CHANGING SECURITY CULTURE

Christopher J. Romeo
CEO
Security Journey
@edgeroute
Agenda

- Security culture hacking and the security culture hacker
- A process to hack security culture
  - Phase 1: Assess
  - Phase 2: Communicate
  - Phase 3: Connect
  - Phase 4: Teach
  - Phase 5: Reward
- An interactive case-study in security culture hacking
The reality of security culture

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

- Shared responsibility for security – “everyone is a security person”
- A mentality of security first
- Role-specific, base level knowledge of security
- Demonstrate impact of security investment
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 (dev vs. gen)</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Skills of the security culture hacker</strong></td>
<td>Plays with an edge; not always the “nice guy or girl”</td>
</tr>
<tr>
<td>Methodology and lingo</td>
<td></td>
</tr>
</tbody>
</table>
Inverse of a social engineer

<table>
<thead>
<tr>
<th>Social Engineer</th>
<th>Security Culture Hacker</th>
</tr>
</thead>
<tbody>
<tr>
<td>Black hat</td>
<td>White hat</td>
</tr>
<tr>
<td>Break in</td>
<td>Build up</td>
</tr>
<tr>
<td>Uses phishing, vishing,</td>
<td>E-mail, web conference, and face-to-face meetings</td>
</tr>
<tr>
<td>impersonation</td>
<td></td>
</tr>
<tr>
<td>Calls Execs to gain passwords</td>
<td>Calls Execs to protect passwords</td>
</tr>
<tr>
<td>Persuasion skills</td>
<td></td>
</tr>
</tbody>
</table>
How to hack a security culture

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

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

- Time box
- Assess --> Strategy
- Other sources
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
Communication tips for success

Map the org

Strategy

Travel

Face to face
Phase 3: Connect

**Goal**: Educate about security and embed expertise within every team.
A Champion program allows your security program to reach beyond a central security team and engage many virtual resources.
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 to other people within their organization
Champion activities

- Monthly training
- Online community
- Mini-conference
- Spot the flaw
- Hack-a-thons
- Full conference
Phase 4: Continuous security education

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

Video

Classroom

Hands-on
A system of learning and achievement

- The missing piece of most security awareness and learning programs is a connection between the content
- Recognize individual achievements or levels
- Create a theme
- Role-based learning
  - Only teach developers what developers need to know; business analysts what business analysts need to know, etc.
Continuous security education tips for success

- Begin with the foundations; never assume that anyone knows the basics
- Start with why; before moving to what and how, focus on why the learner needs to care
- Connect your “Security Champions” with the education program; the Champions become the early adopters and promoters, and perhaps even creators
- Record monthly Champion sessions and add them to the library of content
- Continuously refresh content pool with new lessons
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 tips for success

- Ask team members about the correct rewards for their situation
- Plug into your existing organizational rewards and recognition programs
- Reward early and often; a rewards program is not a place to be stingy
A "hacked" security culture

Phase 5: Reward
Phase 4: Continuous security education
Phase 3: Connect
Phase 2: Communicate
Phase 1: Assess

Recognition
Education program
Security champions
Bottoms up, top down comm’s
Strategy

0-4 years
CASE STUDY: ACME ENTERPRISES
Q+A and Thank you!

Chris Romeo, CEO / Co-Founder
chris_romeo@securityjourney.com
www.securityjourney.com
@edgeroute, @SecurityJourney