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
Security culture

- Systems
- Structure
- Shared Values
- Skills
- Style
- Strategy
- Staff
The reality of security culture

What happens with security when people are left to their own devices.
Security culture goals

- Shared responsibility for security
- A mentality of security first
- Role-specific, base level knowledge of security
- Demonstrate impact of security investment
Avoid the security status quo

THE SECURITY STATUS QUO IS A JOKE.
Security culture is a long game

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

= applying a series of shortcuts or tricks for getting an org to focus on security, one person at a time.
<table>
<thead>
<tr>
<th>Communication, active listening, collaboration</th>
<th>Deep knowledge of the area of security you are trying to reach</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Skills of the security culture hacker</strong></td>
<td><strong>Plays with an edge; not always the “nice person”</strong></td>
</tr>
<tr>
<td>Methodology and lingo</td>
<td></td>
</tr>
</tbody>
</table>
#RSAC

Inverse of a social engineer

<table>
<thead>
<tr>
<th>Social Engineer</th>
<th>Security Culture Hacker</th>
</tr>
</thead>
<tbody>
<tr>
<td>Black hat / works for evil</td>
<td>White hat / works for good</td>
</tr>
<tr>
<td>Break in</td>
<td>Build up</td>
</tr>
<tr>
<td>Uses phishing, vishing, impersonation</td>
<td>E-mail, web conference, and face-to-face meetings</td>
</tr>
<tr>
<td>Calls Execs to steal passwords</td>
<td>Calls Execs to protect passwords</td>
</tr>
</tbody>
</table>

Persuasion skills
How to hack a security culture

Phase 5: Reward
Phase 4: Educate
Phase 3: Connect
Phase 2: Communicate
Phase 1: Assess
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
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

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

Advocates
Ambassadors
Champions
Guilds
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
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
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

San Jose State University logo
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 be 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

- Phase 1: Assess
- Phase 2: Communicate
- Phase 3: Connect
- Phase 4: Educate
- Phase 5: Reward

- Strategy
- Bottoms up, top down comms
- Security champions
- Continuous security education
- Recognition

0-4 years
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