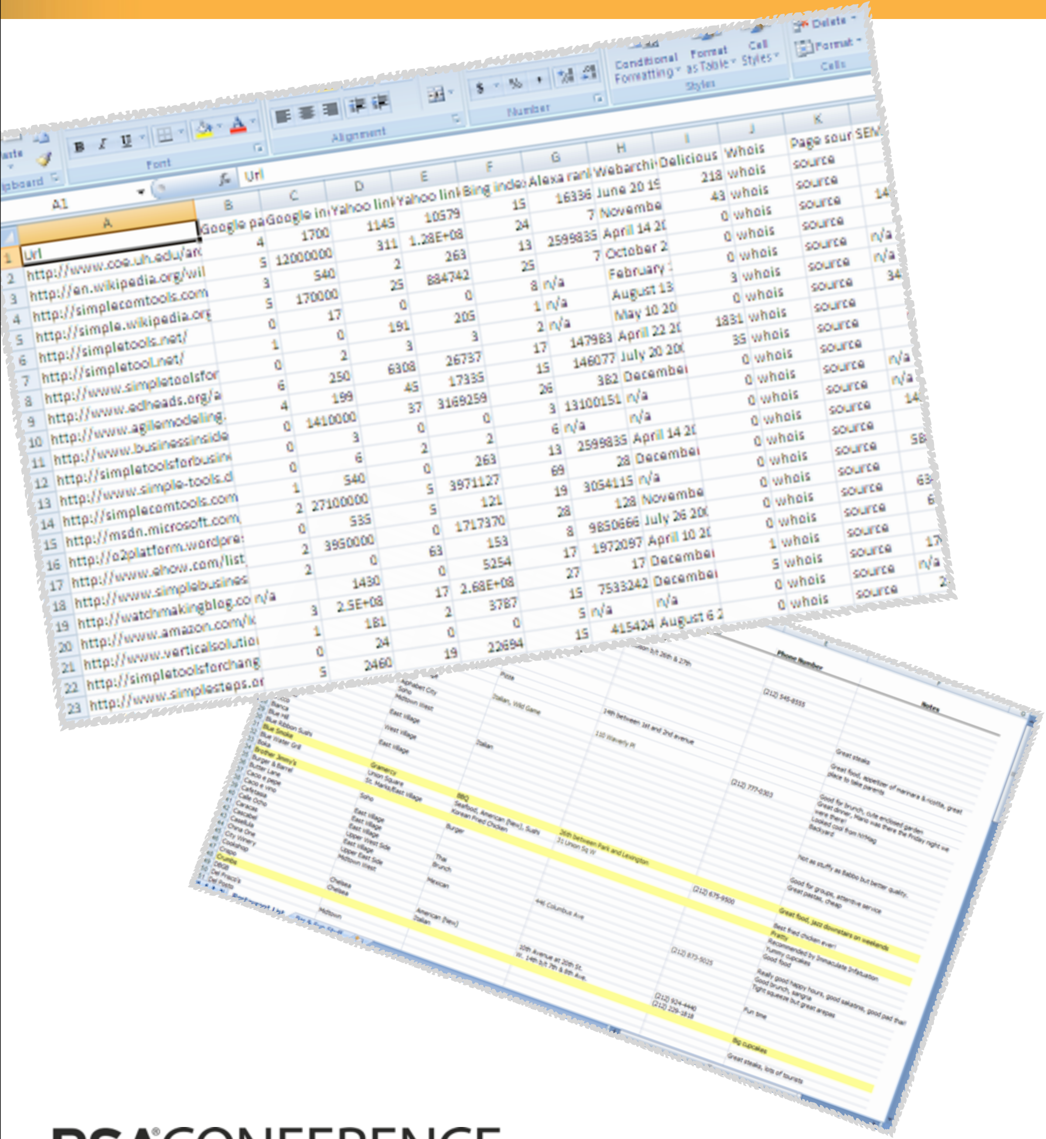
AVAILABILITY (8)



AVAILABILITY (9)



AVAILABILITY (10)



	A	B	C	D	E	F	G	H	I	J	K	
1	Url	Google pa	Google in	Yahoo lin	Yahoo lin	Bing inde	Alexa ran	Webarchi	Delicious	Whois	Page sour	SEM
2	http://www.coe.uh.edu/arc	4	1700	1145	10579	15	16336	June 20 19	218	whois	source	
3	http://en.wikipedia.org/wil	5	12000000	311	1.28E+08	24	7	Novembe	43	whois	source	
4	http://simplecomtools.com	3	540	2	263	13	2599835	April 14 20	0	whois	source	14
5	http://simple.wikipedia.org	5	170000	25	884742	25	7	October 2	0	whois	source	
6	http://simpletools.net/	0	17	0	0	8	n/a	February 1	0	whois	source	n/a
7	http://simpletool.net/	1	0	191	205	1	n/a	August 13	3	whois	source	n/a
8	http://www.simpletoolsfor	0	2	3	3	2	n/a	May 10 20	0	whois	source	34
9	http://www.edheads.org/a	6	250	6308	26737	17	147983	April 22 20	1831	whois	source	
10	http://www.agilemodeling.	4	199	45	17335	15	146077	July 20 200	35	whois	source	
11	http://www.businessinside	0	1410000	37	3169259	26	382	Decembe	0	whois	source	
12	http://simpletoolsforbusin	0	3	0	0	3	13100151	n/a	0	whois	source	n/a
13	http://www.simple-tools.d	0	6	2	2	6	n/a	n/a	0	whois	source	n/a
14	http://simplecomtools.com	1	540	0	263	13	2599835	April 14 20	0	whois	source	14
15	http://msdn.microsoft.com	2	27100000	5	3971127	69	28	Decembe	0	whois	source	
16	http://o2platform.wordpre	0	535	5	121	19	3054115	n/a	0	whois	source	58
17	http://www.ehow.com/list	2	3960000	0	1717370	28	128	Novembe	0	whois	source	
18	http://www.simplebusines	2	0	63	153	8	9850666	July 26 200	0	whois	source	63
19	http://watchmakingblog.co	n/a	1430	0	5254	17	1972097	April 10 20	0	whois	source	6
20	http://www.amazon.com/k	3	2.5E+08	17	2.68E+08	27	17	Decembe	1	whois	source	
21	http://www.verticalsolutio	1	181	2	3787	15	7533242	Decembe	5	whois	source	17
22	http://simpletoolsforchang	0	24	0	0	5	n/a	n/a	0	whois	source	n/a
23	http://www.simplesteps.or	5	2460	19	22694	15	415424	August 6 2	0	whois	source	2

Phone Number

Notes

Bianca
Blue Hill
Blue Ribbon Sushi
Blue Smoke
Blue Water Grill
Boka
Brother Jimmy's
Burger & Barrel
Butter Lane
Caco e pepe
Caco e vino
Cafetasia
Calle Ocho
Caracas
Cascabel
Casellula
China One
City Winery
Cookshop
Crispo
Crumbs
DBGB
Del Frisco's
Del Posto

Alphabet City
Soho
Midtown West
East Village
West Village
East Village
Gramercy
Union Square
St. Marks/East Village
Soho
East Village
East Village
East Village
Upper West Side
East Village
Upper East Side
Midtown West
Chelsea
Chelsea
Midtown

Pizza
Italian, Wild Game
Italian
BBQ
Seafood, American (New), Sushi
Korean Fried Chicken
Burger
Thai
Brunch
Mexican
American (New)
Italian

b/t 26th & 27th
14th between 1st and 2nd avenue
110 Waverly Pl
26th between Park and Lexington
31 Union Sq W
441 Columbus Ave
10th Avenue at 20th St.
W. 14th b/t 7th & 8th Ave.

(212) 545-8555
(212) 777-0303
(212) 675-9500
(212) 873-5025
(212) 924-4440
(212) 229-1818

Great steaks
Great food, appetizer of marinara & ricotta, great place to take parents
Good for brunch, cute enclosed garden
Great dinner, Mario was there the Friday night we were there!
Looked cool from NYMag
Backyard
Not as stuffy as Babbo but better quality.
Good for groups, attentive service
Great pastas, cheap
Great food, jazz downstairs on weekends
Best fried chicken ever!
Pretty
Recommended by Immaculate Infatuation
Yummy cupcakes
Good food
Really good happy hours, good sakatinis, good pad thai
Good brunch, sangria
Tight squeeze but great arepas
Fun time
Big cupcakes
Great steaks, lots of tourists

Restaurant List

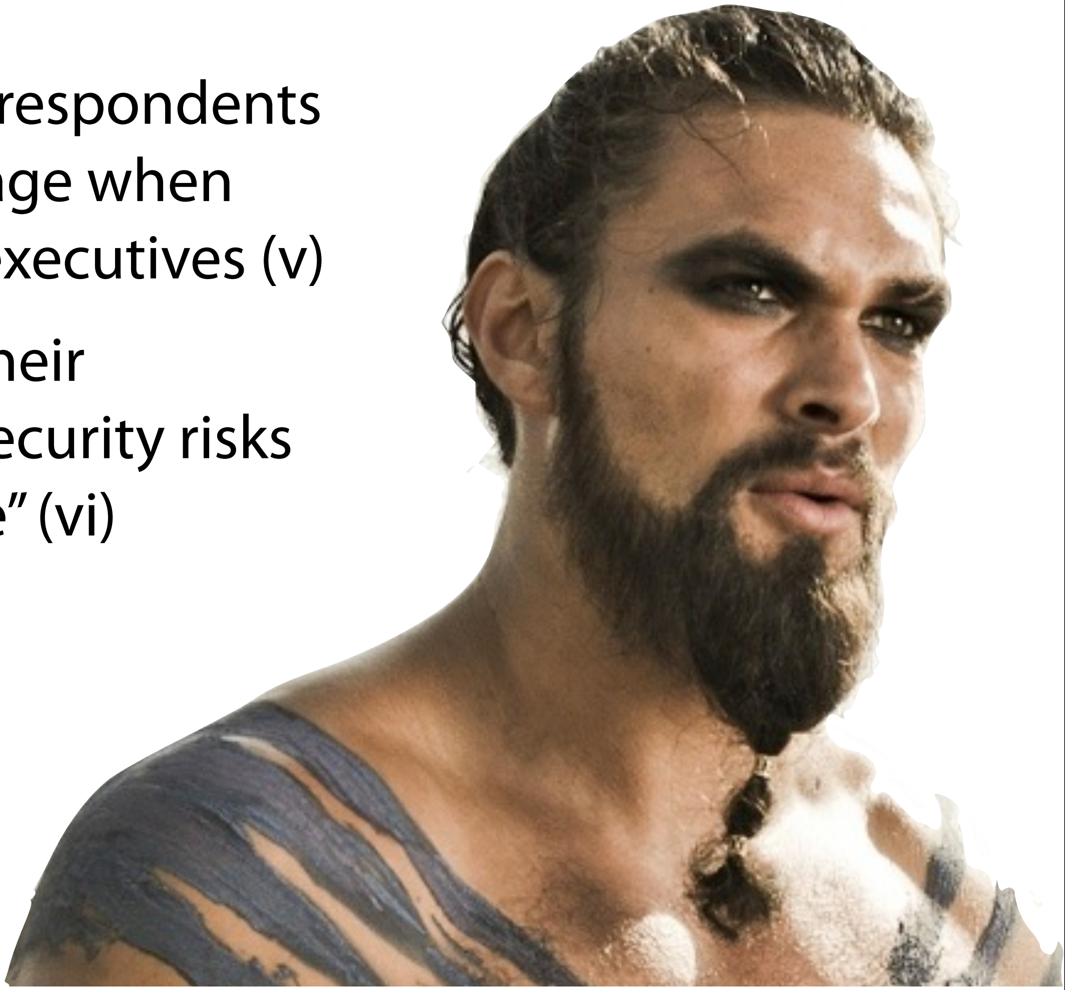
iPad 3G
9:41 AM
Enterprise Risk Report

#RSAC

@thomlangford

CONFIDENCE

- Only 38% of non-executive respondents use business-oriented language when communicating with senior executives (v)
- 51% of respondents rated their communication of relevant security risks to executives as "not effective" (vi)



Source (Hanover Research, v & Ponemon institute vi)

CONFIDENCE (2)

CONFIDENCE (3)

- *"this is what I need digital to do to help me sell more beer"*

- Steve Mura, Director of Digital Marketing, MillerCoors (vii)

CONFIDENCE (4)

HOUSE LANNISTER

"HEAR ME ROAR"

ANNUAL REPORT

FOR ALL KNIGHTS, LADIES AND SERVANTS

GUIDING PRINCIPLES

Only provide information that is necessary

Simplify your experiences & interactions

Be consistent

Build & maintain trust

Optimise dependency activities

KEY TAKE AWAYS

Security in knowledge

VALUE

- Is your organisation is truly getting the full value of all of your activities?

BUSINESS INTELLIGENCE

- Look at how your security group is reporting to the business

UNDERSTANDING

- Ask yourself how much do you really understand your business, and how it operates?

BE CAREFUL WHAT YOU WISH FOR

Security in knowledge

#RSAC @thomlangford

RSA CONFERENCE EUROPE 2013

WITH RESPONSIBILITY COMES...

Security in knowledge

Thank you

Thom Langford

Sapient

@thomlangford

thom@thomlangford.com

http://thomlangford.com

THIS PRESENTATION IS AVAILABLE AT THOMLANGFORD.COM IN KEYNOTE AND PDF

Security in knowledge

REFERENCES

- References
  - (i) Twist & Shout "Rose Tinted Glasses" shown with permission
  - (ii) Here a Chief, There a Chief: The Rise of the CFO in the American Firm by Dirk M. Zorn, Princeton University
  - (iii) PwC, The State of Information Security Survey 2014
  - (iv) In discussion with Simon Hember and Scott West of Acumin
  - (v) Tripwire commentary on Hanover Research, Doctor, My CEO Doesn't Understand Security
  - (vi) Tripwire commentary on Ponemon Institute research Majority of IT Professionals Don't Communicate Security Risks
  - (vii) MarketingProfs Four Tips For a Common Sense Approach to Marketing
  - All Game of Thrones images copyright HBO and relevant authors of their own fan art