LEVERAGING CULTURE TO OPTIMIZE INFORMATION SECURITY

Don McKeown
https://donmckeown.net

June 15, 2020


Culture: A shared set of beliefs and values that defines the proper way to behave within the organization


Resistance [to culture] is futile

THE RIGHT ORGANIZATIONAL CULTURE CAN HELP AN ORGANIZATION MAKE MONEY

ORGANIZATIONS TEND NOT TO INVEST IN SECURITY CULTURE

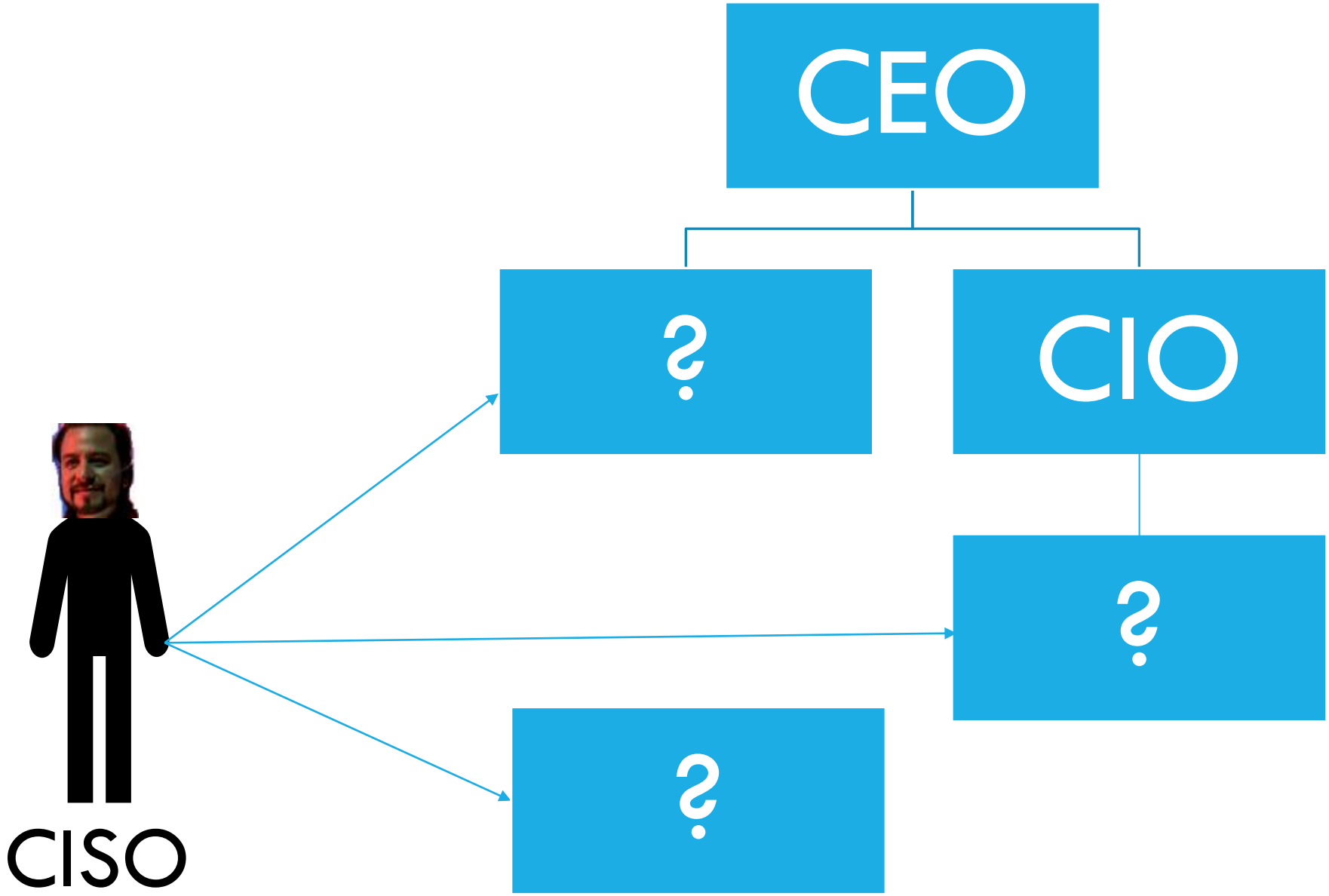
INFORMATION SECURITY

OPTIMIZING CULTURE

Leadership

Strategy

Tactics


CEO
?
CIO
?
?
CISO

IDEALLY, THE CISO SHOULD REPORT TO THE CEO

A CISO needs:

Organization-wide visibility and context

To advise on security early in projects

To advocate for appropriate budget

Authority and influence to set organizational security targets

THE CISO REPORTING TO THE CIO IS PROBLEMATIC

This reporting structure is common

Much more difficult to achieve organization-wide context and visibility

Could be much more difficult to get appropriate budget

Conflict of interest

WHY WAS EQUIFAX BREACHED?

Known, unpatched Apache Struts vulnerability

Root cause: Organizational structure that caused an accountability gap

Good news: Organizations are improving their organizational structures

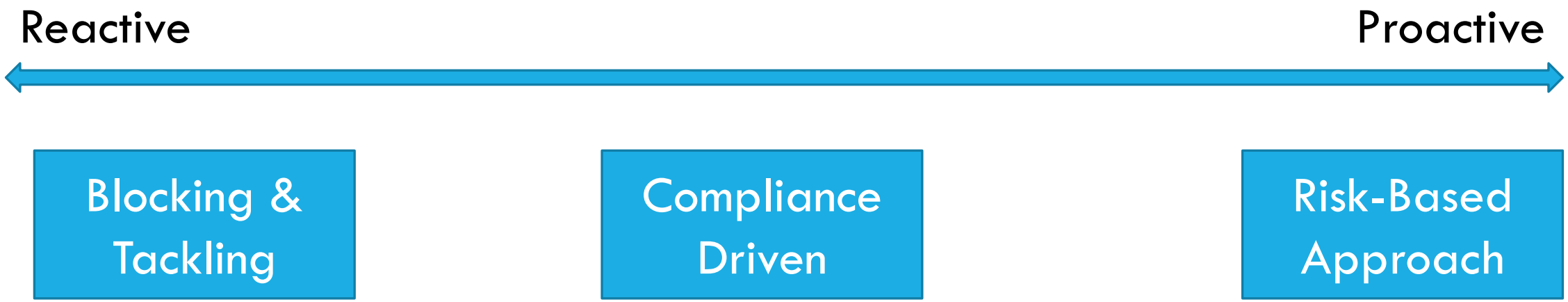
OPTIMIZING CULTURE

Leadership

Strategy

Tactics

Blue-Lava Maturity Model



BLOCKING AND TACKLING

Reactive

Little executive support

Lack of funding

No metrics

A setup for failure

COMPLIANCE DRIVEN

Controls align with mandatory standards

Compliance is a double-edged sword

Why is compliance insufficient?

- Limited scope
- Not updated frequently enough
- Compliance orgs get breached
- Compliance certs give a false sense of confidence

Overcoming the belief that compliance=security is a huge challenge

RISK-BASED APPROACH

Multi layered defense in depth

Behavior analysis, correlating events from across the org

Evaluating new technologies

I would add:

- Zero trust architecture
- Resilience

OPTIMIZING CULTURE

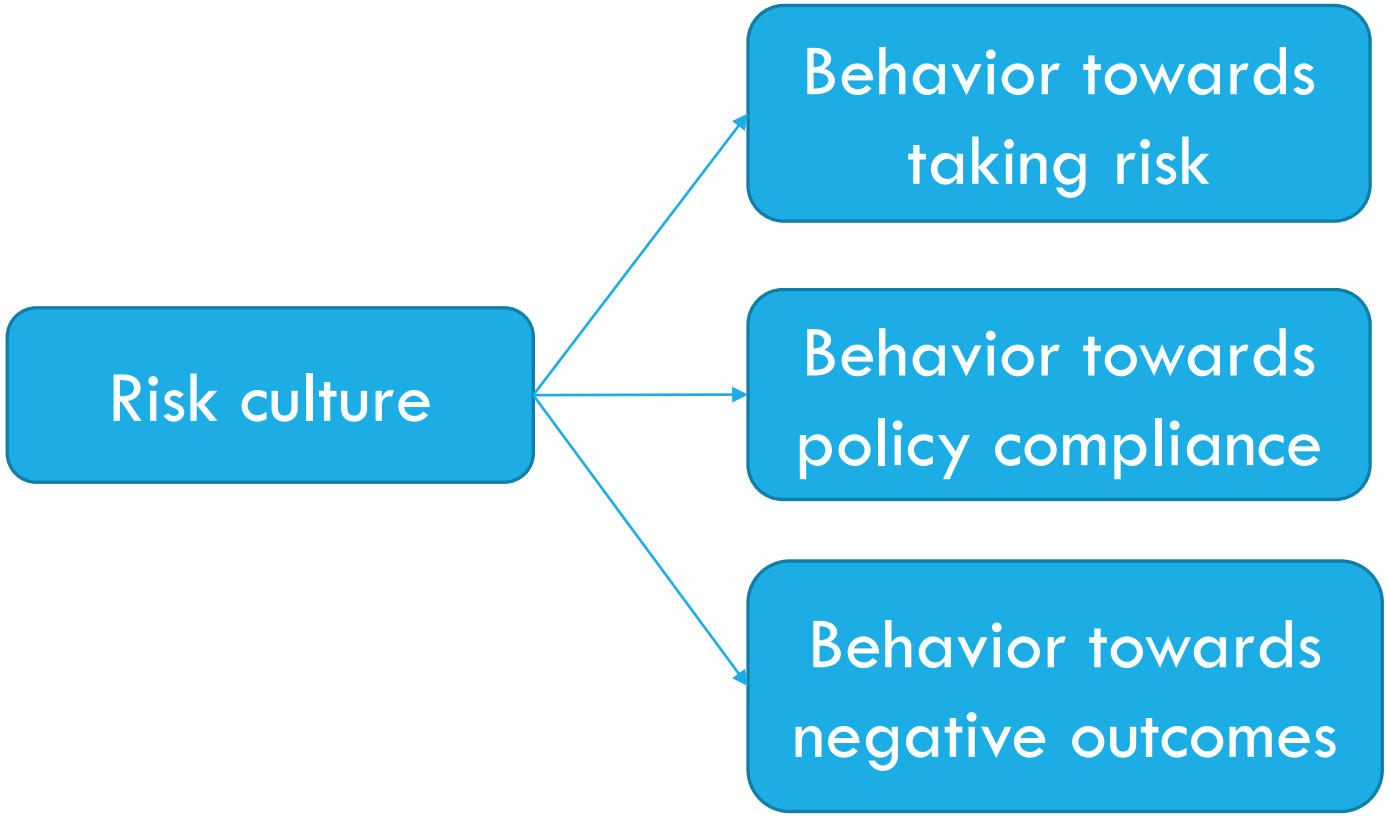
Leadership

Strategy

Tactics

ISACA RiskIT Framework

ISACA RiskIT Framework



FACILITATING A STRONG SECURITY CULTURE

Leadership should model good security practices

Invest

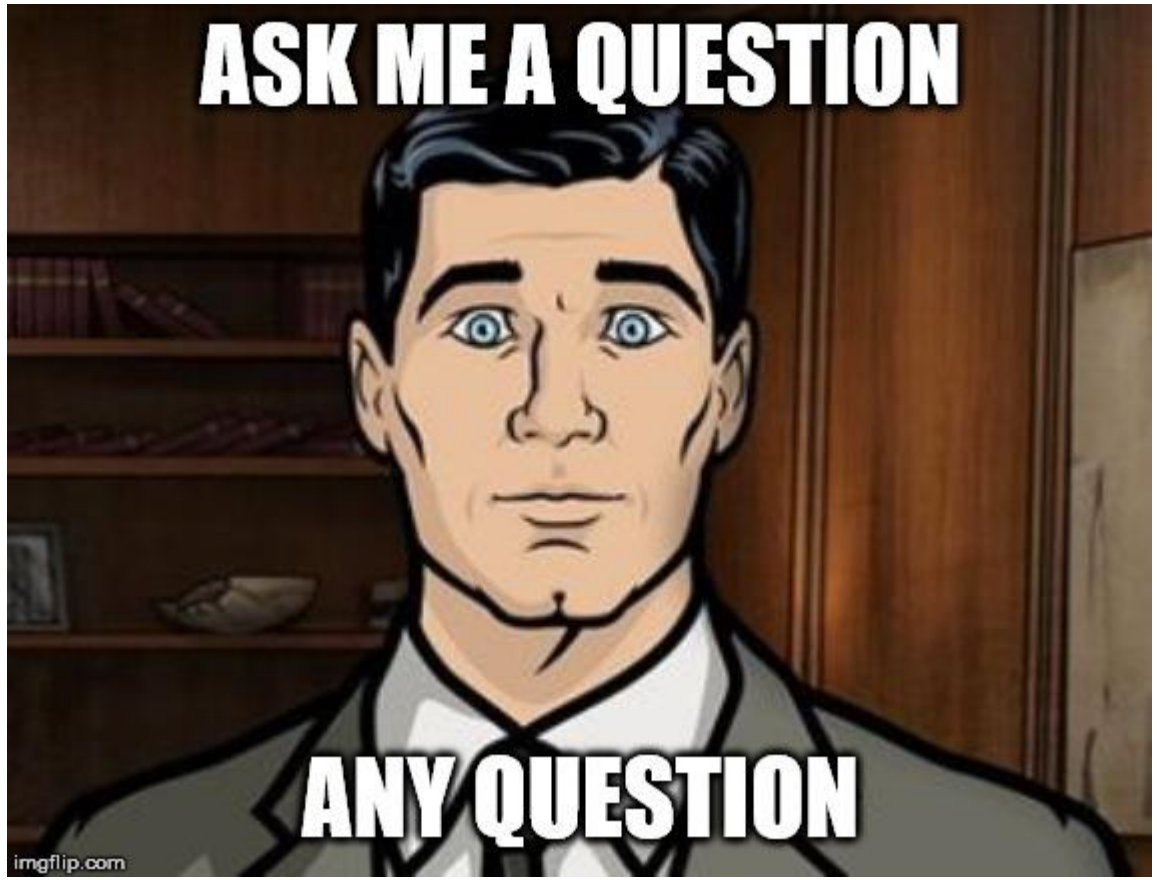
Security Champion program

Disrupt to facilitate change

Engaging and fun

Recognize and reward


Risk Culture
Position CISO
Strategy
Communicate Org Risk Tolerance
Roadmap for a risk-based security program
Tactics
Drive buy in for risk tolerance and roadmap
Foster openness about risk- problem solving


ASK ME A QUESTION
ANY QUESTION
imgflip.com

“There's never enough time.
Thank you for yours.” – Dan Geer

Don McKeown
donmckeown.net

ADDITIONAL RESOURCES

"Building a risk-based security culture," Don McKeown- https://donmckeown.net/Building_a_Risk-Based_Information_Security_Culture_-_Don_McKeown-4-2019-ISSA_Journal.pdf

Leveraging Organizational Change to Build a Strong Security Culture, Lance Spitzner, https://www.sans.org/webcasts/leveraging-organizational-change-build-strong-security-culture-115355