Developing a People-First Security Strategy

Presented by:
Richard Henderson
Global Security Strategist, Absolute Software
Today’s Agenda

• Who am I?
• Why is Security so Hard?
• Introduction into People-Centric Security
• Figuring out where you are now
• Getting from here to there
• Core principles of reduced controls
• Where to start?
• Putting it all together
• Q&A
About Me

• Global Security Strategist, Absolute Software

• Researcher, writer, electronics tinkerer, really slow runner

• Contributing editor, *RloT Control: Understanding and Managing Risks and the Internet of Things*

• Contributing author, upcoming 2nd Edition of *Cybersecurity for Industrial Control Systems*

• Defcon 25 Trainer, Defcon China Trainer
Why is Security so Hard?

• We’ve got too many point solutions, too many vendors

• Not enough qualified people

• “Log Overload”

• They only need to be right once…
Why is Security so Hard?

Tweet along: #Sec360

www.Secure360.org
People-centric Security (PCS)

• We continue to believe security can be delivered almost entirely through technology

• I don’t agree: culture matters

• Security is a *people problem*: users sometimes make risky choices. Why?
“Semantic attacks directly target the human/computer interface, the most insecure interface on the Internet. Only amateurs attack machines; professionals target people. And any solutions will have to target the people problem, not the math problem.”

- Bruce Schneier, 2000
Where Are You Now?
Security Culture

- You have to know where you are before you can get to where you need to be

- Optimize your organizational self-awareness

- If culture was simple to change through awareness alone...
Evaluating Your Current Cultural Baseline

• What does your security culture look like today? Do you know?

• Enter the Security Culture Diagnostic Survey: http://lancehayden.net/culture/ - sample surveys free to use under Creative Commons

Attribution: People-Centric Security: Transforming Your Enterprise Security Culture by Lance Hayden
### Evaluating Your Current Cultural Baseline

<table>
<thead>
<tr>
<th>What's valued most?</th>
<th>Score</th>
</tr>
</thead>
<tbody>
<tr>
<td>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.</td>
<td></td>
</tr>
<tr>
<td>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.</td>
<td></td>
</tr>
<tr>
<td>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.</td>
<td></td>
</tr>
<tr>
<td>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.</td>
<td></td>
</tr>
</tbody>
</table>

Total Score: 10

---

Attribution: People-Centric Security: Transforming Your Enterprise Security Culture by Lance Hayden
## Evaluating Your Current Cultural Baseline

### 2. How does the organization work?

<table>
<thead>
<tr>
<th></th>
<th></th>
<th>Score</th>
</tr>
</thead>
<tbody>
<tr>
<td>A.</td>
<td>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.</td>
<td></td>
</tr>
<tr>
<td>B.</td>
<td>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.</td>
<td></td>
</tr>
<tr>
<td>C.</td>
<td>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.</td>
<td></td>
</tr>
<tr>
<td>D.</td>
<td>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.</td>
<td></td>
</tr>
</tbody>
</table>

**Total Score** 10

---

*Attribution: People-Centric Security: Transforming Your Enterprise Security Culture by Lance Hayden*
## Evaluating Your Current Cultural Baseline

### 3. What does security mean?

<table>
<thead>
<tr>
<th></th>
<th></th>
<th>Score</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>A.</strong> 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.</td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>B.</strong> 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.</td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>C.</strong> 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.</td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>D.</strong> 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.</td>
<td></td>
<td>10</td>
</tr>
</tbody>
</table>

**Total Score**: 10

* Attribution: People-Centric Security: Transforming Your Enterprise Security Culture by Lance Hayden*
Evaluating Your Current Cultural Baseline

• Aggregate your results:
  • Category A questions represent security cultures focused on process
  • Category B questions: compliance-based culture
  • Category C questions: autonomy-based culture
  • Category D questions: trust-based culture

Attribution: People-Centric Security: Transforming Your Enterprise Security Culture by Lance Hayden
How Do These Cultures Compete?

- **Process-Based**
  - "Toe the Line"
- **Compliance-Based**
  - "Audits Matter"
- **Trust-Based**
  - "Empower All of Us"
- **Autonomy-Based**
  - "Just Get it Done"

Attribution: People-Centric Security: Transforming Your Enterprise Security Culture by Lance Hayden
Which Culture is Yours?

Culture Radar Chart

Process

Trust

Autonomy

Compliance

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

Tweet along: #Sec360

www.Secure360.org
Which Culture is Yours?

• Process-based?
  • Formal
  • Centralized
  • No surprises
Which Culture is Yours?

• Compliance-based?
  • Audits rule everything
  • Needs (or must have) external validation
  • Demands consistent and standard behavior from users, regardless of role or location
Which Culture is Yours?

• Trust-based?
  • Empowers people
  • Creates a sense of community
  • Leadership behave more like coaches than managers
Which Culture is Yours?

• Autonomy-based?
  • Freedom
  • Results matter, rules rarely do
  • Entrepreneurial leadership

Attribution: People-Centric Security: Transforming Your Enterprise Security Culture by Lance Hayden
With That Out of the Way…

Attribution: Cultural Risks and Gains: Metrics and ROI for People-Centric Security by Lance Hayden
With That Out of the Way…
How You Gonna to Get There?

• How can you increase people potential by increasing **trust** and independent decision making?

• How can you convince the powers-that-be to improve security culture? It might be easier than you think…
Let Me Repeat Myself…

TRUST
“Yes, but...”
Core Principles of Reduced Controls

• You provide:
  • Set of core standards that must be followed
  • Define your fundamental security principles
  • What are your ethical guidelines that must be adhered to?

• Govern and guide. Don’t dictate from above.
But... but... but...

• Reducing security controls... are you daft?

• Are there actual benefits?
How Can You Build a More Effective Security Culture?

Security awareness is good, but a good security culture is better.
Gamification Works

1. Purpose: having meaning amplifies what we do
2. Autonomy: we like having choices
3. Mastery: we like getting better
4. Feedback: we like feedback, especially positive
5. Social: fosters a “we’re all in this together” culture
Gamification of Security

- Pick Vital Behaviors
- Connect to Purpose
- Test And Give Feedback
- Reward/Recognize or Educate
- Socialize

Attribution: Salesforce
Gamification of Security

Novice: Basic awareness
Apprentice: Successful Testing
Knight: Doing
Master: Teaching
Grand Master: Innovating

Attribution: Salesforce
What to Start with First?

1. Phishing
2. Better Passwords/Auth
3. Patching
4. Mobile/BYOD
5. Data

Attribution: SANS Securing the Human, Top Human Risks, Lance Spitzer
Phishing

• Ease people into it!
• Don’t send out embarrassing emails
• Do not name names. The goal is education.
• Don’t trick people.
• Have an easy-to-use avenue to report issues, including if they clicked!

• Encourage (and reward!) people who report things, better safe than sorry.

Attribution: SANS Securing the Human, Top Human Risks, Lance Spitzer
Passwords/Auth

• NIST changed it again!

• Scan against known breach lists, reject matches.

• MFA/2FA.

• Passphrases instead of passwords?

• People are confused. Make them understand why.
Patching

• We’re all tired of Windows Update, right? Users are.

• But patching is probably the most single important piece to secure the endpoint

• People need to know why it’s so important.
  • *Was WannaCry a watershed moment??*
Mobile/BYOD

• Devices are cheap

• *The data on them is not.*

• No MDM/EMM?
Data

- Is encryption essential?

- People forget about the basics:
  - Oversharing, bcc: field
  - Taking things home and not protecting them
  - Leaving documents behind, unshredded, in the printer
  - Uploading data to a test server, not removing when done
Applying Cultural Transformation

• What can you do when you get back to the office?

• What can you do in a couple of months?

• What can you expect to see in 6 months? A year?
Applying Cultural Transformation

• What can you do when you get back to the office?
Applying Cultural Transformation

• What can you do in a couple of months?
Applying Cultural Transformation

• What can you do in 6 months or a year?
Putting it all Together…

• The more people understand and internalize your company’s cultural norms… the better their security behaviors will be.

• Focus on building simpler, more clear, more concise security policies and norms.

• You can’t change your culture overnight. Iterate and iterate.
Putting it all Together…

• How can you tell that your culture is changing?

• How can you prove it?
Putting it all Together…

• Know where you want to go, and build a map to get there.

• Get that executive-level buy in.

• Treat your employees like children, they’ll act like children.

• People are inherently good.
Questions?

rhenderson@absolute.com

@richsentme

Tweet along: #Sec360
www.Secure360.org
Questions?

THANK YOU!
Sources/More Reading

- **People-Centric Security: Transforming Your Enterprise Security Culture.** Lance Hayden, PhD

- **Trust, Mental Models, Semantic Attacks, Social Engineering, and User Education.** Jie Chen

- **Cultural Risks and Gains: Metrics and ROI for People-Centric Security.** (ISC)2 Security Congress 2016, Lance Hayden, PhD

- **SANS Securing the Human Project, Top Human Risks.** Lance Spitzner

- **Impacts of security climate on employees’ sharing of security advice and troubleshooting: Empirical networks.** Duy Dang-Pham, Siddhi Pittayachawan, Vince Bruno

Tweet along: #Sec360  www.Secure360.org