RSAConference2020

San Francisco | February 24 – 28 | Moscone Center

HUMAN ELEMENT

SESSION ID: **STR-R09**

The First 6 Months as a CISO Determines Success or Failure

Michael Coates

CEO
Altitude Networks
@_mwc

RSAConference2020

The “CISO”

Putting Security Into Perspective

Day 0 - Role of the CISO

The role of the CISO is NOT to single-handedly prevent all security vulnerabilities or be responsible for every security failure

Day 0 - Role of the CISO

The role of the CISO is NOT to single-handedly prevent all security vulnerabilities or be responsible for every security failure

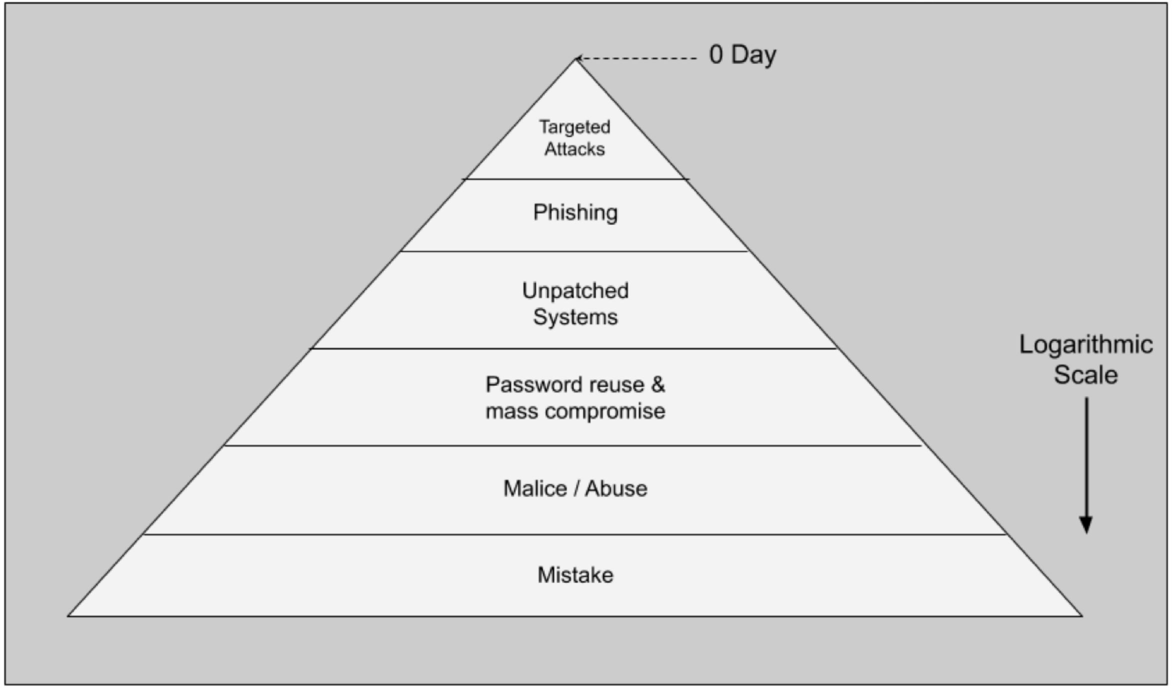
Instead, the CISO’s role is to build systems, technology, and processes that **surface risks**, empower informed **risk management** and enables the company to **mitigate risks to an acceptable level**…

Day 0 - Role of the CISO

The role of the CISO is NOT to single-handedly prevent all security vulnerabilities or be responsible for every security failure

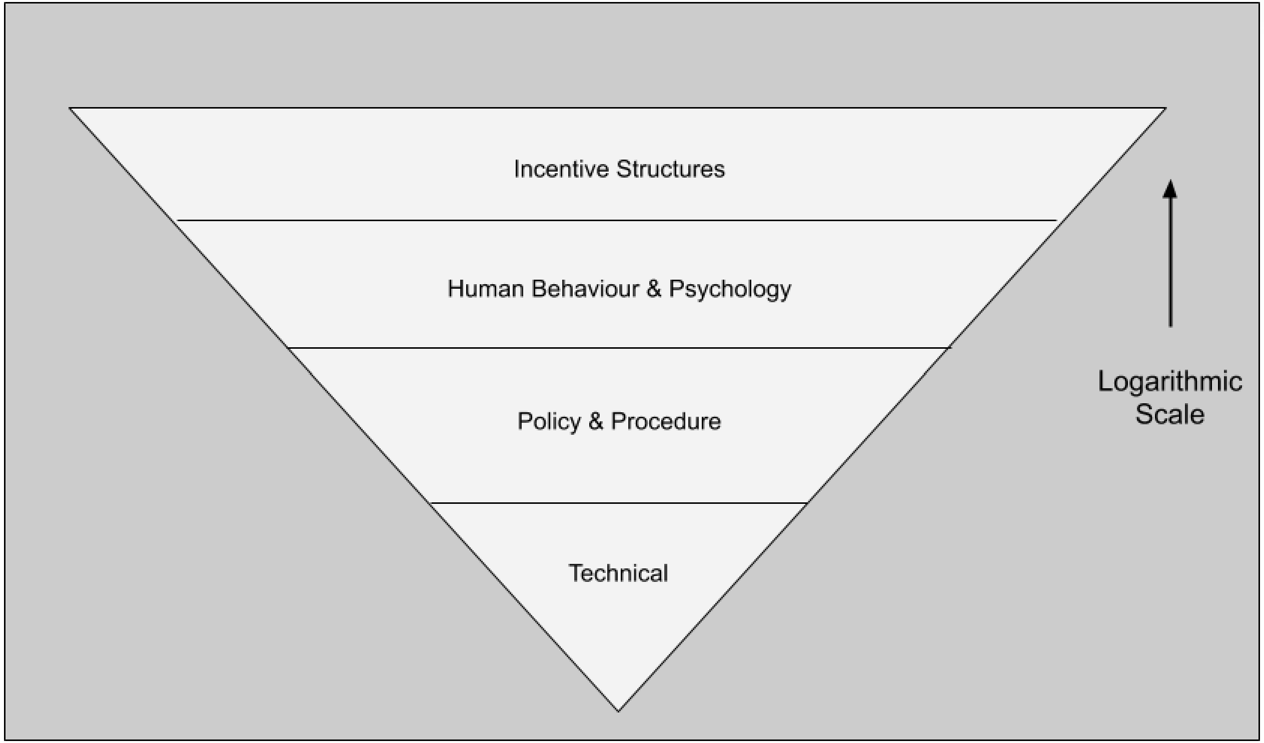
Instead, the CISO's role is to build systems, technology, and processes that **surface risks**, empower informed **risk management** and enables the company to **mitigate risks to an acceptable level**… while moving at the speed of business

Day 1 - Risks: What Actually Matters



Modification of Threat Pyramid, Alex Stamos, BlackHat 2017

Day 1 - What Is Security at Enterprise Scale?



Incentive Structures

Human Behaviour & Psychology

Policy & Procedure

Technical

Logarithmic Scale

Don’t Act, Listen First

Day 2 - Don’t Rush to Action

CISO Instinct - Immediately take action and begin “delivering value”

Day 2 - Don’t Rush to Action

CISO Instinct - Immediately take action and begin “delivering value”

Contrarian CISO Advice - Don’t. Actually do “nothing” for first 90 days. Instead Listen!

Day 10 - CISO to Business Leaders: 5 Questions

Empathy	- What does your org do?
History	- Previous interactions between org & security?
Perspective	- How do you view security at the company?
Ideas	- What areas should security investigate?
Alignment	- Best way to stay connected & updated?

Day 17

Ask Your Security Team

Where are the “dead bodies”?

RSAConference2020

Deliverables: Strategy, Plans & Support

Easier Said Than Done

Day 60 - Five Core Deliverables from CISO

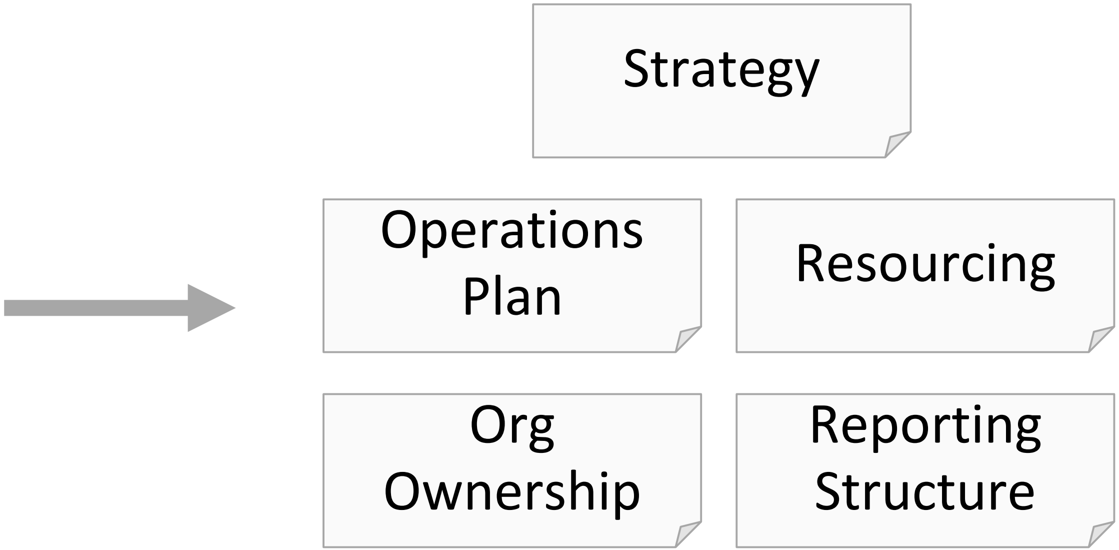
Company Risk Tolerance

Listening Tour

Security Core Controls

Compliance Requirements

Security as Enabler



Strategy

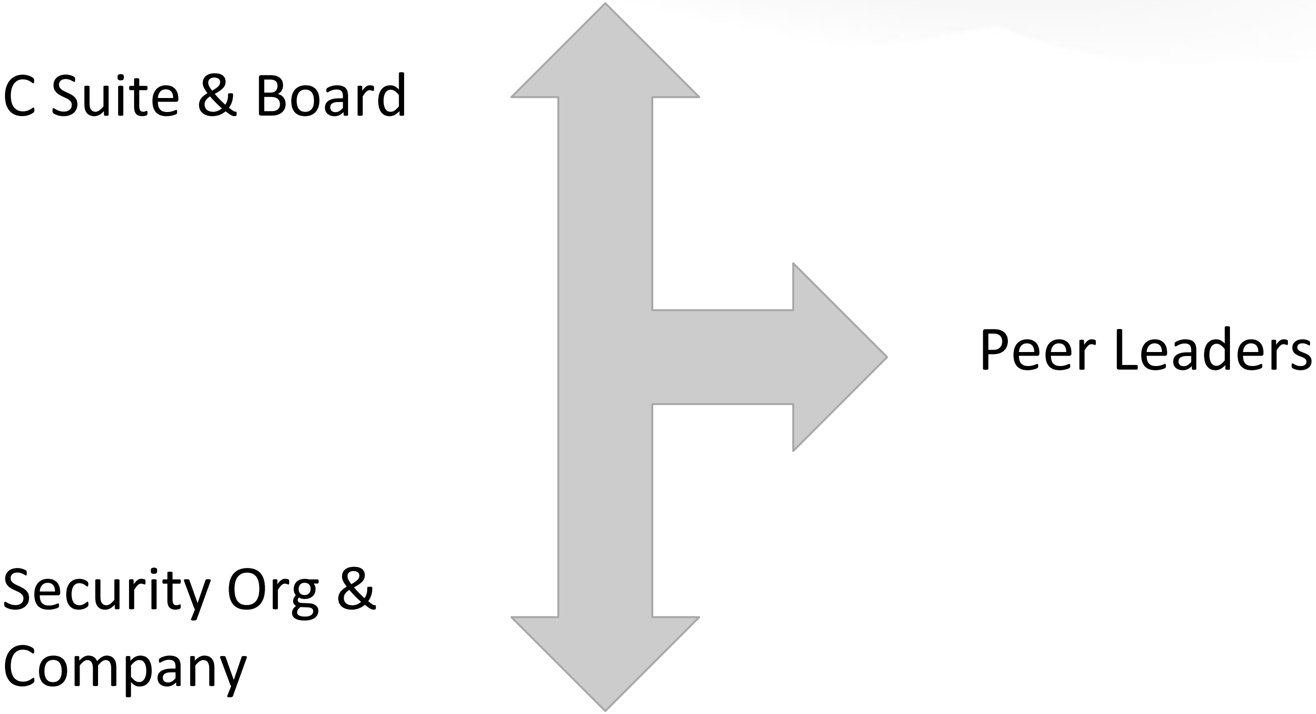
Operations Plan

Resourcing

Org Ownership

Reporting Structure

Day 61 - The Delivery

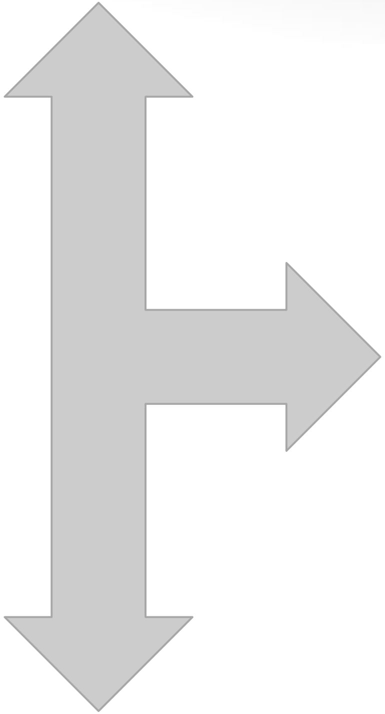


C Suite & Board

Peer Leaders

Security Org & Company

Don’t forget Security Allies



C Suite & **Board**

Security Org & Company

Peer Leaders

Internal Audit

Legal

BizDev

Why All Breaches are(n't) the CISOs Fault

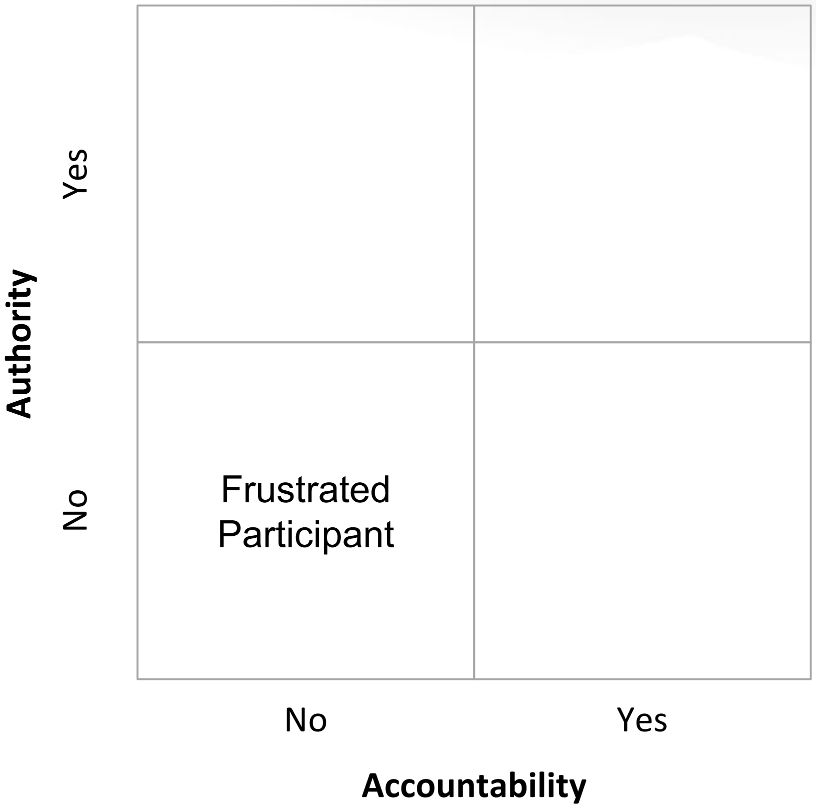
Establishing Security Accountability

Day 90 - Why CISOs are (often) setup to fail

		No	Yes
Authority	Yes		
	No		

Accountability

Handling Security & Risk Ownership



		Accountability	
		No	Yes
Authority	Yes		
	No	Frustrated Participant	

Handling Security & Risk Ownership

		No	Yes
Authority	Yes		
	No	Frustrated Participant	Helpless Scapegoat

Accountability

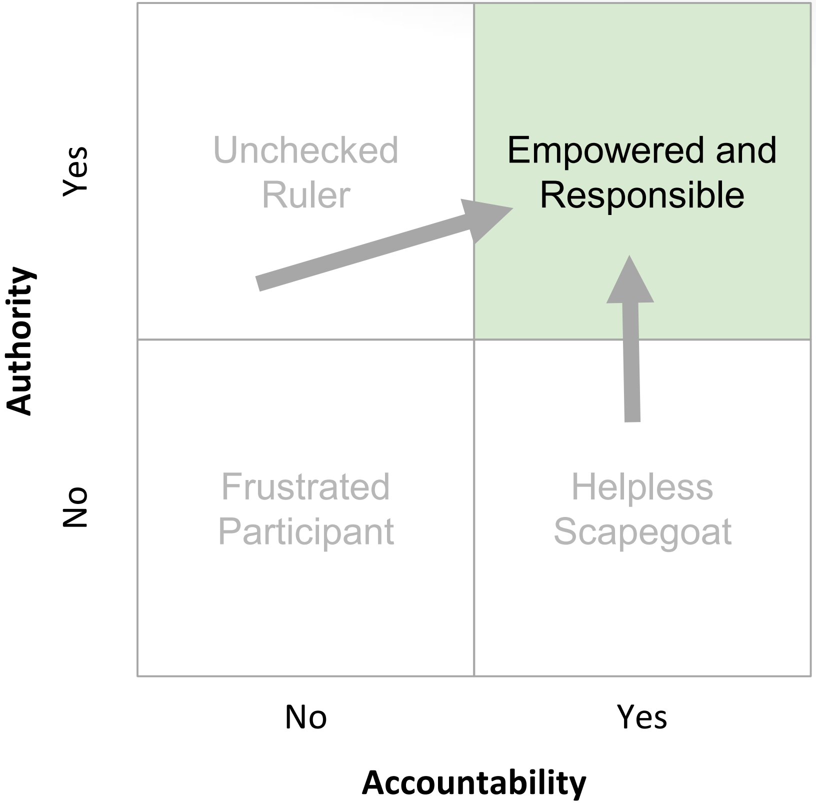
Handling Security & Risk Ownership

		Accountability	
		No	Yes
Authority	Yes	Unchecked Tyrant	
	No	Frustrated Participant	Helpless Scapegoat

Risk Ownership Defines Culture

Authority	Accountability: No	Accountability: Yes
Yes	Unchecked Ruler	Empowered and Responsible
No	Frustrated Participant	Helpless Scapegoat

Risk Ownership Defines Culture

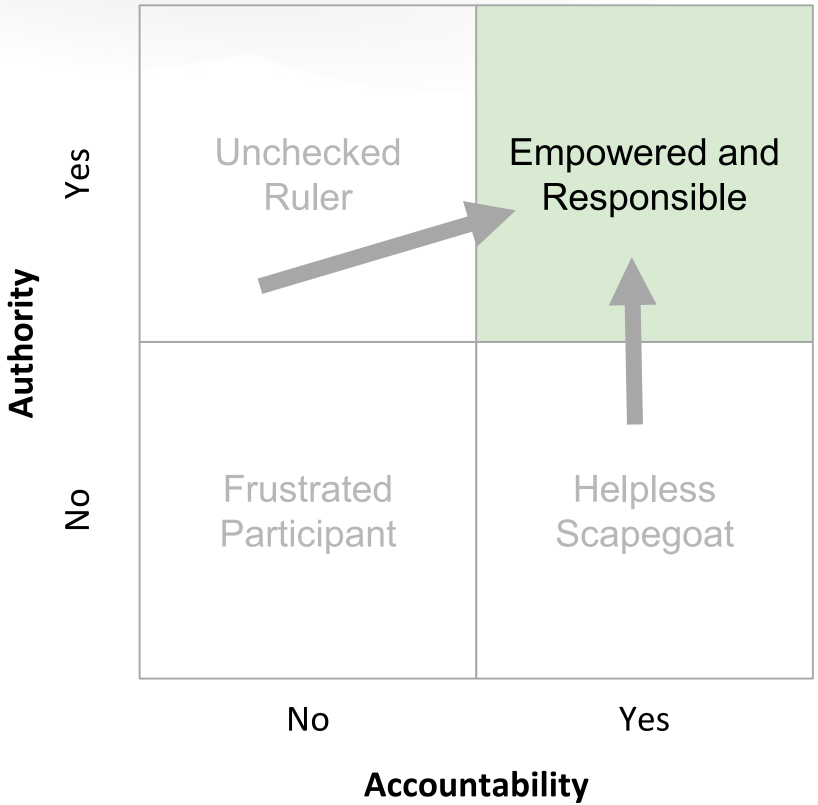


Authority		Accountability: No	Accountability: Yes
	Yes	Unchecked Ruler	Empowered and Responsible
	No	Frustrated Participant	Helpless Scapegoat

Empowered and Responsible: The How

How to Do It

- Establish culture of risk taking & ownership
- Don’t fight risky decisions - redirect with mitigation and visibility
- Gamify for leadership traction
- Eliminate IC to IC priority battles
- Track, retro, praise/adjust
- Build feedback loops for improvement



Authority \ Accountability	No	Yes
Yes	Unchecked Ruler	Empowered and Responsible
No	Frustrated Participant	Helpless Scapegoat

Build Security Culture at Leadership Level

Align

Authority & Accountability

for Security Actions

RSA Conference2020

Day 90: Security Team Building in Negative Unemployment Markets

Security Unicorns: Stop looking for them

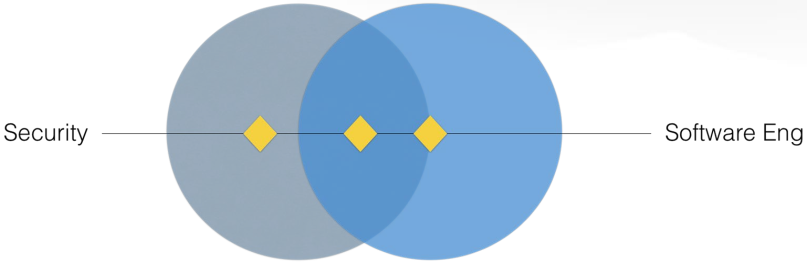
Reality

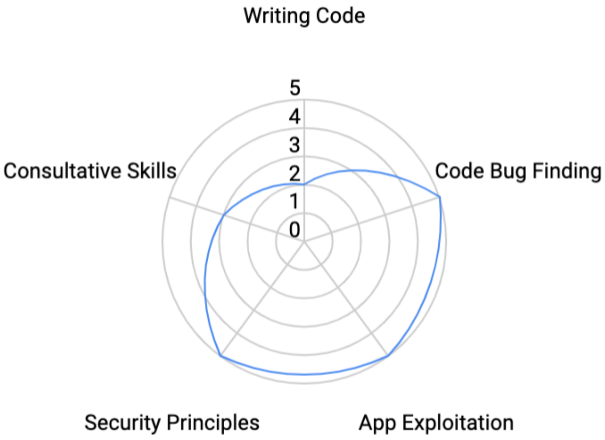
Awesome teams are built with great people in well-defined roles

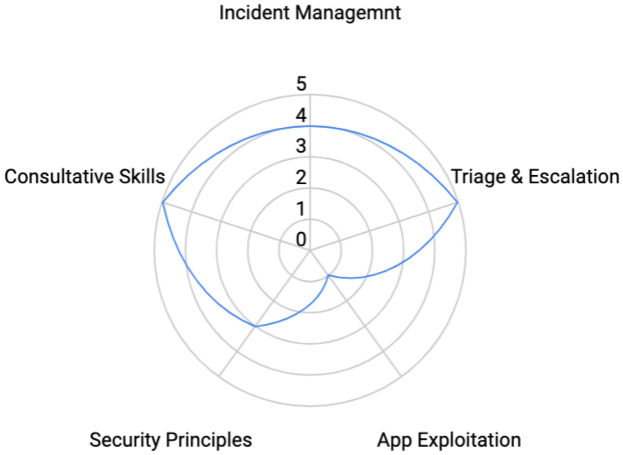
CISO Anti-pattern

Wedging multiple security disciplines into a single headcount

Amazing Teams Need Different Roles





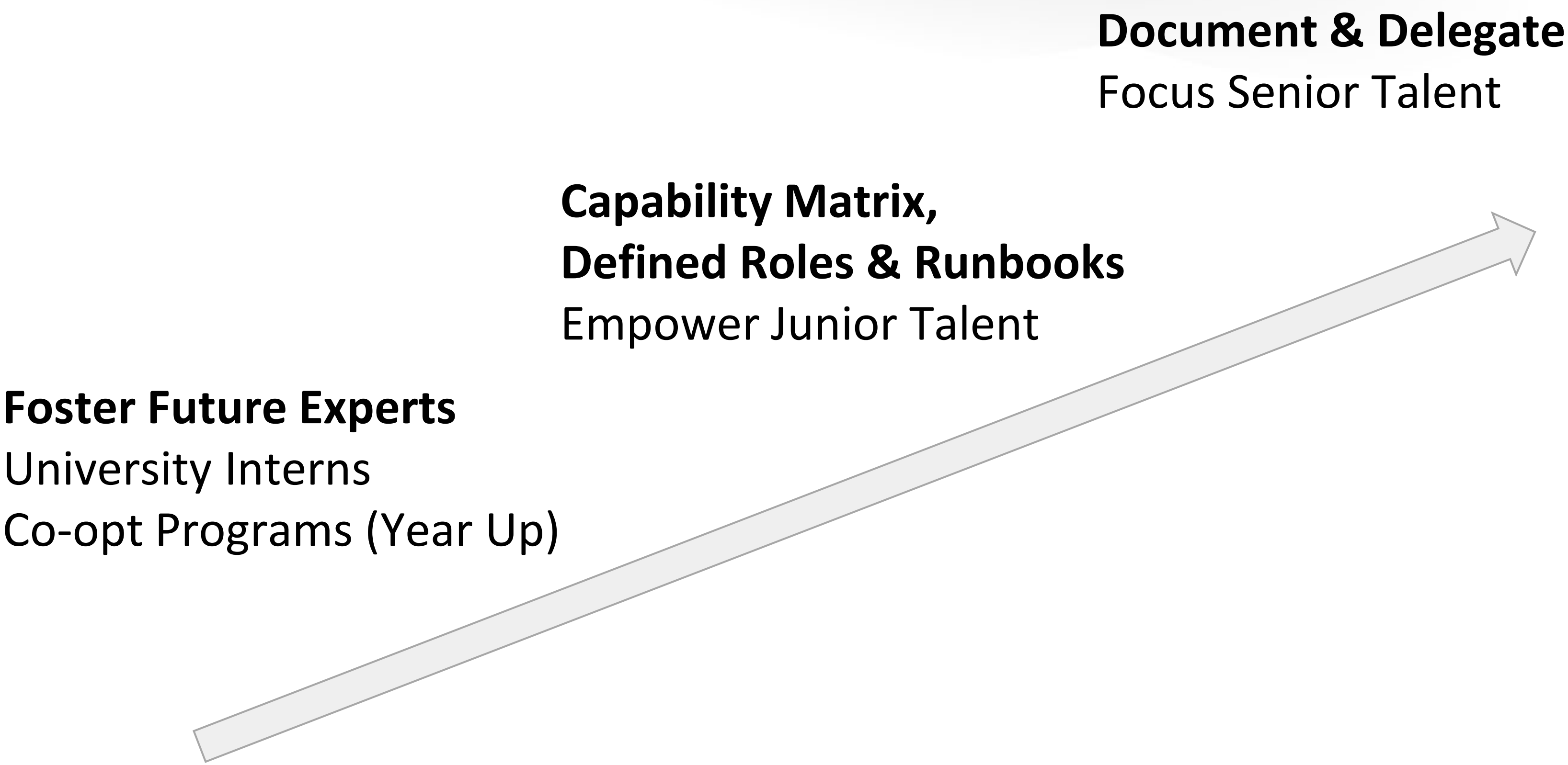


Spending Time vs Money

Which do you have more?

Opex, Capex, Security Staff Hours

Build a Security Talent Funnel



Document & Delegate

Focus Senior Talent

Capability Matrix,
Defined Roles & Runbooks

Empower Junior Talent

Foster Future Experts

University Interns

Co-opt Programs (Year Up)

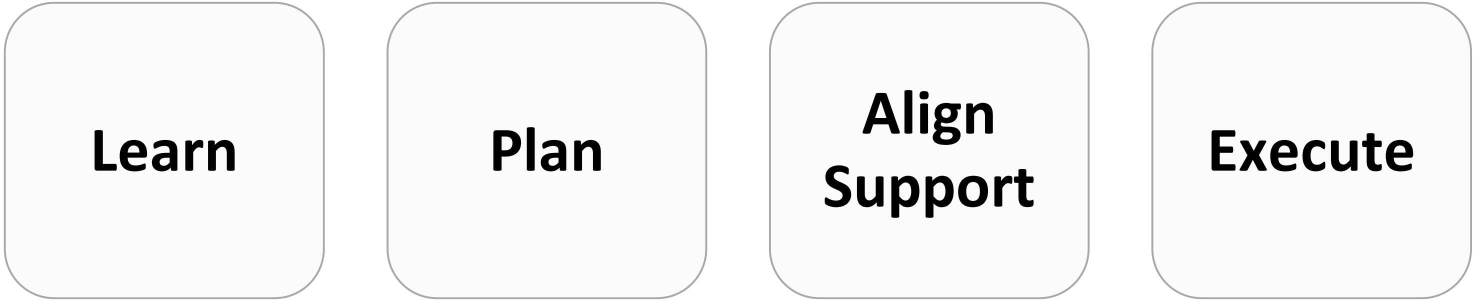
Successful Teams Require Diversity of Thought and Background

Be a CISO and a Great Leader

RSAConference2020

Bringing it all Together

Days 1 - 180: The CISO’s First Journey



Learn

Plan

Align Support

Execute

Role of the CISO Revisited

The role of the CISO is NOT to single-handedly prevent all security vulnerabilities or be responsible for every security failure

Instead, the CISO's role is to build systems, technology, and processes that **surface risks**, empower informed **risk management** and enables the company to **mitigate risks to an acceptable level**… while moving at the speed of business

CISO Revisited

The CISO is not the *Super Hero* that Prevents All Security Risks

CISO Revisited

The CISO is the Pathfinder who guides a company to responsibly embrace risk for competitive advantage

Thank you!

Michael Coates

michael@AltitudeNetworks.com

@_MWC