The Coca-Cola Company

Creating a Culture of Security

August 23, 2011

Agenda

- **Objectives**
- **Background**
- **Definitions**
- **Culture in Context to Security**
- **Security in Context to Culture**
- **Benefits of a Culture of Security**
- **Creating a Culture of Security**
  - Who?
  - What?
  - How?
- **Sustaining a Culture of Security**
- **Challenges to Maintaining a Culture of Security**
- **Resources**
- **Q&A**

Objectives

- To provide a high level review of the ISACA Publication "*Creating a Culture of Security*"
- To discuss the impact that day to day human behavior and habits have on security, this is not a technical discussion
- To discuss how human involvement can increase the efficiency of security solutions
- To understand how a culture of security will benefit you and your organization
- To learn how to become a security champion and begin fostering a culture of security

Background

Who is The Coca-Cola Company?

"We began serving a delicious and refreshing sparkling beverage 125 years ago in Atlanta, Georgia. With that first moment of refreshment came a thirst for more that continues to this day. We now have more than 500 brands and 3,500 beverage products and sell 1.7 billion servings per day in over 200 countries. We are growing our reach, strengthening our brands and advancing our global momentum, every moment of every day." *- The Coca-Cola Company 2010 Annual Review*

The Coca-Cola Company

Definitions

What is Security?

Defined by the CIA (public source information)

- Security may be (and often is) defined solely as confidentiality, integrity and availability.

What is Culture?

- A common history shared by a group of people , which in turn creates a set of behaviors that become the expected and normal responses to certain events.

What is a Culture of Security?

Defined by ISACA

- *A culture of security is the existence of meaningful security so clearly aligned with the mission of the business that management does not need to apply intentional measures.*

According to BMIS

- *A culture of security is a pattern of behaviors, beliefs, assumptions, attitudes and ways of doing things that promotes security.*

Definitions

What is Information?

According to ISO/IEC 27000:2009

- *Information is facts; in this sense, information is made up of words, bits and bytes. Information is also the communication of knowledge which incorporates documents, conversations and networks. Additionally, it is the sequence of bits that produce specific effects, in other words, the programs that manipulate data.*

What is Information Security?

According to ISO/IEC 27000:2009, since various meanings exist in multiple contexts, a statement of why information security is important has been created to replace the lack of a common definition:

- *Whatever form information takes, or means by which information is transmitted, it always needs appropriate protection.*

Culture in Context to Security

Attributes of Culture in Context to Security:

Societal, Organizational and Personal Cultural Influence

- Societal, Organizational and Personal culture as a whole will have a dramatic impact on a culture of security.

Media's Influence on the Cultural View of Security and Threats

- With the onset of cyber crime as a common theme in today's media, a non-realistic view of security, technology and exposure to threats exists.

In the 2007 film Live Free or Die Hard, a global terrorist network is attempting to attack the US national infrastructure and John McClane, played by Bruce Willis, is the only person who can stop them.

Culture in Context to Security

Attributes of Culture in Context to Security:

General Lack of Understanding

- A higher barrier to a robust culture of security will exist if the general population within an organization do not understand the reality of:
    - How computers and technology generally work
    - How information flows
    - Touch points information is exposed to (i.e., hard copies, person to person, programs)
    - Security threats that they are readily exposed to
    - How security is dealt with

Pharmacies are now posting signs reminding customers not to discard their personal prescription information in public trash cans.

Security in Context to Culture

Attributes of Security in Context to Culture:

Security

- With varying definitions of both security and information, utilized in various ways depending on the type of business being conducted, the appropriate amount of security, for various sources of information is to be determined by the business in question. Appropriateness of security for various information sources should be determined based on **the regulations that must be held by the business, risk exposure, and cost of communicating, replacing, storing, disposing of and/or verifying the information.**

It would not be appropriate for a small Bed and Breakfast to put security practices into place that are as stringent as the FBI's.

Security in Context to Culture

Attributes of Security in Context to Culture:

Trust

- If information is consistently reliable, and available, time spent on verifying data used to report information both internally and externally will be saved. Consistency and stability are the most effective ways of establishing trust of information, which is necessary to support a robust culture of security.

Risk Mitigation

- A robust culture of security acts as an extended barrier to fraud prevention. By focusing on security as a whole, holistically from within the organization, fraud and misuse of information for financial gain is dramatically reduced. In cases where fraudulent activities occur, employees of an organization that contains a holistic culture of security are more apt to report suspicious activity before it becomes a larger issue.

Benefits of a Culture of Security

Benefits to Implementing a Culture of Security Include:

Organizational Benefits

- Improved Ability to Manage Risk
- Improved Return on Security Investment
- Improved Compliance with Laws and Regulations
- Increased Shareholder Value
- Increased Trust from External Sources and General Population

Benefits of a Culture of Security

Benefits to Implementing a Culture of Security Include:

Personal Benefits

- Less time spent on verifying data needed to perform job functions
- Less time spent duplicating efforts to ensure information communicated is consistent
- Less time problem solving information inconsistencies
- Less time trouble shooting programs relied on to gather information
- Less time spent manually maintaining information due to lack of trust of the main source

Creating a Culture of Security

Who?

Getting the right people involved

- **Champions of security** – All technology is controlled and used by people. If people are not invested in the involvement of the development, maintenance and day to day of business technologies, people will not be invested in the confidentiality, integrity and availability of information. Security champions are individuals who are invested in fostering security as a culture, not so much as a rule. When people start seeing the benefit of security, they will stop seeing it as punishment for not following a rule.
- **Executive Leadership** – When executive leadership is invested in the overall culture of security, people will follow. A culture cannot thrive in an environment where the leaders do not seem to view security as a benefit.

Creating a Culture of Security

What?

Attributes of a Culture of Security

- **Accountability** exists at a personal, team, departmental and organizational level
- **Policies, Standards and Guidelines** exist, are communicated and are aligned with the overall organizational culture
- **Go/No-Go Decisions** are consistently made with a healthy balance between business missions and security. This allows involved parties to feel safe that a project or operation will properly cease if security or ethics become an issue.
- **Rewards** are consistent across the organization
- **Response to Breaches** are consistent across the organization
- **Satisfied Customers**
    - Internally people feel safe, are able to rely on information steadily and trust business activity across teams and departments
    - Externally people feel safe conducting business and readily trust information

Creating a Culture of Security

What?

Attributes of a Culture of Security

- *ISACA Security Culture Maturity Model*

Figure 9—Security Culture Maturity Model					
Role	**Lagging**	**Aware**	**Partially Effective**	**Effective**	**Leading Edge**
Senior management	Uncaring	Caring, but more concerned about cost	Funds a security program	Involves security in tactical decision making	Involves security in strategic decision making
Middle management	Actively opposed to most security requirements	Concerned, but bypasses security when it seems to hamper goals	Respects security as long as other goals can be met	Involves security professionals in major initiatives	Sees security as a competitive advantage
Staff	Unconcerned	Concerned, but inactive	Follows security rules	Considers the security of information while using it	Thinks about security before using information
IT	Does not build security into systems	Builds minimal security into systems	Builds required security into systems	Seeks the assistance of security professionals in building security into systems	Anticipates the need for security in the systems it builds
Security professionals	Are only administrators	Write policy	Implement security safeguards	Advise management on tactical issues	Advise management on strategic issues

Creating a Culture of Security

How?

Acceptance

- Recognition that something should be done, in itself, is the first step to success.

Active Involvement

- Simply attempting to pursue a culture of security, and accepting that there are no defined ways to implement, document, balance or measure exact results is the second step to success.

Commitment to Managing the Culture

- Commitment to managing the culture by remaining flexible to account for organizational, societal and economic changes that will impact group behavior is needed to ensure slippage does not occur.

Changing Perceptions

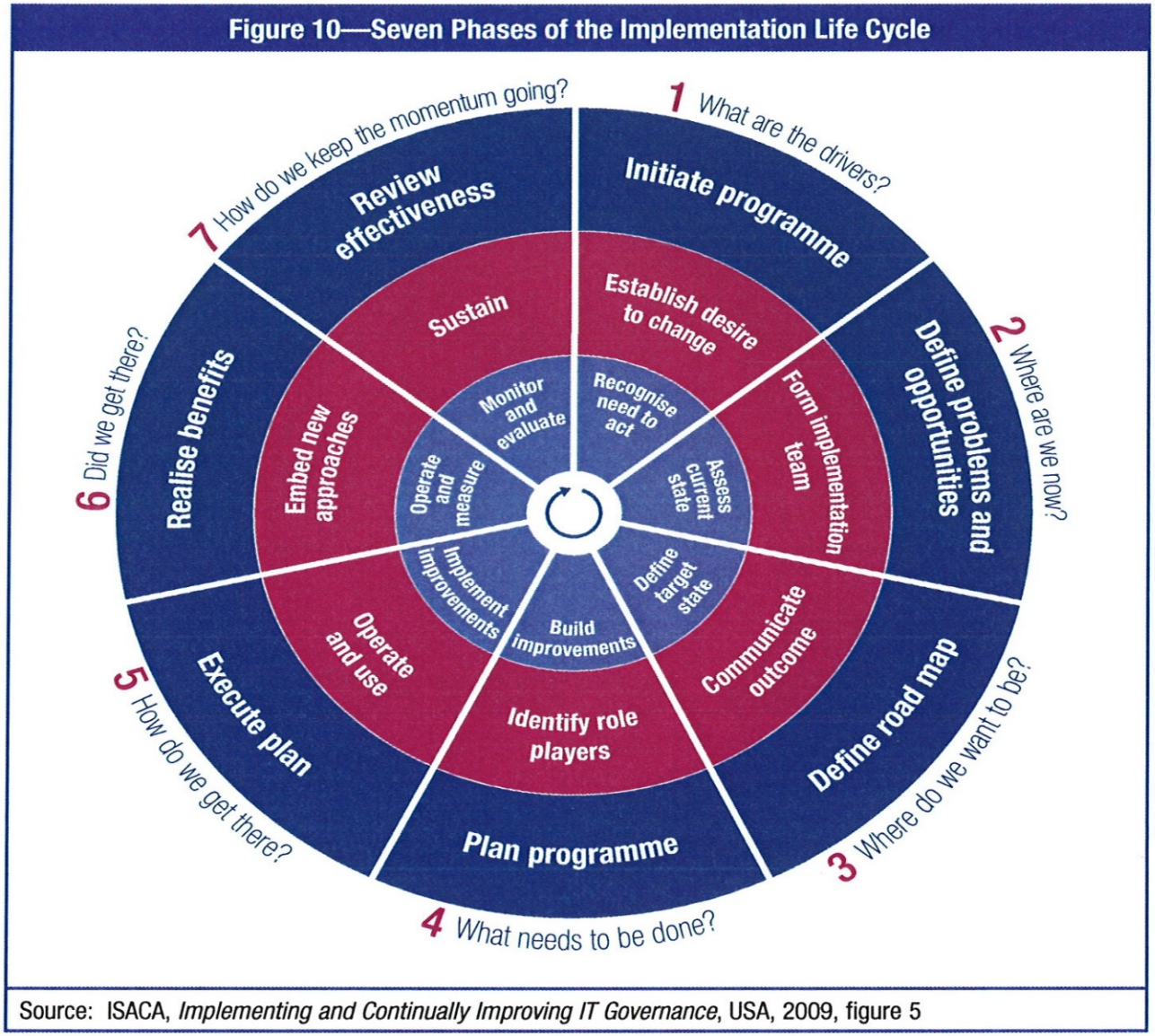
- Branding
- Education and awareness

Creating a Culture of Security

How?

ISACA IT Governance Implementation Model

- Although not exact, the ISACA IT Governance Implementation Model has many overlaps in content and can serve as guidance for creating and implementing a culture of security. In fact, IT Governance cannot fully thrive in an organization with a weak culture of security and vice-versa.



Sustaining a Culture of Security

Positive Reinforcement

- Aligning Information Security with Business Objectives
- Finding the right balance
- Convergence of security roles
- Automated Tools
- Organizational support

Positive reinforcement should be used to instill standard security practices by creating an atmosphere of trust.

Sustaining a Culture of Security

Negative Reinforcement

- Personal incentives
- Vigilance
- Automated detection
- Alerts
- Penalties

Negative reinforcement should not be used to instill standard security practices which would create an atmosphere of fear.

Challenges to Maintaining a Culture of Security

Differing Cultures

Organizations contain unique blends of cultures within each individual

- Societal Culture
- Economic Culture
- Regional Culture
- Differing religious and political views
- Differing upbringings and backgrounds

Challenges to Maintaining a Culture of Security

Organizational Culture

Organizational Inconsistency

- Lack of /unclear requirements
  - Insufficient Awareness
- Lack of systematic view
    - Differing comprehension of risk
    - Differing personal experience

Challenges to Maintaining a Culture of Security

Departmental Culture

Departmental Inconsistency

- Variances in Monitoring Routines
- Variances in Enforcement Practices
- Lack of Rewards
  - Lack of financial connection to security
  - Failure to measure security risk properly
  - Failure to properly report incidents
- Lack of Security Budget
- Lack of proper influence
- Lack of Management Attention

Resources

ISACA

- The following referenced materials can be found on the ISACA website:
  - BMIS
  - ISO/IEC 27000:2009
  - CIA Definitions for security professionals

https://www.isaca.org

Q&A

Thank you

Please feel free to contact us with any questions or comments regarding these materials.

Cecilia Holman ~ *cholman@coca-cola.com*

- IT - Corporate Internal Controls for The Coca-Cola Company

David N. Harrison ~ *dnharrison@coca-cola.com*

- IT - Corporate Internal Controls for The Coca-Cola Company

Anitra Swann ~ *answann@coca-cola.com*

- Security Governance - Corporate Internal Controls for The Coca-Cola Company