RSAConference2018
San Francisco | April 16–20 | Moscone Center

SESSION ID: HUM-R14

SECURITY CULTURE HACKING: DISRUPTING THE SECURITY STATUS QUO

Christopher J. Romeo

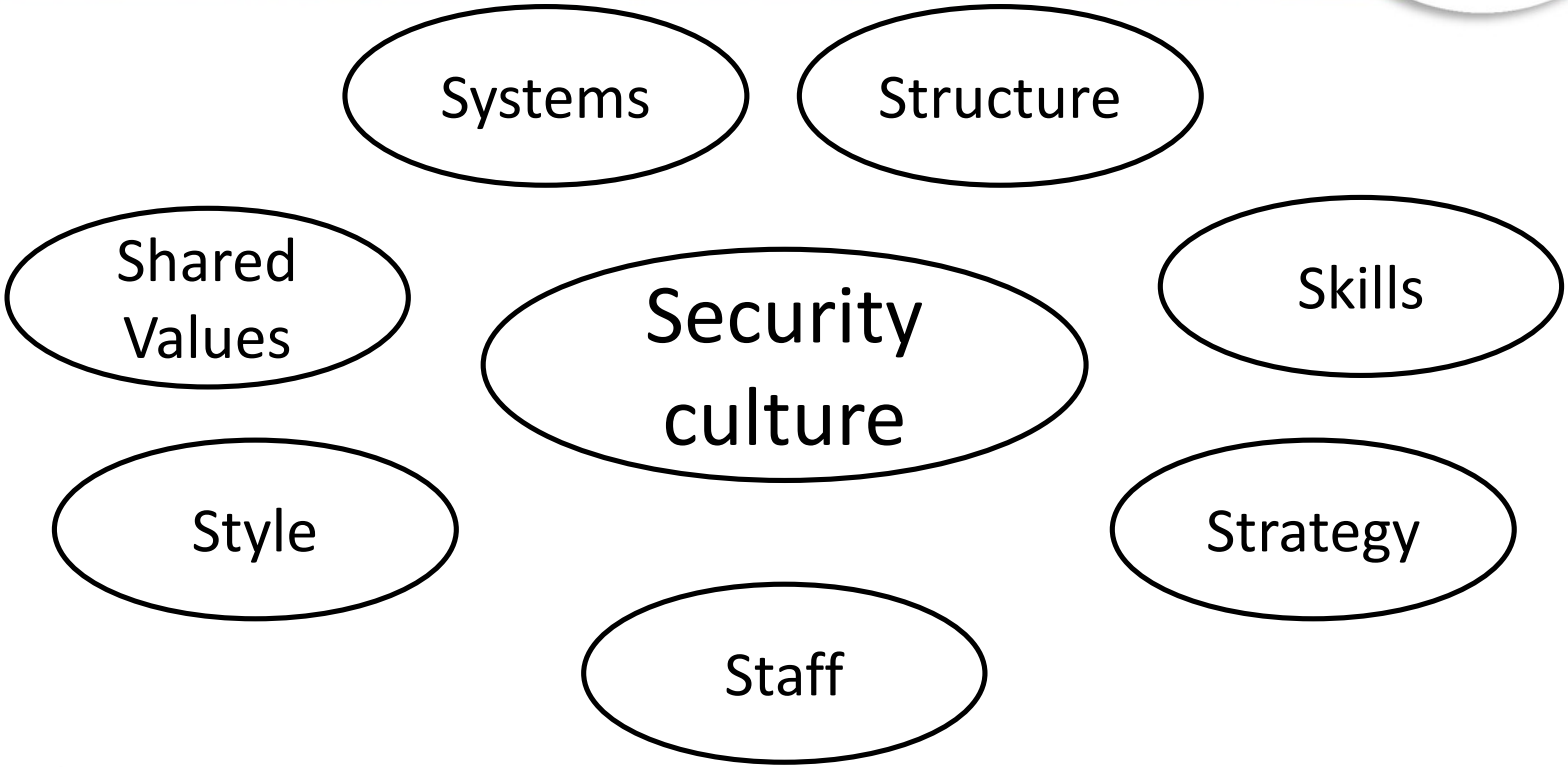
CEO
Security Journey
@edgeroute

Agenda

- Security culture hacking
- The security culture hacker
- How to hack a security culture
  - Phase 1: Assess
  - Phase 2: Communicate
  - Phase 3: Connect
  - Phase 4: Teach
  - Phase 5: Reward
- Where to start and year one


SECURITY CULTURE
I AM YOUR WORST ENEMY
memegenerator.net

Security culture



The reality of security culture

What happens **with security** when people are left to their own devices.

Security culture goals

Security Journey

Avoid the security status quo

Security culture is a long game

“Security” people	Security interested	Early Majority	Forced compliance	Not going to happen
0-3 months	3-12 months	1-2 years	2-4 years	Never

Security Journey

Security culture that lasts

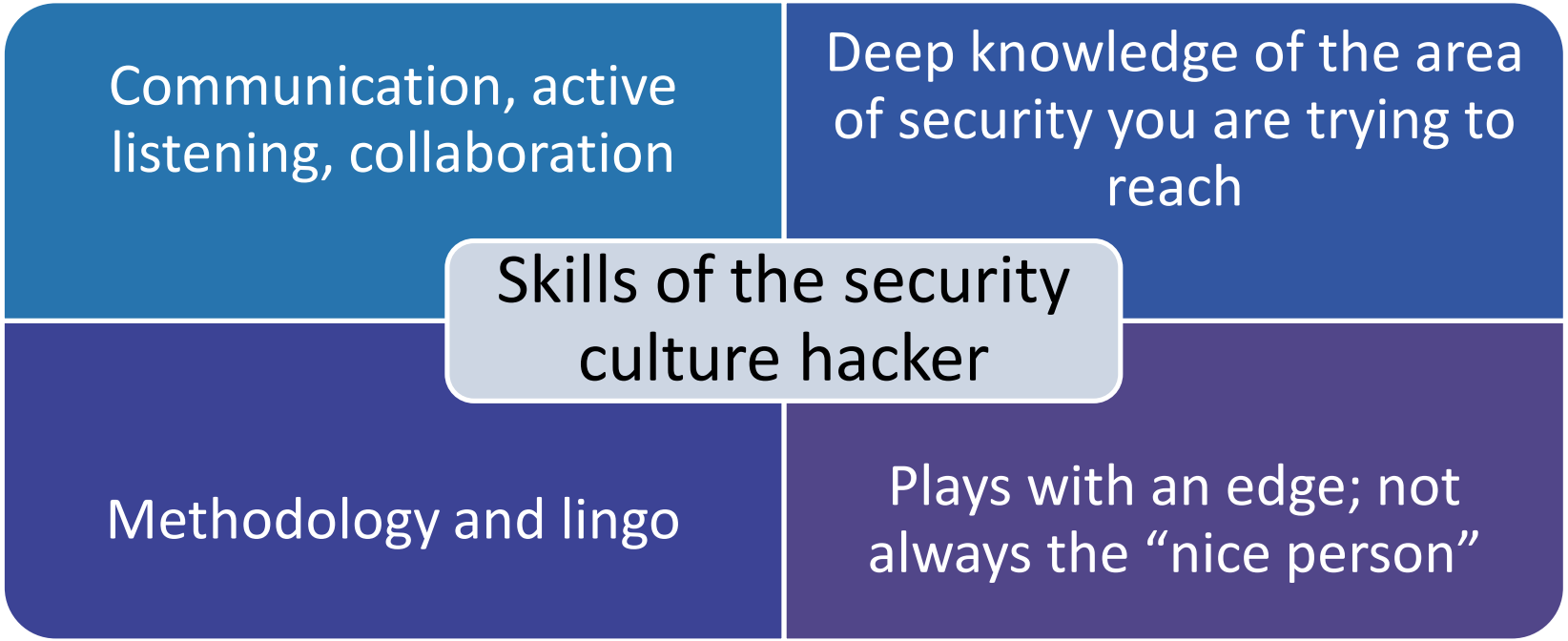
- A plan with a disruptive edge 
- Fun for all parties involved 
- Rewards engage with stuff 
- Return on investment via metrics 

Security Journey

Security culture hacking

Security culture hacking = applying a series of shortcuts or tricks for getting an org to focus on security, one person at a time.

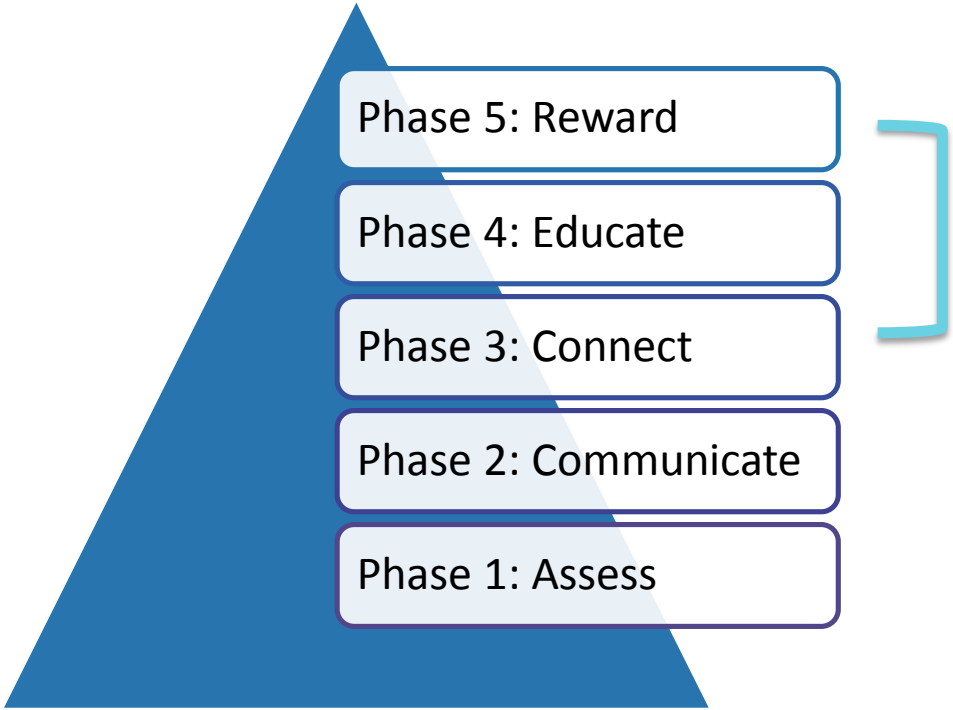
Security Journey


Communication, active listening, collaboration
Deep knowledge of the area of security you are trying to reach
Skills of the security culture hacker
Methodology and lingo
Plays with an edge; not always the “nice person”

Inverse of a social engineer

Social Engineer	Security Culture Hacker
Black hat / works for evil	White hat / works for good
Break in	Build up
Uses phishing, vishing, impersonation	E-mail, web conference, and face-to-face meetings
Calls Execs to steal passwords	Calls Execs to protect passwords
Persuasion skills	

How to hack a security culture



Security Journey

Phase 1: Assess

Goal: Create a strategy based on where the organization needs to go in the quest for a strong security culture.

Assessment random sampling

Information Security

Developers

Executives

Program Managers

Finance

HR

Security Journey

RSAConference2018

A simple self-assessment

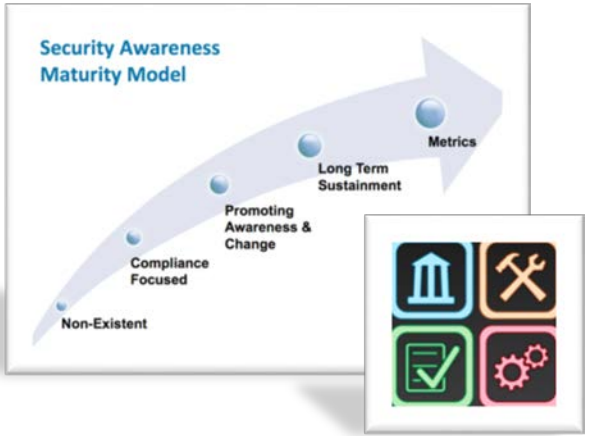
- What does security mean to us as an organization?
- How do we “do security”? How does security impact each job role?
- How risky is our application fleet or data that we store?
- Who are the attackers we face?
- Do we do high-level security awareness training? Role-specific?
- Ever heard of a secure design principle? What are some that we apply?
- Do we have a security response team? How do we contact them?

Case study: water cooler

Assessment tips for success

Time box

Assess --> Strategy

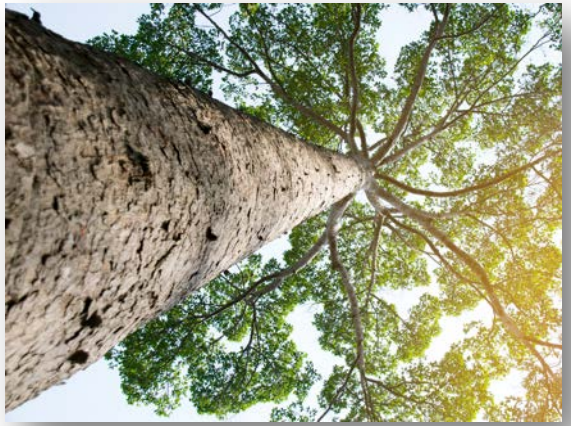


Other sources

Phase 2: Communicate

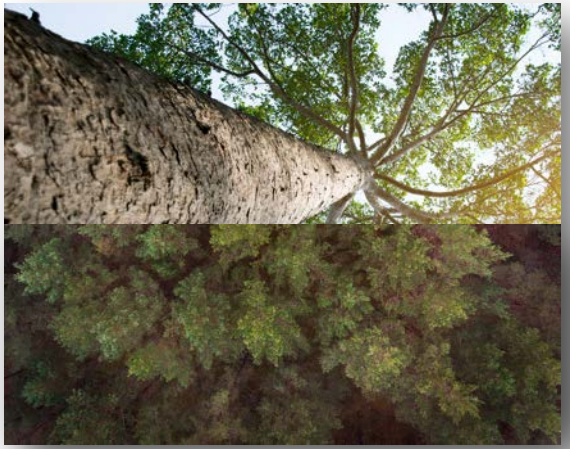
Goal: Reach out to people from across the organization, at all levels, and tell them about security.

Various communication approaches



Bottoms up

Top down



Hybrid

Case study: scare tactics

Break whatever you build in front of your Executives

Communication tips for success

Strategy

Travel

Face to face

Phase 3: Connect

Advocates
Ambassadors
Champions
Guilds

Goal: Educate about security and embed expertise within every team.

Security Journey

Champion case study

Champion tips for success

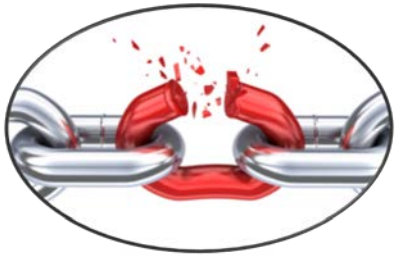
- Organizational distribution
- Clear roles and expectations
- Management support and buy-in is mandatory
- Program as destination; create a program that people seek out
- Invest in the champions and they will pay it forward

Champion activities

Monthly training

Online community

Mini-conference



Spot the flaw

Hack-a-thons

Full conference

Security Journey

Phase 4: Educate

Goal: Provide meaningful, transformational security education that everyone wants to consume.

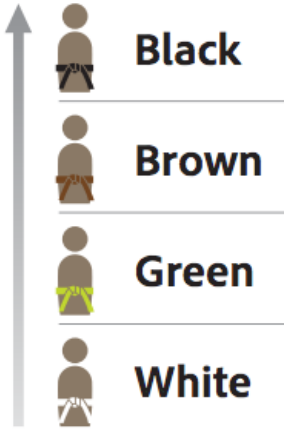
Mechanisms of security learning

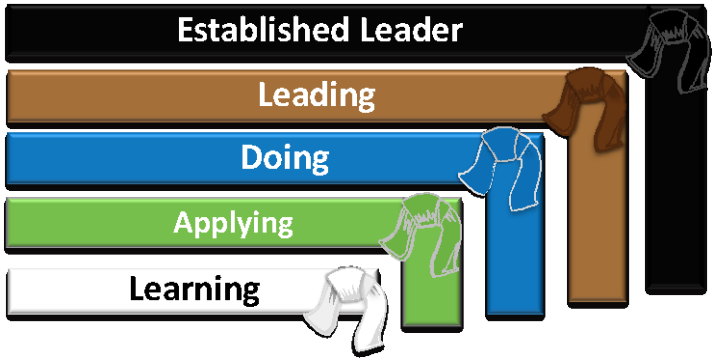
Video

Classroom

Hands-on

Continuous security education case study





Apprentice	Basic awareness
Padawan	Successful Testing
Jedi Knight	Doing
Jedi Master	Teaching
Jedi Grand Master	Innovating

Continuous security education tips for success

- Begin with the foundations; never assume base knowledge
- Start with why; focus on why the learner needs to care
- Connect “Security Champions” with the education program
- Recognize individual achievements or levels
- Pick a fun theme and market the program using the theme
- Role-specific education

Phase 5: Reward

Goal: Use more carrot and less stick to encourage the adoption of security culture.

Reward using the tools you already have

Good job in front of team

E-mail

Gift cards

Cash

Enhanced training

External conferences

Rewards case study

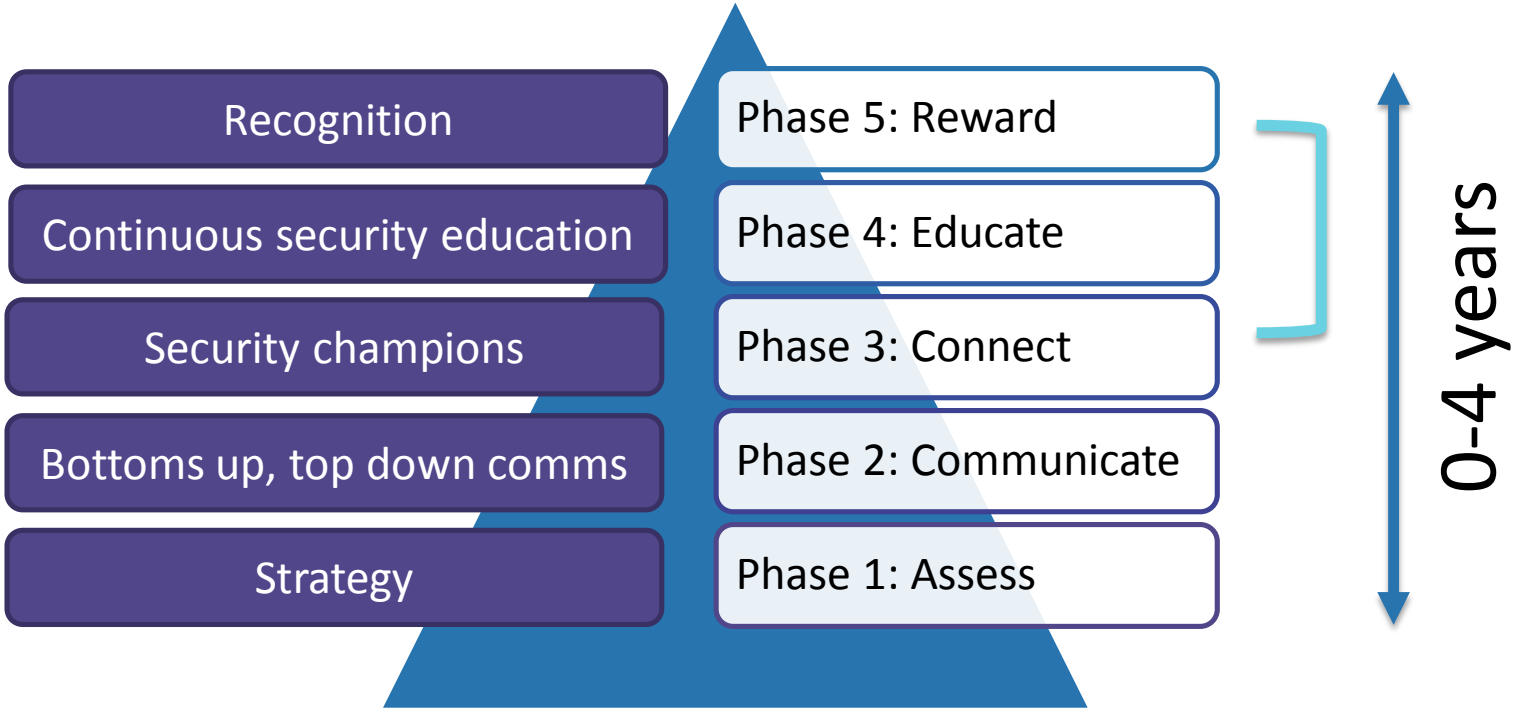
Rewards tips for success

- Ask team members for reward ideas
- Plug into existing organizational rewards and recognition programs
- Reward early and often; a rewards program is not a place to by stingy

Data (Metrics)

- Flaw prevalence -- lower count of vulnerabilities and security bugs
- Security bug fix rate
- Physical security incidents (tailgating)
- Total number of people that reach each education level
- Total number of security activities
- Security community engagement
- Positive engagements with the security team

A ”hacked” security culture



“Apply” Slide

- Next week you should:
  - Begin the security culture assessment process and build out a culture strategy
- In the first three months following this presentation you should:
  - Begin the communicate phase (ongoing forever), and connect at grass roots and Executive levels
  - Begin the process of identifying rewards and recognition
- Within six months you should:
  - Launch your Security Champions program
  - Deploy continuous security education
  - Continue rewards and recognition roll-out

Q+A and Thank you!

Chris Romeo, CEO / Co-Founder

chris_romeo@securityjourney.com

www.securityjourney.com

@edgeroute, @SecurityJourney

Security Journey

RSAConference2018