RSA Conference 2016

San Francisco | February 29 – March 4 | Moscone Center

Connect to Protect

SESSION ID: HUM-R04

People-Centric Security: Transform Culture, Reduce Risk, Drive Success

Dr. Lance Hayden

Managing Director, *Security Culture Practice*
Berkeley Research Group
@hay_lance

Masha Sedova

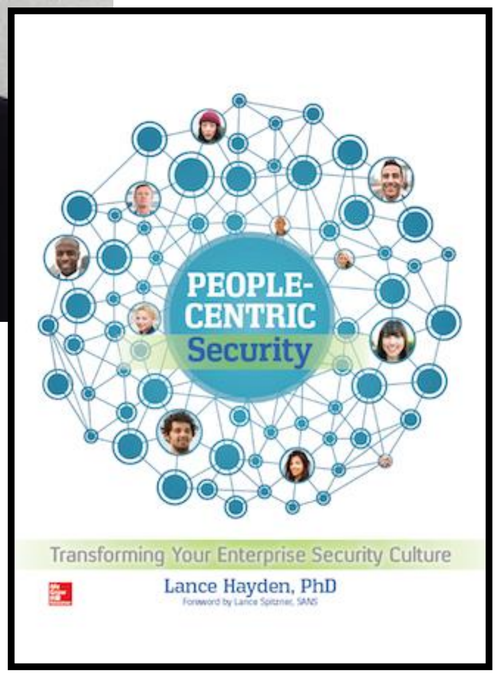
Senior Director, *Trust Engagement*
Salesforce
@modMasha

Today's Agenda

- Introductions
- Understanding and measuring security culture
- Case study: Security culture in practice at Salesforce
- How to transform your own security culture
- Application and call to action
- Q&A

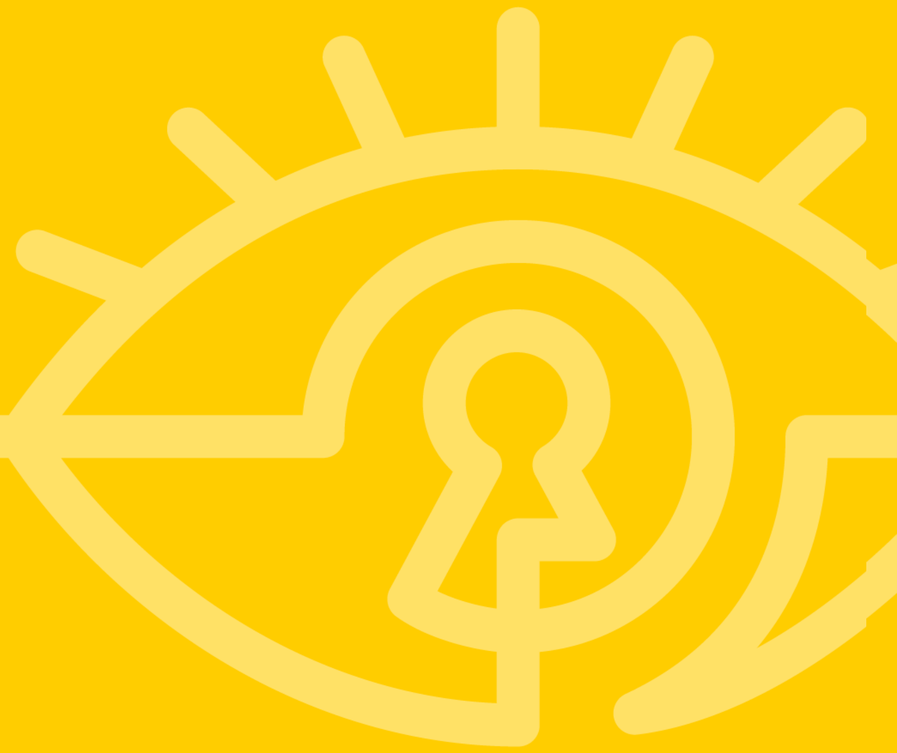
Introduction - Lance Hayden, Ph.D

- Managing Director at Berkeley Research Group
- Leads BRG's Cybersecurity Culture Practice
- Research and consulting to help organizations understand, measure, and transform security culture



Introduction - Lance Hayden

- Senior Director, Trust Engagement @ Salesforce
- Run a team of 6+ people focused on security culture
- Scope includes internal employees, engineers, developers, customers, and vendors

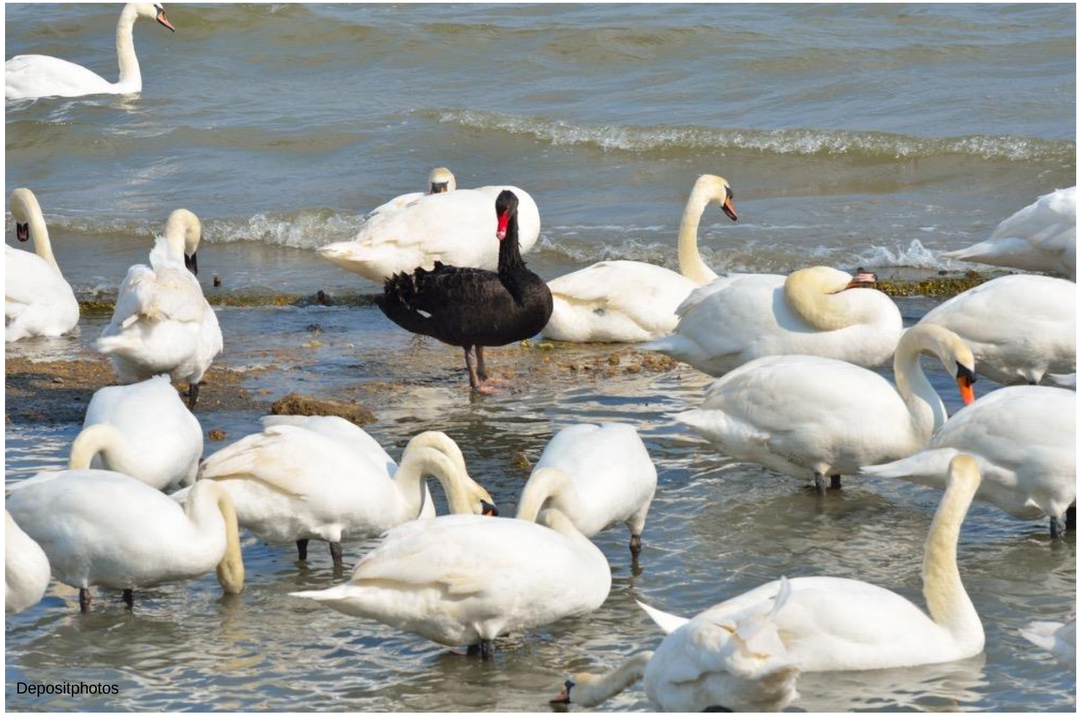


Understanding and Measuring Security Culture

A Comment on Theory…

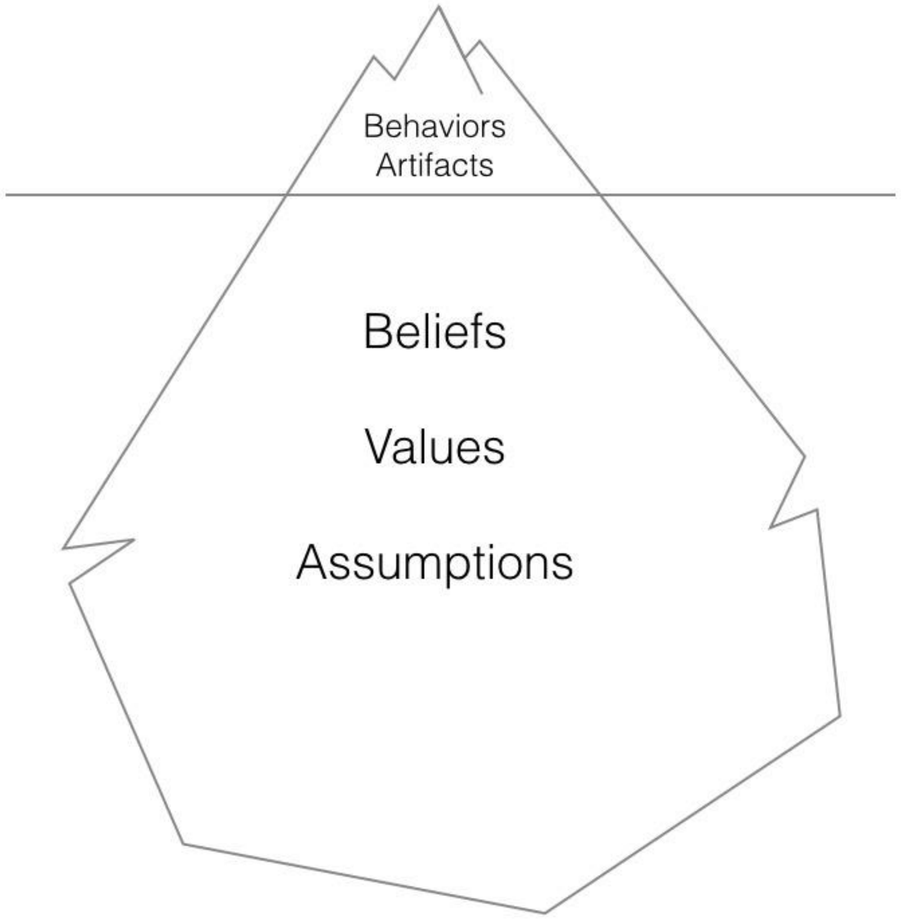
In theory there is no difference between theory and practice. In practice there is.

Yogi Berra



What is Security Culture?

- “The way we do things around here…”
- Invisible until you clash with a different one
- Incredibly hard to change unless you are starting one from scratch…



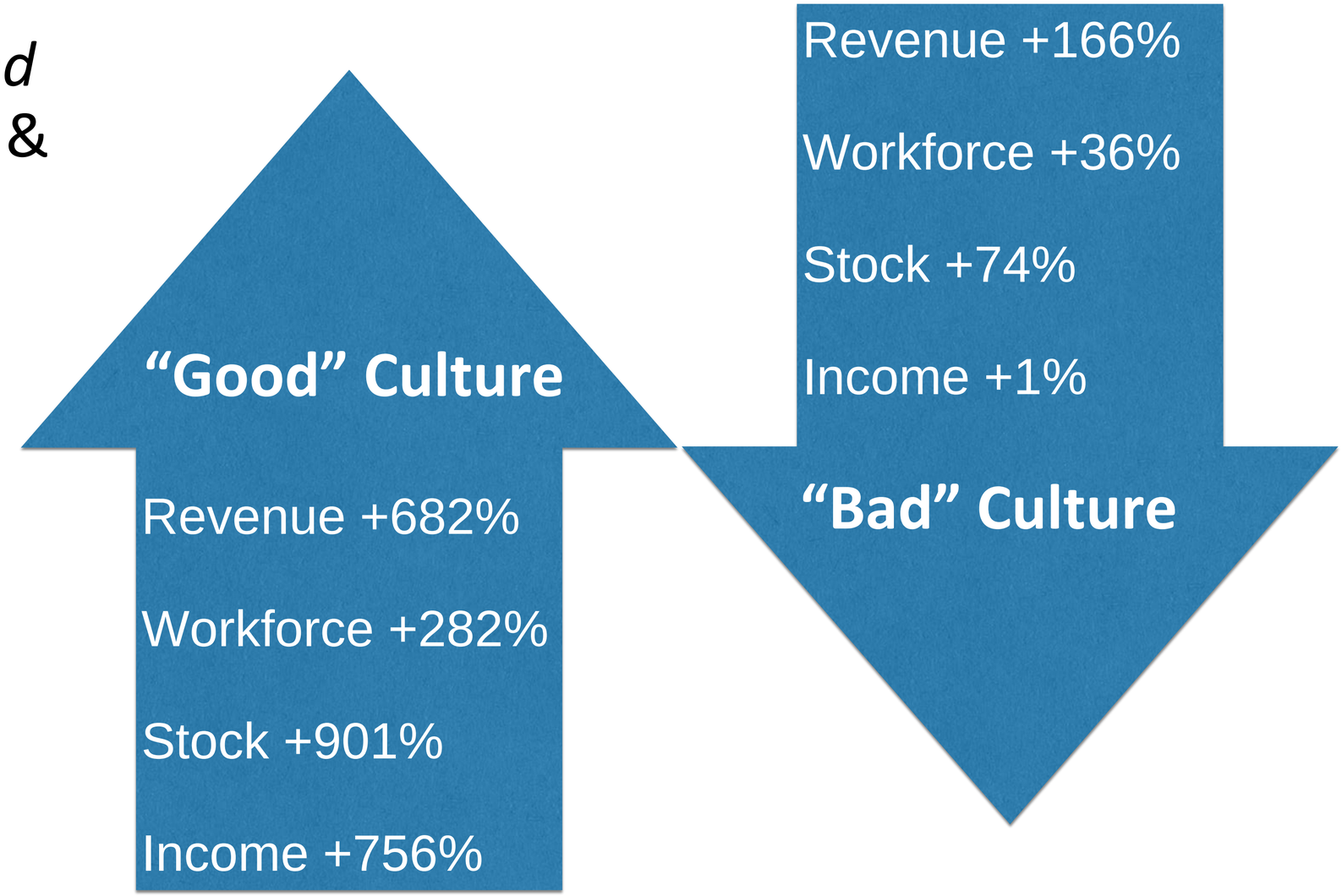
Culture and Behavior

“Culture eats strategy for breakfast.”

Peter Drucker

What is Security Culture?

- *Corporate Culture and Performance* (Kotter & Heskett)
- Research (and anecdotal) evidence that culture impacts organizational performance

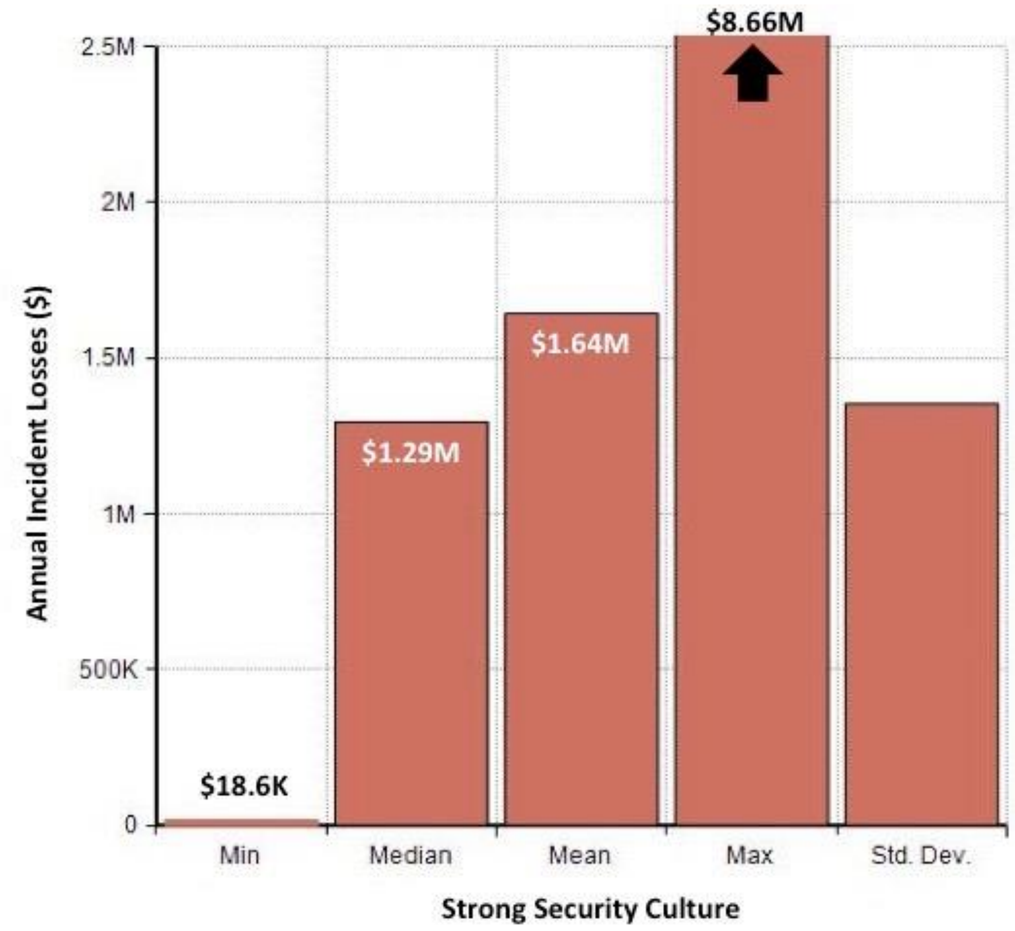


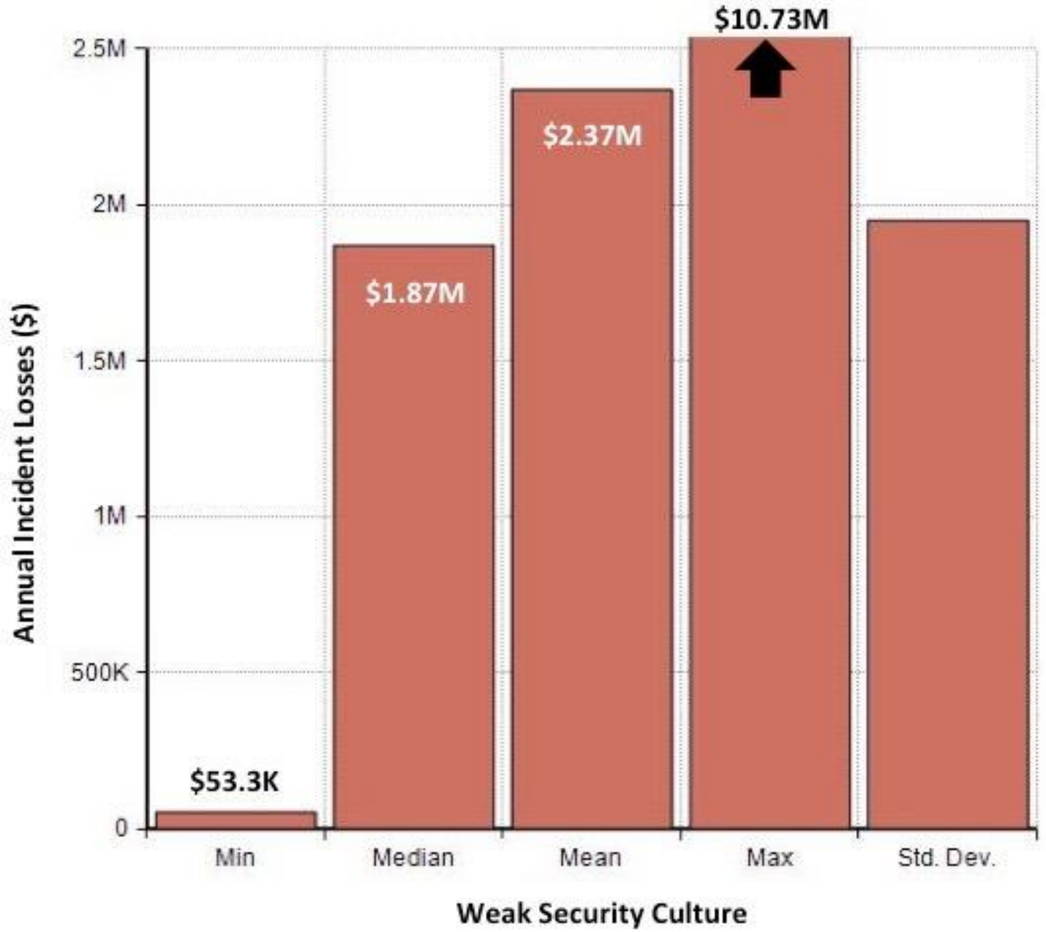
Security Culture and Security Risk

- Culture is about values and priorities (assumed and unspoken, “invisible”)
- Security risk increases when different values, priorities, and cultures compete for scarce resources
- “I have **3** goals to accomplish, and the time and resources to complete **2**…”
- Security often loses out to the competition (efficiency, usability, profit)

Depositphotos

Culture and Performance in Security

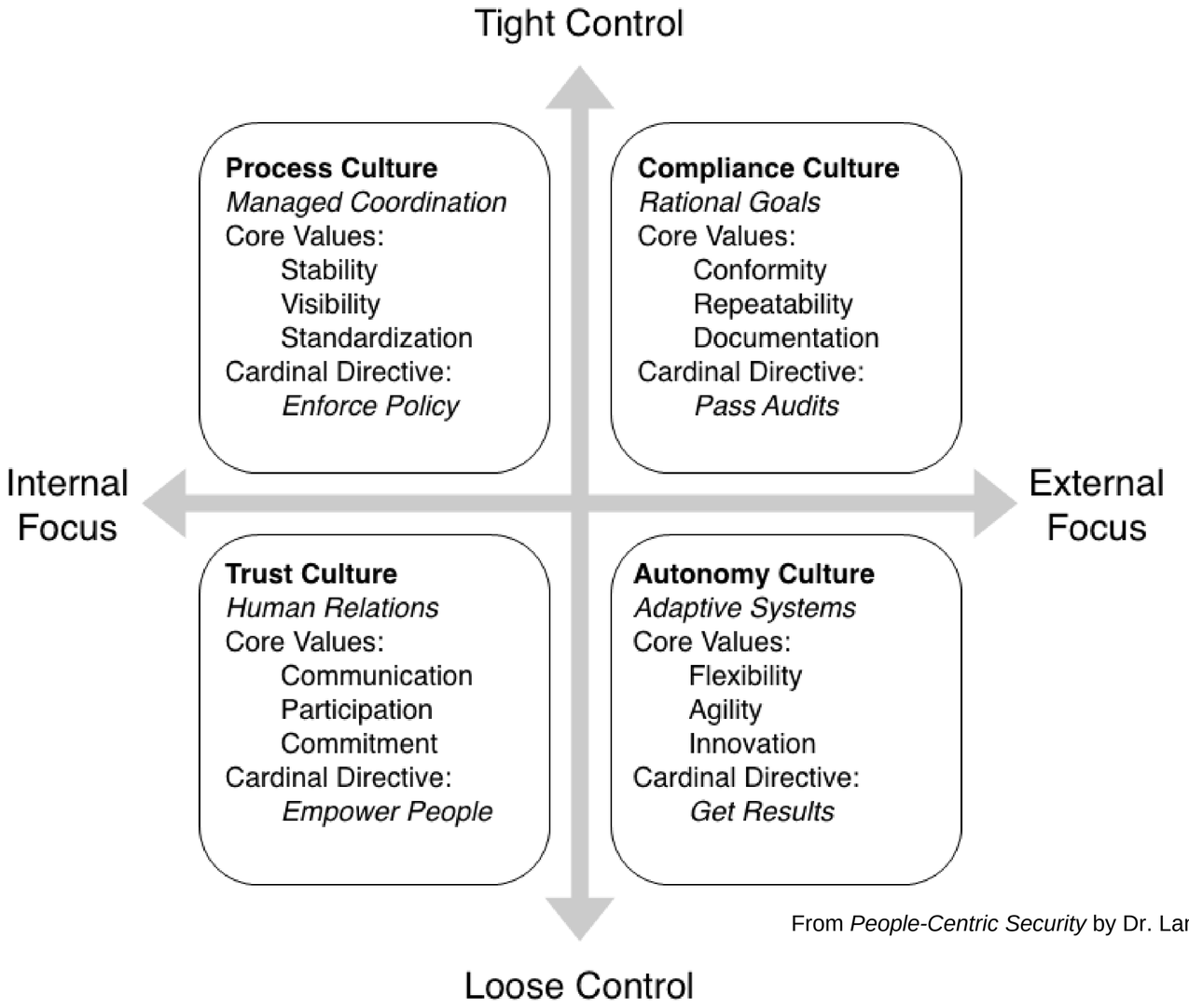




For the source of these findings, see http://securityispeople.lancehayden.net/2015/11/the-cost-of-a-bad-decision-measuring-the-impact-of-security-culture/

The Competing Security Cultures Framework

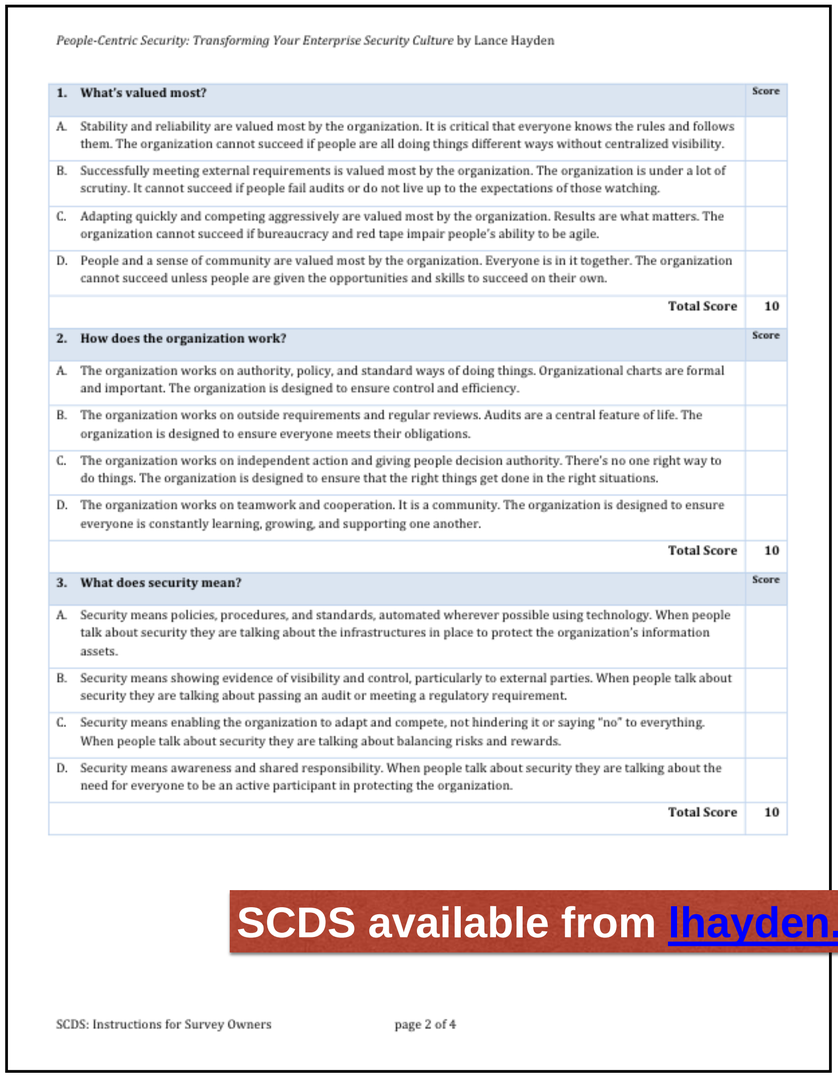
- Think of the CSCF as a personality test for your security program…
- Is your program a control freak? A conformist? A cowboy? A community builder?
- How do different personalities get along?



From *People-Centric Security* by Dr. Lance Hayden

Measuring and Mapping Security Cultures

- A measurement instrument (*Security Culture Diagnostic Survey*) provides data allowing visual mapping of a security culture
- Priorities, biases, and competing priorities become visualized



People-Centric Security: Transforming Your Enterprise Security Culture by Lance Hayden

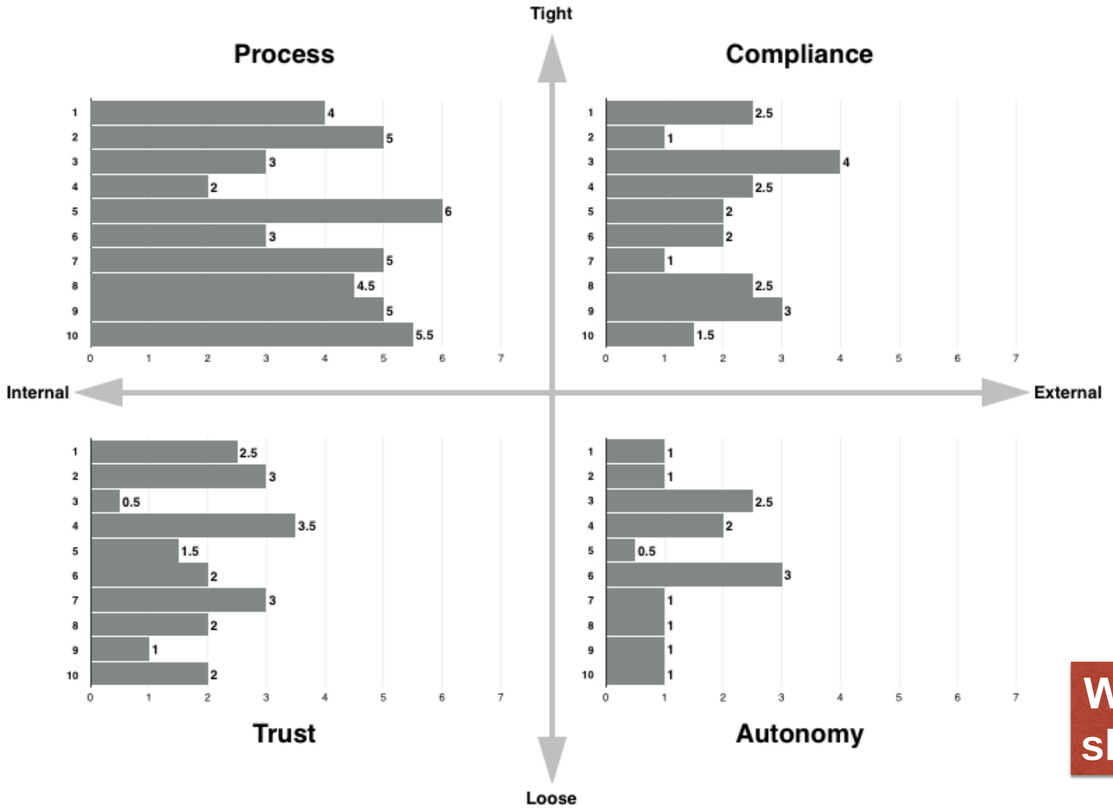
1.	**What's valued most?**	**Score**
A.	Stability and reliability are valued most by the organization. It is critical that everyone knows the rules and follows them. The organization cannot succeed if people are all doing things different ways without centralized visibility.	
B.	Successfully meeting external requirements is valued most by the organization. The organization is under a lot of scrutiny. It cannot succeed if people fail audits or do not live up to the expectations of those watching.	
C.	Adapting quickly and competing aggressively are valued most by the organization. Results are what matters. The organization cannot succeed if bureaucracy and red tape impair people's ability to be agile.	
D.	People and a sense of community are valued most by the organization. Everyone is in it together. The organization cannot succeed unless people are given the opportunities and skills to succeed on their own.	
	Total Score	**10**
2.	**How does the organization work?**	**Score**
A.	The organization works on authority, policy, and standard ways of doing things. Organizational charts are formal and important. The organization is designed to ensure control and efficiency.	
B.	The organization works on outside requirements and regular reviews. Audits are a central feature of life. The organization is designed to ensure everyone meets their obligations.	
C.	The organization works on independent action and giving people decision authority. There's no one right way to do things. The organization is designed to ensure that the right things get done in the right situations.	
D.	The organization works on teamwork and cooperation. It is a community. The organization is designed to ensure everyone is constantly learning, growing, and supporting one another.	
	Total Score	**10**
3.	**What does security mean?**	**Score**
A.	Security means policies, procedures, and standards, automated wherever possible using technology. When people talk about security they are talking about the infrastructures in place to protect the organization's information assets.	
B.	Security means showing evidence of visibility and control, particularly to external parties. When people talk about security they are talking about passing an audit or meeting a regulatory requirement.	
C.	Security means enabling the organization to adapt and compete, not hindering it or saying "no" to everything. When people talk about security they are talking about balancing risks and rewards.	
D.	Security means awareness and shared responsibility. When people talk about security they are talking about the need for everyone to be an active participant in protecting the organization.	
	Total Score	**10**

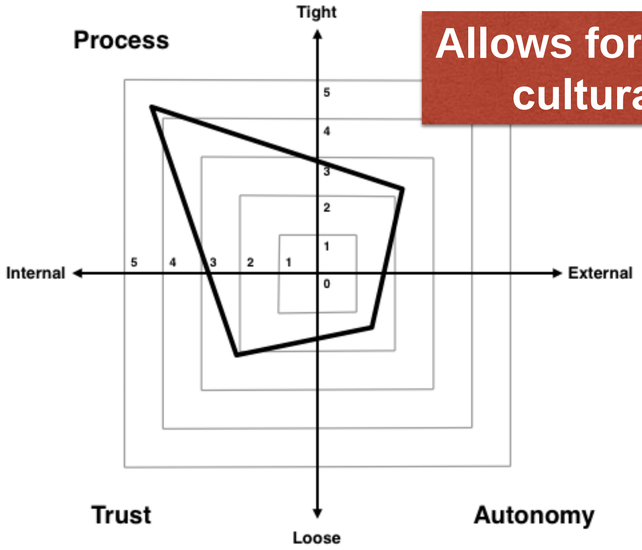
SCDS: Instructions for Survey Owners page 2 of 4

SCDS available from lhayden.net/culture

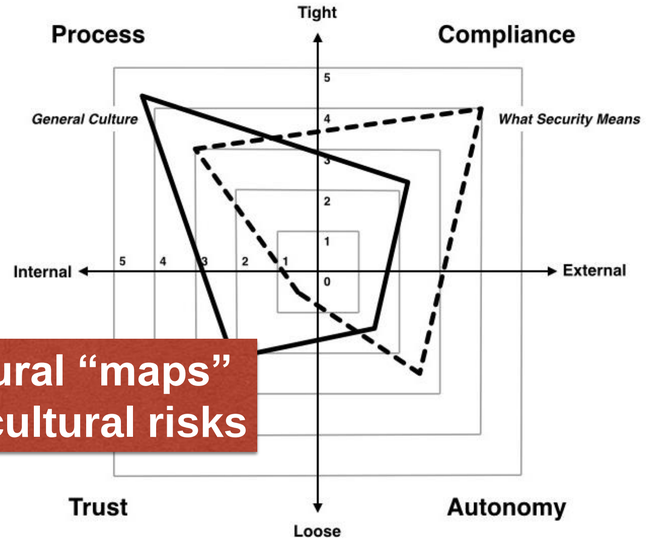
Measuring and Mapping Security Cultures

Granular SCDS response visualization





Allows for more intuitive cultural "shapes"



Which become comparative cultural "maps" showing potential conflicts and cultural risks

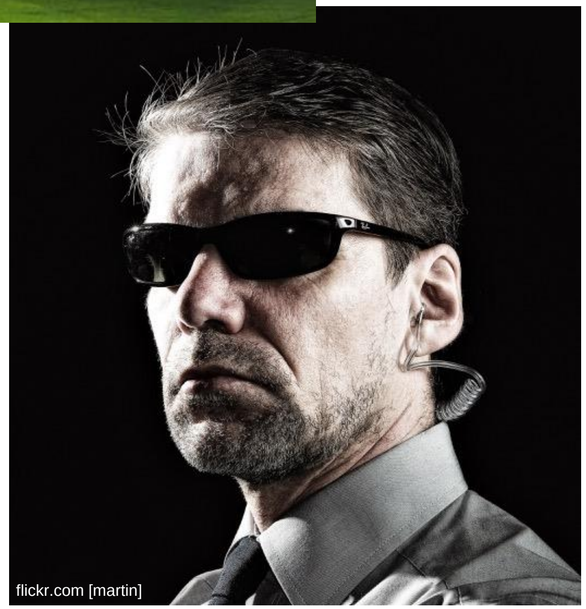
Case Study: Security Culture in Practice at Salesforce

Perception is Reality

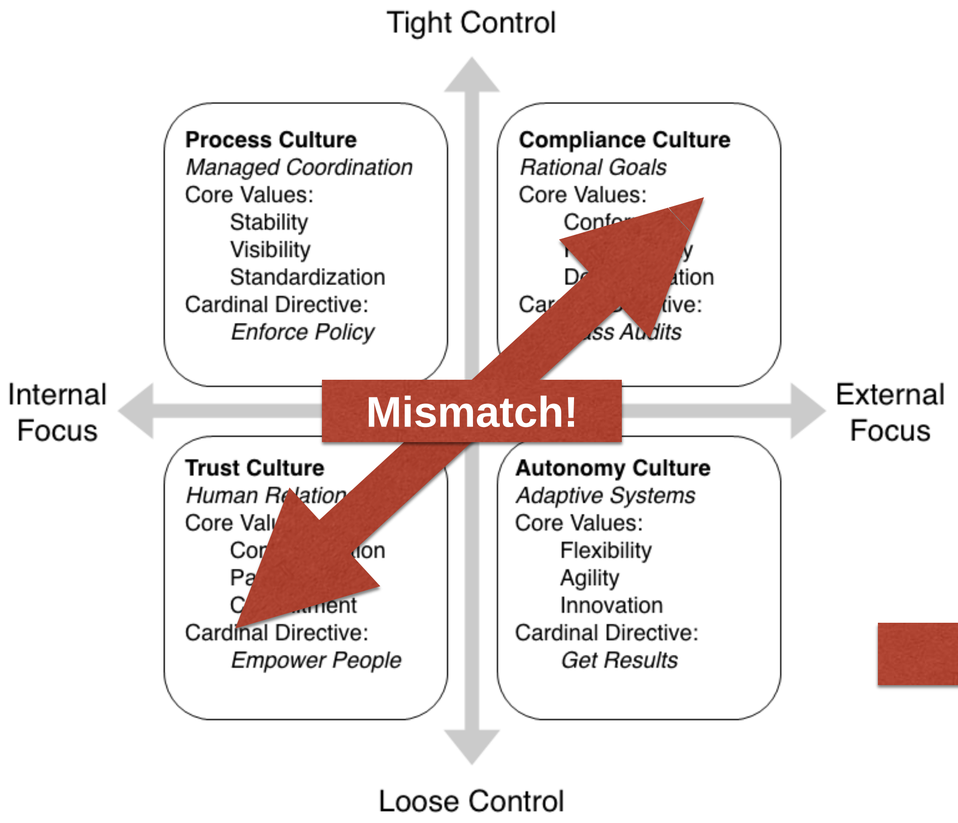

pixabay.com

flickr.com [sean macentee]

pixabay.com


flickr.com [martin]

Salesforce and the Culture Framework - Where We Were & Where We Wanted to Go



Assessment revealed a Compliance Culture

Company has a Trust Culture

Gamification: It's Not About Playing Games at Work…

- Though 70% of execs have admitted playing video games at work…

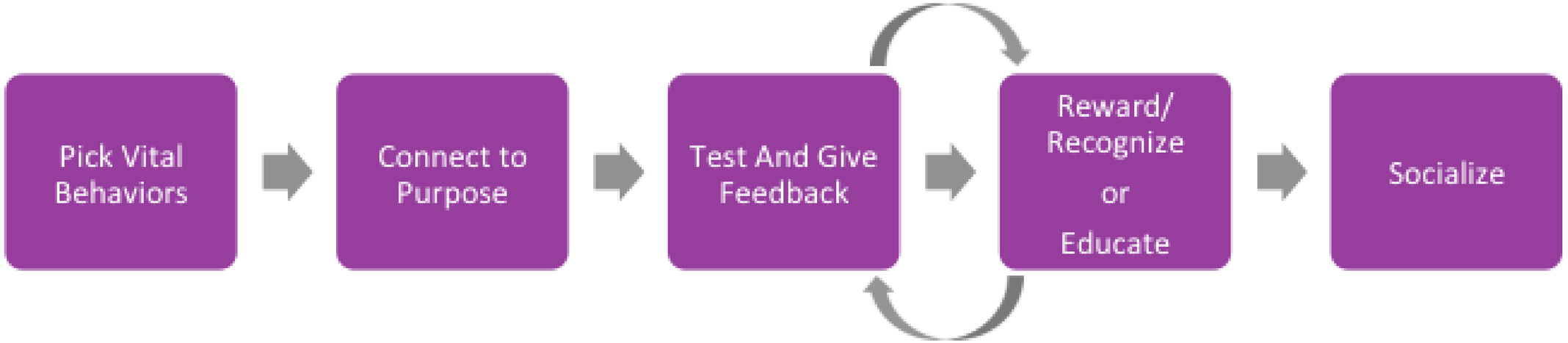
Information Solutions Group/PopCap White Collar Gamer Survey

Gamification Elements

1. **Autonomy:** we like having choices
2. **Mastery:** we like getting better at what we do
3. **Feedback:** we like getting feedback on how we are doing
4. **Purpose:** meaning amplifies what we do
5. **Social:** all this means more with others

Based on "Reality is Broken" by Jane McGonigal

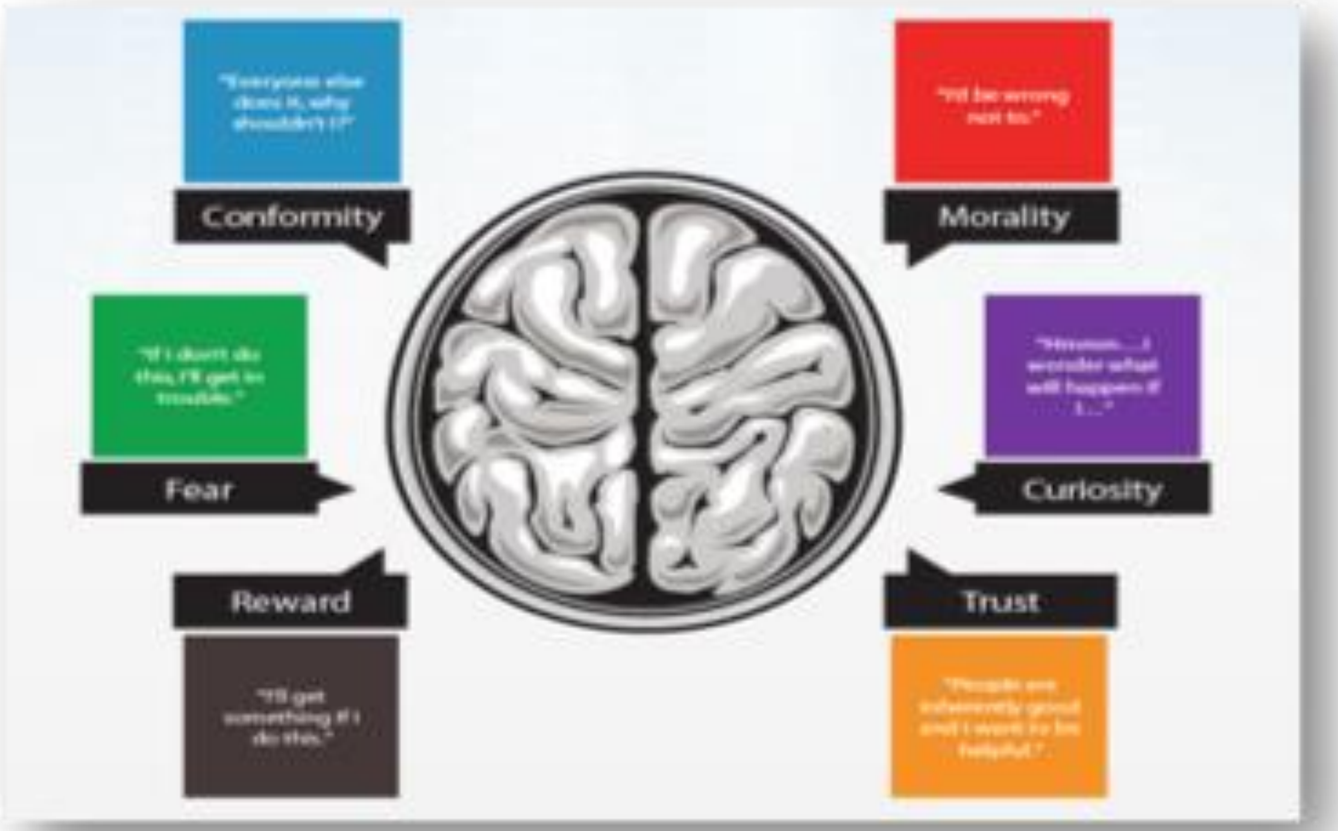
Gamifying Security



Vital Behaviors:
Phishing, Reporting, Badge Surfing

Connecting to Purpose

How attackers exploit bugs in “human hardware”…

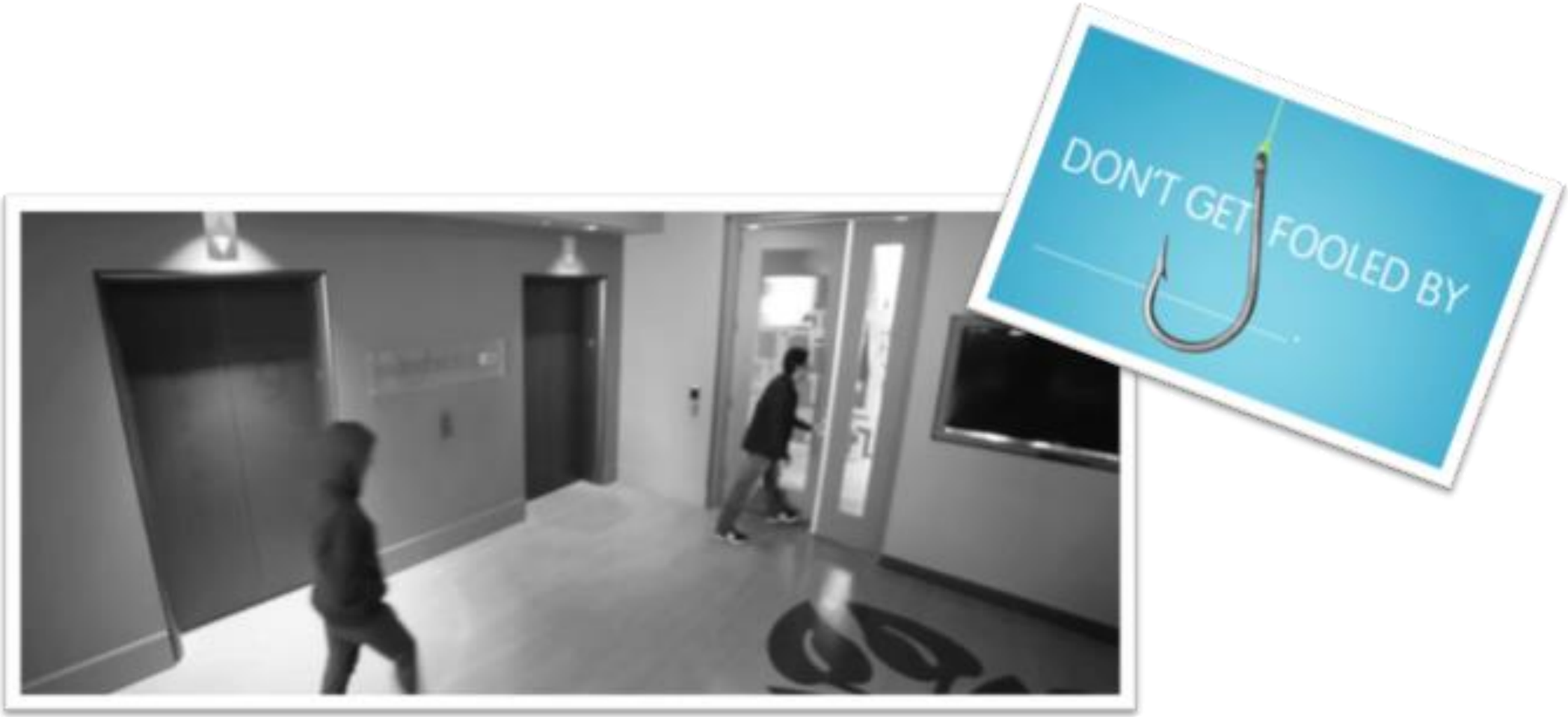


“Can you hold that office door open for me? My arm’s broken and this package is heavy…”

“Holy wow! Check out this video of a giant snake eating a zookeeper!”

“If you don’t pay the fine, your files will be locked and you will be reported to the FBI.”

Test with Feedback



Recognizing Badge-Surfing Awareness

Reward: Security Champion Program

Novice	Basic awareness

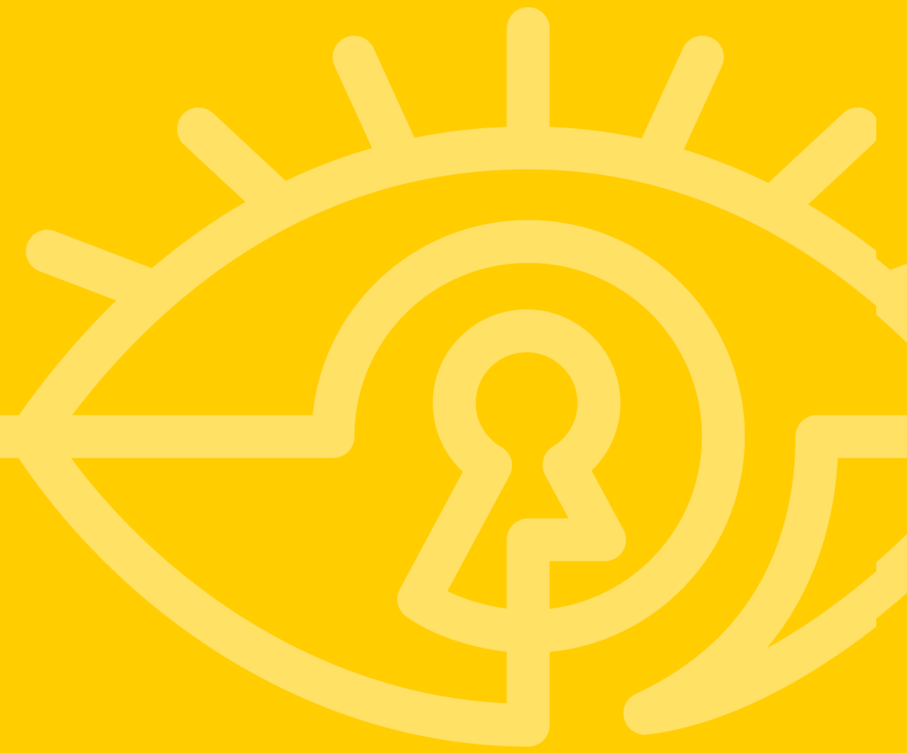
Apprentice	Successful Testing

Knight	Doing

Master	Teaching

Grand Master	Innovating

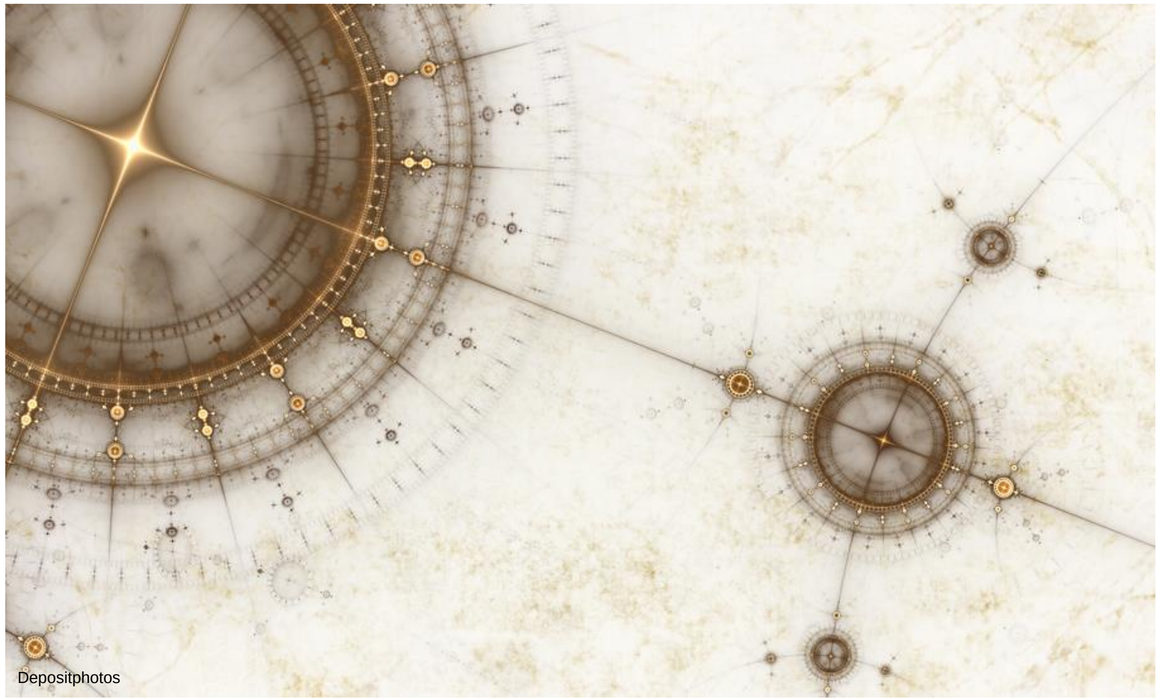
Trust Points



How to Transform Your Own Security Culture

Evaluating & Improving Security Culture

- You have to know where you are before you can get where you want to go
- Cultural maturity is about optimizing organizational self-awareness
- If culture was easy enough to change with an awareness campaign, every company would be innovative, fun, and secure



Culture as an Organizational Capability

- Culture is a capability
- Maturity is about measurement
- How do you know culture is changing?
- How do you know when it needs changing?
- How do you prove it?

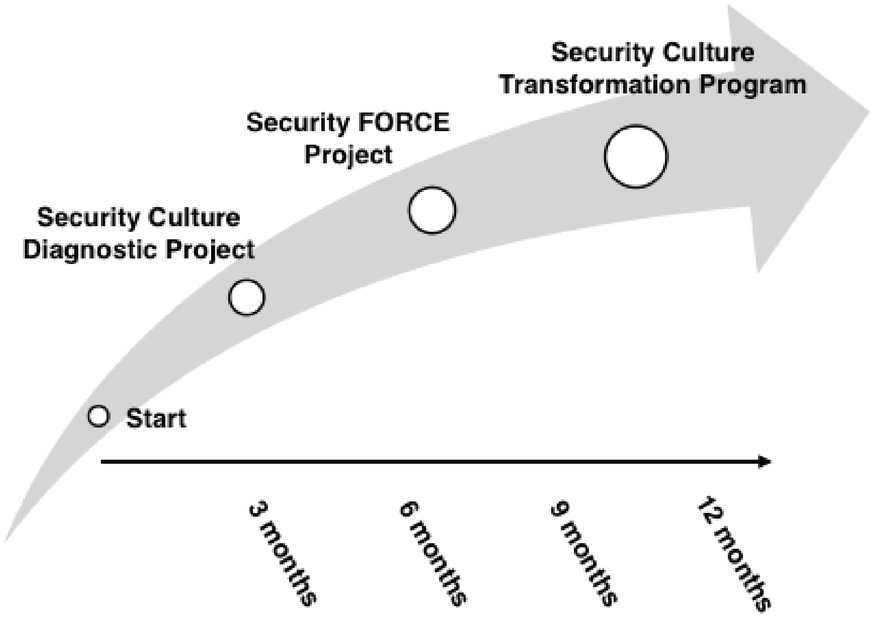
5 - Mastery

4 - Transformation

3 - Visibility

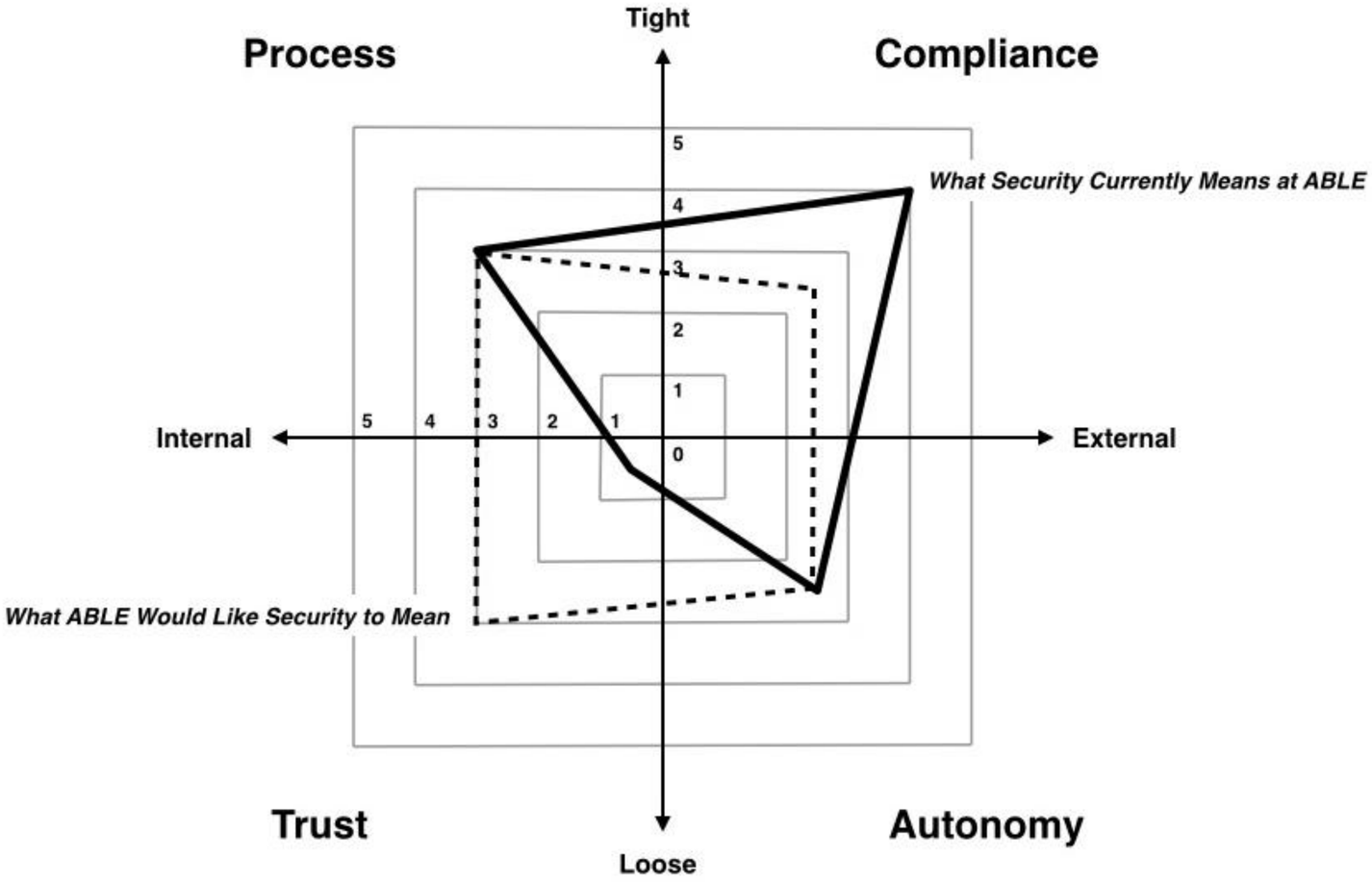
2 - Awareness

1 - Instinct



Mapping out a Transformation Plan

- Observe the terrain
- Orient the map
- Take a bearing
- Start moving…



Evaluating Cultural Change

- Maps show you where to go
- They also show you where you've been (and how much progress you have made)
- Cultural transformation projects must regularly self-evaluate
  - Repeated SCDS surveys over time to see changes in shape
  - Tying culture and awareness to behaviors and activities
  - Analyzing cultural ROI by tying behaviors to the business

Salesforce Culture Transformation: Outcomes and Impacts

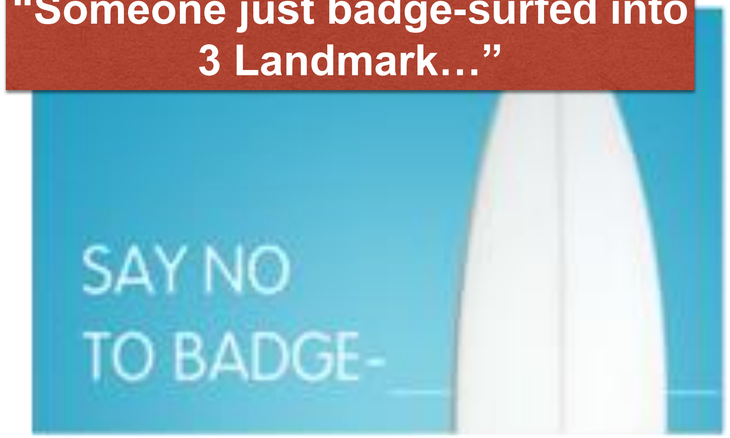
- Increase quantity/quality of reporting
- Social accountability
- Relationship to failure

Incident Detection

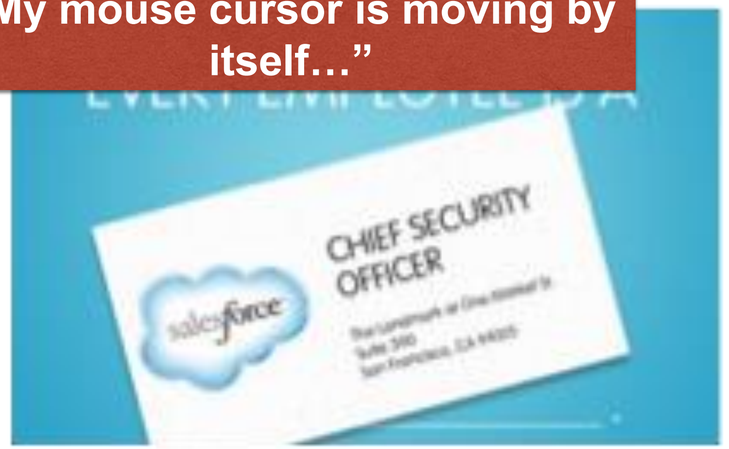
- Salesforce employees trained to report *any* suspicious activity.
- Customer reports also welcome.

“My browser proxy settings were changed…”

“Someone just badge-surfed into 3 Landmark…”



“My mouse cursor is moving by itself…”



“Is this email really from American Express..?”

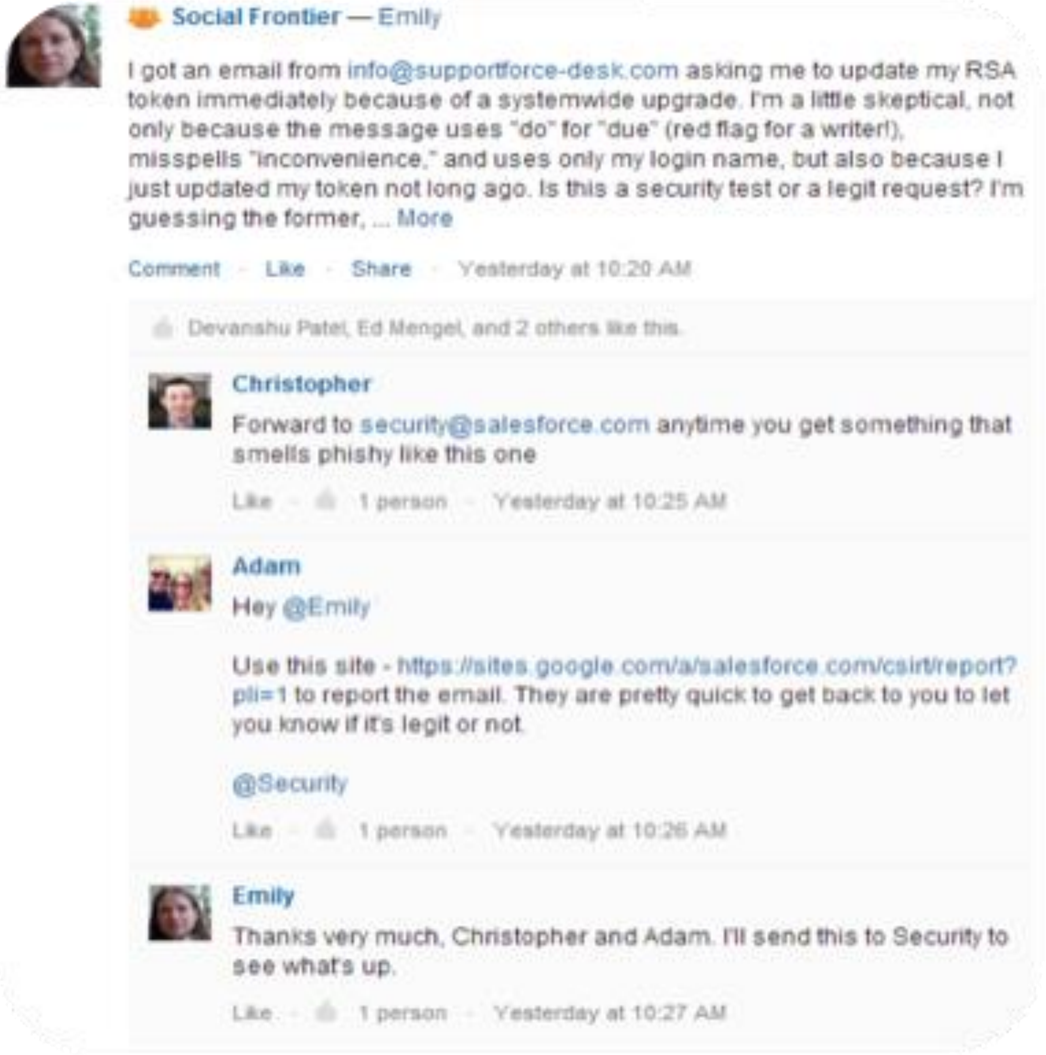
Results

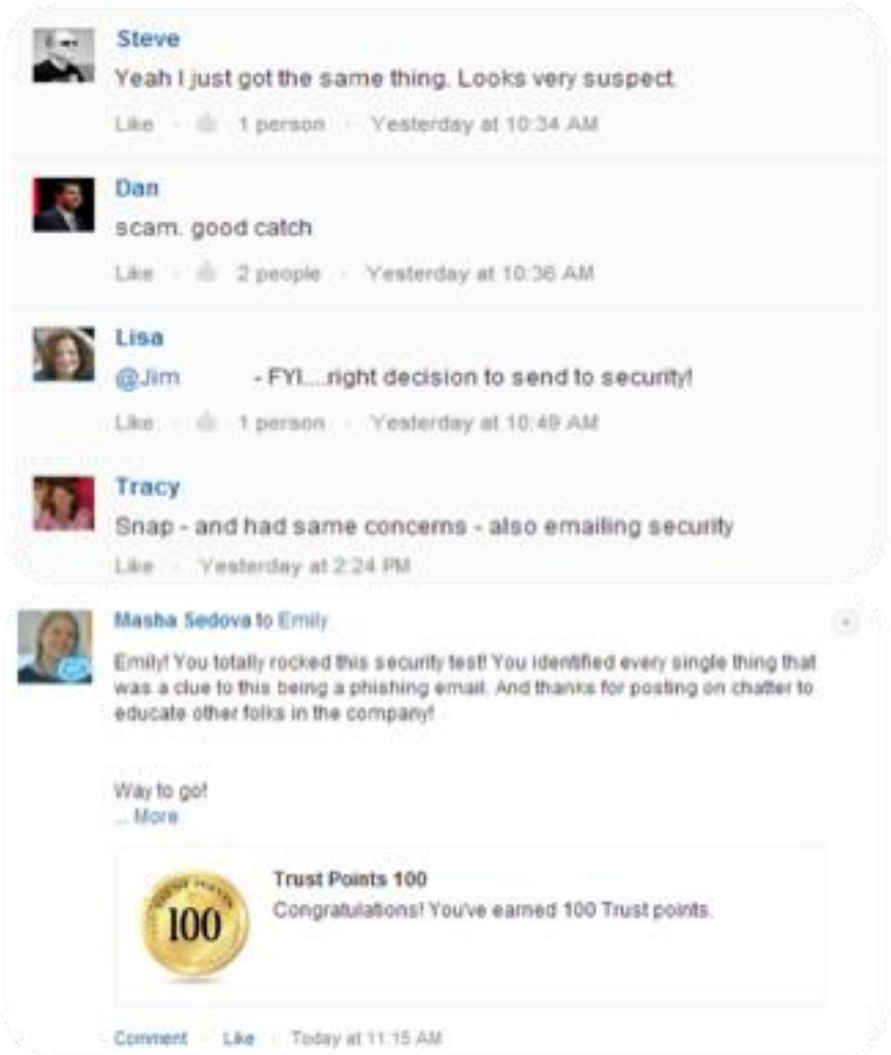
350% Increase in reporting rates in 6 months period across all employees

52% Less clicks on malicious links by champion program participants than the average Salesforce employee.

82% More reporting of threats than non-security champion program participants.

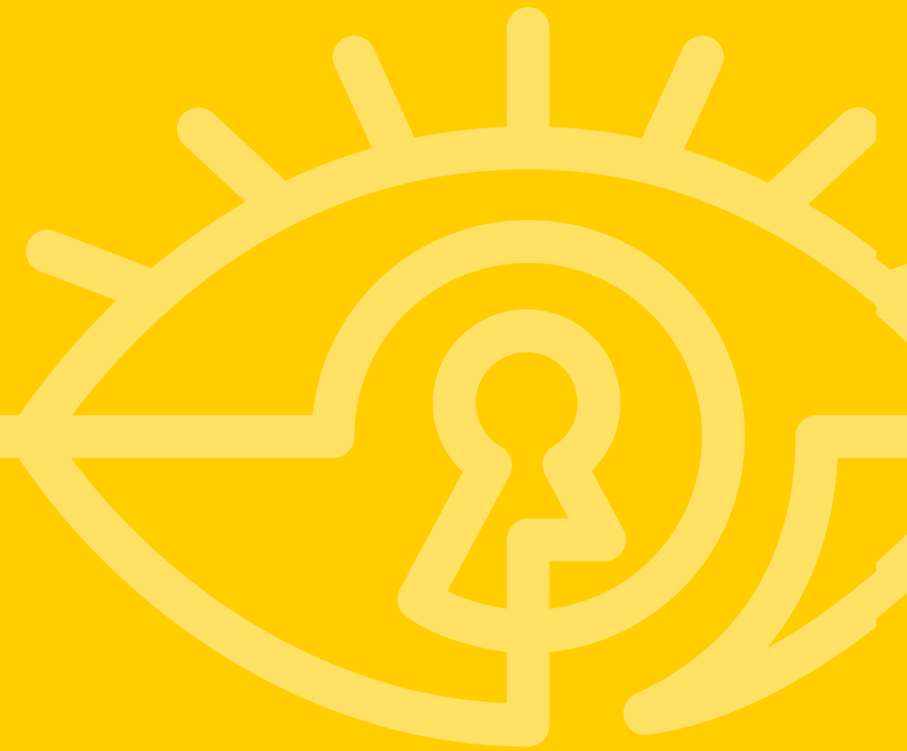
Community and Communications





Apply Cultural Transformation to Your Own Security Program

- **Next week**
  - Ask colleagues which culture you have (process, compliance, autonomy, or trust?) Do you get different answers?
  - Are there things that always get prioritized above security? Why?
  - Review your existing awareness program - is it aimed at changing what people ***do*** or what they ***think***?
- **Over the next 90 days**
  - Download the SCDS and conduct your own informal survey of your security culture; give it to your CISO
  - Assess your organization's security culture maturity - can you trace specific behaviors back to priorities and values?
  - Identify three improvements to your awareness program that are culturally specific (gamification, champions, etc.)
- **Over the next 6 months**
  - Document and evaluate how often security "loses" to other priorities - is it a lot?
  - Measure how well your awareness program improvements have changed the "shape" of your security culture
  - Formally expand your security awareness program, using your results, to drive culture and not just behaviors



Thank You! Any Questions?