Zen & the Art of Transformational Security

Kim L. Jones CISM, CISSP, M.Sc.
Agenda

• Some Hard Truths
• The Six Understandings of a CISO
• Parting Thoughts
• Questions
ASU’s Cybersecurity Education Consortium

The mission of the CEC is Engage & Partner With Today’s Security Community to Create Tomorrow’s Cyber Workforce
Some Quick Disclaimers…

• These are my personal opinions/observations only

• There are two things I know…

• These are guidelines/starting points only. You need to figure out the pieces that make the best sense for you & your organizations.
Some Hard Truths
Your Job Isn’t Getting Any Easier...
For Many Years, Our Leadership Has Had Little Respect for Us…*

• July 2015:
  • 44% believe CISOs should be accountable for any organizational data breaches
  • 54% believe CISOs should not be responsible for cybersecurity purchasing decisions
    • Chief Scapegoat Officer anyone?
  • 61% do not believe their CISO would be successful in a leadership role outside of security
  • 51% believe it was “unfair” for the Target CEO and CIO to be fired in the wake of its data breach…

…but To Be Honest, We Are To Blame for Much of This Image Problem

• Haste to Jump on the Compliance Bandwagon

• Inability to Quantify Risk

• We (still) Suck at Metrics

• Communication Skills Can Be Lacking
  • “Pizza Boys” still abound (and are still necessary! But…)
More Hard Truths...

• You are all transformation agents
  • You are getting people and cultures to do stuff they don’t necessarily want to do…or see the value in doing

• Technology transformation is the easy part

• ROI/value realization doesn’t occur if practices/processes aren’t adopted

• What got you here won’t get you there
The Six Understandings of a CISO
1. Understand the Business
Understand the Business…

- Ability to understand the business: 72%
- Technical skills: 46%
- Communication: 42%

Source: “State of Cybersecurity: Implications for 2015,” ISACA and RSA; based off responses from 842 IT professionals.
Understand the Business…

• Why are you (really) here?
  • Breach response?
  • Compliance?
  • Peer pressure?
  • Competitive advantage?
  • Market differentiation?
  • Security Focus?

• Remember the Starbucks Test
  • What do you do to make money?
  • What keeps you up at night?
  • What is the one thing I can do to make things better for you?
2. Understand the Culture
Understand the Culture...

• The Intersection of People and Organization

• A pattern of behaviors, beliefs, assumptions attitudes, and ways of doing things

*Culture has a direct impact upon security implementation*
Four Cultural Drivers…

- Top Down
  - Marine Corps
- Bottom Up
  - Federal Government
- Inside Out
  - Healthcare
- Outside In
  - BPO/Call Centers

Important: All cultures are influenced to some extent by all four factors!!
  - Our own methodologies/best practices ignore this!!
3. Understand the Audience
Understand the Audience…

Five Sources of Meaning

- **Mission /Society**
  - Improving Society
  - Building Community
  - Stewarding Resources

- **Company/Shareholder**
  - Shareprice Targets
  - Industry Leadership
  - Beating Competition

- **Customer**
  - Easier for the Customer
  - Superior Service
  - Better Quality Product

- **Team**
  - HighPerforming Teams
  - Improved Work Experience
  - Sense of Belonging

- **Me**
  - Personal Development
  - Paycheck/Bonus
  - Empowerment

For your communications – and your program – to be successful, you should address as many of the sources of meaning as possible
- This includes – understanding your culture’s primary source of meaning
Understand the Audience…

- What is security?
  - “The state of being secure.”
  - “Freedom from risk”

- Different people, different perspectives
  - Police
  - IT
  - Manager
  - CEO
  - Others??

- Do we understand what it takes to make people feel secure? Are the things we focusing on enabling people’s concept of security??
4. Understand the Message
Three Types of Risk Messages…Each With Different Challenges

- Care
  - “If you see something, say something”
  - “Don’t copy that floppy”

- Consensus
  - Global warming
  - Patch management issues

- Crisis Communication
  - Hurricane
  - Breach
Understand the Message…

Three Types of Risk Messages...Each With Different Challenges

• Care
  • Different needs & levels of risk based upon demographics, geography, etc.

• Consensus
  • Different starting-level perceptions of risk
  • Understanding of the technical data re: the problem is usually limited
  • Need for involvement in solution

• Crisis Communication
  • Provide just enough information to create a desired action without overwhelming the audience
5. Understand the Value
“Values” Defined…

- Things that are important to “someone”
  - Individual
  - Group
  - Organization

- “The embodiment of what an organization stands for”
Values May Be Stated or Implied…

- Quality
- Candor
- Innovation
- Safety
- Legality/Compliance
- Integrity
- Speed-to-Mkt
- Cust. Service
There is a healthy, supportive tension between an organization’s values.

Note: where stated and implied values are in conflict, implied (“operational”) values win.
The Values Construct Directly Impacts the Decision Process

- Every decision the organization makes – or considers – is influenced by the values construct.
- If security is *not* a part of this values construct, then we are already behind the curve re: influencing these decisions.
  - Our objections become “roadblocks” which are not necessarily supportive of the values.
We Do Not Articulate the Value of Security Well…

- In most places, security is *at least* an implied value
  - Organizations *do* lock their doors/keep secrets 😊

- Programmatic, holistic security, however, is something organizations may struggle with
  - This tends to be the thing that we need to sell

- When asked re: the importance of programmatic security, we tend to leap to C-I-A

- Most people have some level of agreement with these tenets; the real question is “why do I need more/why is what I’m doing insufficient?”

- When pressed, we default towards frameworks, regulations, and legal compliance – which does not promote *security* as a value.
One Example of Value Articulation…

ACCESS CONTROL

- **Goal/Objective** – Enabling access to that which is required for to perform one’s duties

- **Operating Principles**
  1. Personnel should have access to the tools and facilities necessary for them to perform their job functions
  2. Not every *one* should have access to every *thing*
     - This includes internal resources as well as external resources
     - Examples:
       - Visitors to your manufacturing floor (or your executive offices)
       - Workers to porn sites

  - **Note** – this tenet applies to access by systems and applications as well
6. Understand Yourself
Understand Yourself

• Leadership Style?
• Management Style?
• What Type of CISO Are You?*
  • Technical
  • Managerial
  • Large Organization?
  • Small Organization?
  • Transformative?
  • Sustaining?

*http://cio-asia.com/tech/security/who-should-the-ciso-report-to/?page=1

The right CISO for the wrong organization – or vice versa – is problematic for all
Understand Yourself

Understand Yourself

For each of the following, rate your level of agreement with the statement:

- Strongly disagree
- Disagree
- Neutral
- Agree
- Strongly agree

1. I am comfortable discussing personal issues with others.
2. I am comfortable discussing personal issues in public.
3. I am comfortable discussing personal issues in private.
4. I am comfortable discussing personal issues with my friends.
5. I am comfortable discussing personal issues with my family.

The items below are designed to help you understand your own personal characteristics.

1. I am confident in my ability to make decisions.
2. I am confident in my ability to solve problems.
3. I am confident in my ability to communicate effectively.
4. I am confident in my ability to work independently.
5. I am confident in my ability to work in a team.

The items below are designed to help you understand your own personal tendencies.

1. I am a natural leader.
2. I am a natural follower.
3. I am a natural problem-solver.
4. I am a natural thinker.
5. I am a natural feeler.

The items below are designed to help you understand your own personal goals.

1. I want to achieve success.
2. I want to achieve happiness.
3. I want to achieve knowledge.
4. I want to achieve power.
5. I want to achieve recognition.

The items below are designed to help you understand your own personal values.

1. I value honesty.
2. I value integrity.
3. I value fairness.
4. I value compassion.
5. I value humor.

The items below are designed to help you understand your own personal beliefs.

1. I believe in science.
2. I believe in religion.
3. I believe in reason.
4. I believe in tradition.
5. I believe in innovation.

The items below are designed to help you understand your own personal behaviors.

1. I am organized.
2. I am disciplined.
3. I am spontaneous.
4. I am creative.
5. I am practical.

The items below are designed to help you understand your own personal Outlook.

1. I am a practical thinker.
2. I am a conceptual thinker.
3. I am a sociable thinker.
4. I am an imaginative thinker.
5. I am a logical thinker.

The items below are designed to help you understand your own personal Emotions.

1. I am expressive.
2. I am reserved.
3. I am sensitive.
4. I am independent.
5. I am dependent.

The items below are designed to help you understand your own personal Moods.

1. I am cheerful.
2. I am sad.
3. I am angry.
4. I am scared.
5. I am calm.

The items below are designed to help you understand your own personal Temperament.

1. I am easy-going.
2. I am tense.
3. I am laid-back.
4. I am active.
5. I am passive.

The items below are designed to help you understand your own personal Social Orientation.

1. I am a loner.
2. I am a socialite.
3. I am a team player.
4. I am a leader.
5. I am a follower.

The items below are designed to help you understand your own personal Communication Style.

1. I am direct.
2. I am indirect.
3. I am open.
4. I am closed.
5. I am sensitive.

The items below are designed to help you understand your own personal Learning Style.

1. I learn by doing.
2. I learn by reading.
3. I learn by listening.
4. I learn by observing.
5. I learn by thinking.
Parting Thoughts
“There is nothing more difficult to carry out, nor more doubtful of success, nor more dangerous to handle, than to initiate a new order of things. For the reformer has enemies in all who profit by the old order, and only lukewarm defenders in all those who profit by the new order. This lukewarmness arises partly from fear of their adversaries, who have law in their favor; and partly from the incredulity of mankind, who do not truly believe in anything new until they have actual experience of it.”

-Machiavelli, *The Prince*, 1513 A.D.
Questions?
Kim L. Jones CISM, CISSP, M.Sc.
Director, Cybersecurity Education Consortium
Arizona State University
(602) 543-6038
KimJones.CISM@ASU.edu
Warrioroflightsecurity.blogspot.com