

Beyond Information Security Awareness Training: It's Time to Change the Culture ¹

Stan Stahl, Ph.D.
President
Citadel Information Group, Inc.

Introduction

The effectiveness of an information security program ultimately depends upon the behavior of people. Behavior, in turn, depends upon what people know, how they feel, and what their instincts tell them to do. While an awareness training program can impart information security knowledge it rarely has significant impact on people's feelings about their responsibility for securing information, or their deeper security instincts. The result is often a gap between the dictates of information security policy and the behaviors of our people.

One sees this phenomenon every time an employee opens an unexpected email attachment from a friend. They may not really care about the potential that the attachment is a virus, or they may care, but their instincts are not finely enough honed to intuitively recognize the threat.

It's the same issue every time an employee falls victim to social engineering. People's instincts are to be helpful. We amplify this instinct every time we tell employees about the importance of customer service. And then we wonder why, in that moment of truth, after the social engineer has sounded so friendly and seemed so honest, that the employee disregards the awareness training program and gives up his password

Sometimes it's management who, in a weak moment, falters. What of the Operations Manager who needs to share information with a vendor? Yes. He knows he's supposed to arrange this through the *CISO*. But time is of the essence. He's known the vendor for 20 years. The vendor would never do any harm. And before you know it, he's connected the corporate crown jewels to an untrusted third party.

The root cause of the recent rash of thefts of bank account and social security numbers at companies like Choicepoint and Lexis-Nexis is the failure on the part of people to recognize an information risk and, having recognized it, to act on it. Phishing schemes succeed only because people are not sensitive to the potential for information harm. Identity theft has become the fastest growing white-collar crime in America because society has not yet evolved a strong sensitivity to information risk. Information risk has not yet become something we feel in our gut.

Yet, until and unless we affect how people feel about the need to secure information ... until and unless our people develop good information security instincts ... the gap between the dictates of information security policy and the behaviors of our people will persist.

¹ This article appeared in *Information Security Management Handbook, Sixth Edition*, edited by Hal Tipton and Micki Krause, Auerbach, 2006.

It is the role of culture to close this gap.

Organizational Culture

The culture of an organization can be defined as:

*A pattern of shared basic assumptions that the group learned as it solved its problems of external adaptation and internal integration, that has worked well enough to be considered valid and, therefore, to be taught to new members as the correct way to perceive, think, and feel in relation to those problems.*²

What this means is simply that as an organization evolves, it discovers ways to adapt to market, competitive, regulatory and other changes in its external environment. It also figures out ways to organize itself internally—both formally as represented by the organization chart but, more importantly, informally—the way the work actually gets done. These ways are never perfect, but they are satisfactory for achieving the organization's goals and objectives. These 'ways' of being and of adapting, then become the norm for the organization, they characterize the organization's culture.

Cultures have subcultures. Thus one finds a 'marketing subculture,' and a 'sales subculture.' These two subcultures emphasize relationship-building with one's markets and customers. That's why a lot of golf is played by people in these subcultures.

² *Organizational Culture and Leadership*, 2nd Edition, Edgar H. Schein, Jossey-Bass, 1992

We all know the penuriousness of those in the financial subculture; they're not called 'bean counters' without good reason. Operations people have their own subculture, focused on managing the supply chain, transforming streams of orders and raw materials into the delivery of products and invoices.

The IT organization, too, has its own subculture, very distinct from other organizational subcultures. It even speaks a language of its own.

If the organization is big enough it will even have its own 'security' subculture, typically populated by former law enforcement personnel, expert at guarding people and things.

One of the things to observe is that the marketing, sales, operations, and financial subcultures form the "core" of an organization and, consequently, they dominate in setting the culture of the entire organization.

A second thing to observe is that there is a great deal of interaction between people in these four core subcultures. They work together in accomplishing the mission of the organization. As a result there is a mixing of subcultures, people throughout these parts of the organization evolve a somewhat similar way to *perceive, think, and feel* about problems and challenges.

One of the major challenges in strategically integrating the IT organization into the senior management team is that the cultural barriers are often difficult to break through. As IT has become more readily acknowledged as being strategically critical to the success of the organization, more leadership energy is being put into breaking

down the cultural barriers between IT and the core organization.

Note, finally, that in the typical organization the entire protection function is externally located in the security function, with little if any mixing between the security culture and the rest of the organization. Responsibility for protection lies with the security organization; everyone else gets to go about their business without worrying about security because the guards are presumed to have it all covered.

The Information Security Cultural Challenge

Given the cultural context in which the information security organization finds itself, the cultural realities of the situation are, to be honest, somewhat bleak.

- Information security is a new kid on the block. In most organizations the information security function is at most a few years old. The field itself dates only to 1970.³
- Information security is nowhere near core to the organization. Even when there is a regulatory requirement for information security controls, these are ‘pushed’ by senior management only because they are legally required. Top-level support for information security could dry up in an instant if the legal and regulatory landscape were to change.
- Even more challenging, the information security organization manages a set of

³ I date the origin of the field as the publication date of *Security Controls For Computer Systems, Report of Defense Science Board Task Force on Computer Security*, edited by Willis H. Ware. A classified version was published in 1970 for the Office of the Secretary of Defense. The Rand Corporation published an unclassified version in 1979.

concerns seemingly disconnected from those of the marketing, sales, operations, and financial organizations, with the result that the information security subculture is dramatically disconnected from these other, much more dominant, subcultures.

- Because “information security” contains the word “security,” the cultural expectation is that the information security group will take care of security just like the guards do, with no need for ‘me’ to get involved
- Except for the annual awareness training, the only time the information security culture “touches” the rest of the organization is when someone forgets his password or when the system won’t let someone “do her job.” Consequently, there are likely to be few ‘natural’ opportunities for cultural blending, with the result that the information security subculture will tend to evolve in isolation from the dominant culture.

It is against this backdrop that the information security organization must embed its culture into the culture of the larger organization, for this is the only way to transfer to the larger organization the *correct way to perceive, think, and feel in relation to information security problems.*

The CISO’s New Job

The energy for the required cultural change must come from the information security organization, ultimately from the Chief Information Security Officer.

Without the *CISO’s* commitment, organizational change will not occur. With adequate commitment, with enough time and energy put into the challenge of embedding information security into the

very sinews of the organization, with this commitment, applied wisely, success can be a nice easy marathon.

Any *CISO* who takes the *CISSP Security Management Practice Domain* seriously, and thinks logically about it, can come to no other conclusion than that cultural change is and must be a part of his or her job description. The alternative, frankly, is a cop-out. And, frankly, it results in more crisis work for your staff cleaning up after user messes.

Consequently, every *CISO* should add the following to her job description.

Embed information security subculture itself as quickly as feasible into the larger culture, so that the larger culture *perceives, thinks, and feels correctly in relation to information security problems.*

Leadership: The Force for Cultural Evolution

Cultures are never static. Left to their own devices, they continuously evolve in reaction to the internal and external pressures faced by the organization. The challenge of leadership is to optimally affect the ongoing course of organizational evolution, to be the change agent directing this evolution.

Culture and leadership are two sides of the same coin ... If cultures become dysfunctional, it is the unique function of leadership to perceive the functional and dysfunctional elements of the

existing culture and to manage cultural evolution and change in such a way that the group can survive in a changing environment.

*Leadership ... is the ability to step outside the culture ... and to start evolutionary change processes that are ... adaptive. This ability to perceive the limitations of one's own culture and to develop the culture adaptively is the essence and ultimate challenge of leadership.*⁴

This aspect of leadership—to change the larger culture in the direction of information security—must be part of any *CISO's* job description. Until and unless “the information security way of seeing the world” becomes a part of the organization’s culture, the organization is dysfunctional. Every time there is a security breach—even if it fell in the forest and no one was there to hear it—every time there’s an information security breach whose root cause is human, that’s evidence of the dysfunctionality.

So the *CISO*, must step outside the culture and look at it from the outside, molding and shaping its evolution, so that, over time, people are doing the right thing: they’re being careful, they’re paying attention, and they are even training each other—all because an information security mindset has become embedded in the larger culture.

⁴ *Organizational Culture and Leadership*, 2nd Edition, pgs 15, 2, Edgar H. Schein, Jossey-Bass, 1992.

Strategic Imperative: Evolve an Information Security Learning Organization

Real security lies not just in firewalls, passwords and awareness training but in the culture *perceiving, thinking, and feeling correctly in relation to information security problems*. This can only happen gradually, as the culture evolves an *information security learning organization*.

David Garvin, in an article in the *Harvard Business Review*, defines a learning organization as follows:

*A learning organization is an organization skilled at creating, acquiring and transferring knowledge, and at modifying its behavior to reflect new knowledge and insights.*⁵

An information security learning organization is an organization skilled at creating, acquiring and transferring knowledge about information security, and at modifying its behavior to reflect new information security knowledge and insights.

In *The Fifth Discipline*, Peter Senge, one of the pioneers of learning organizations identified five key disciplines that are prerequisites to establishing a learning organization.⁶ These five disciplines are

Personal Mastery: Approaching one's life as a creative work, living life from a creative as opposed to a reactive viewpoint. This requires that we continually clarify what is

important to us and continually learn how to see reality more clearly.

We can only learn when we are unafraid. Consequently, the *CISO* has to create a trusting environment in which people are willing to open up to their information security inadequacies without fear of feeling stupid or otherwise inadequate. Implementing this discipline gives the *CISO* a great opportunity to help people recognize the significant risks that their behavior subjects information to. As people's defenses fall the *CISO* will gain greater opportunities to help people gain greater clarity about their information security responsibilities. In this way, the *CISO* can lead the culture to become ever-more conscious of information risk and the things we must all do to counter it.

Mental Models: Continually managing our mental models – surfacing them, testing them, and improving them – so as to bring our mental models of how we think things are into greater and greater alignment with how things really are.

This means providing people the intellectual tools needed to understand information security so that its principles come to be applied in every situation where people might put information at risk. The *CISO* must define the very language by which the organization can talk about the security of information.

Shared Vision: Developing and nurturing a shared vision of the future as a powerful force for aligning the organization; out of a shared vision can come transcendental powers of accomplishment.

The information security leader needs to connect information security to the very success or failure of the organization, helping people understand, for example, how an information breach could close the company and put people out of work. With

⁵ *Building a Learning Organization*, David Garvin, Harvard Business Review, July-August, 1993,

⁶ *The Fifth Discipline*, Peter Senge, Doubleday Currency, 1990

the heightened concern about identity theft, the *CISO* has the opportunity to connect information security to the ethics of the Golden Rule: Everyone's information, including our own, is at risk. We must protect other people's information just as we rely on others to protect ours.

Team Learning: Aligned learning, based on dialogue and discussion, having the power to efficiently move an organization towards its shared vision.

The *CISO* must help people understand the reasons behind all the security rules. People don't like to follow rules. But they willingly embrace behavior when they have discovered its necessity for themselves. Thus, the *CISO* must work with people so they come to train each other. A goal should be to make information security a common theme in discussions around the water cooler.

Systems Thinking: The ability to fully understand the cause and effect relationships that exist between events; that everything we do can be – simultaneously – both cause and effect.

The *CISO* must understand the forces on the organization's culture, the myriad of causes and effects that impact the culture's evolution. And having understood them, the *CISO* must create and implement a strategy for information security cultural change that aligns with these forces. To be effective, the change strategy, must amplify those cultural forces, like increased compliance and the organization's need for information availability, that demand greater cultural change. Conversely, an effective strategy must overcome systemic realities like information security usually being relatively inconsequential to the core of the organization.

Real Power: The Force for Evolving the Information Security Culture

The greatest challenge the *CISO* faces as she goes out into the world of culture change is the lack of any of the trappings of power. The typical power of the *CISO* is negative: "It's the information security group that makes me change my password." "Well I don't see why I can't have wireless in my office. Who made them God?" "Sorry Bill. We can't go over end-of-month reports until Thursday. I have to take my information security awareness training. Boring!"

And while you may be able to convince a CIO or CEO to support you, you know their attention will be diverted with the next crisis. And then they'll kind of forget about you again ... until the next disaster where, unless you're lucky, you'll be blamed ... for a human error ... who's root cause is firmly embedded in the culture.

And, even if you had the power to impose an information security perspective on the larger culture, the reality of organizational change programs—upwards of 75% of them fail—suggest that you'd be unlikely to succeed.

Fortunately, there's a better way. One that does work. It involves changing the culture imperceptibly, one moment-of-truth at a time, but doing so with strategic insight. Like the butterfly effect in complexity science, the *CISO*'s objective is to achieve large outcomes from small inputs.⁷

2,500 years ago the strategic guide for accomplishing this was written in China. According to legend, the *Tao Te Ching*, eastern philosophy in the Buddhist tradition,

⁷ The *butterfly effect* asserts that a butterfly flapping its wings in Los Angeles can cause a storm in Singapore 14 days later.

was written by a monk named Lao-tzu.

In their book *Real Power*, management consultant James Autry along with the noted religious scholar Stephen Mitchell, apply the *Tao Te Ching* to the modern business organization.⁸

Mitchell describes the *Tao* as follows: “*Tao* means literally *the way*. ... The *Tao* has been called the wisest book ever written. It is also the most practical book ever written. In eighty-one brief chapters, the *Tao Te Ching* looks at the basic predicament of being human and gives advice that imparts balance and perspective ... the classic manual on the art of living.”

The authors describe the essence of the *Tao*'s applicability to work as follows:

The most important understanding we can have about work is not that we are there to cultivate ideas, but that we are there to cultivate the space that holds ideas.

Think about it. When the *CISO* is talking to the Purchasing Department about information security, the purpose is not to tell people the results of our thinking about information security. The purpose is to create opportunities for people to think about information security for themselves.

Autry and Mitchell write the following as an analogy:

We use materials and techniques to make a wheel or a pot or a house -- yet what makes them useful is not

⁸ *Real Power: Business Lessons from the Tao Te Ching*, James Autry and Stephen Mitchell, Riverhead Books, 1998.

their form but the space that their form defines and creates. A room is what is inside its four walls; the walls make the room possible but they aren't the room. Even what is inside the room—its furniture, lighting, floor coverings, and so on—only accommodates how people live within the room; they are not the living itself.

It's not the passwords and the anti-virus software and the policies and the awareness training that are the information security culture. From the perspective of real power, these are merely the trappings of security. Real security lies in the culture *perceiving, thinking, and feeling correctly in relation to information security problems*. The culture does this by becoming an *information security learning organization*. And this happens, little by little, as those who know more about information security create opportunities for others to learn. And it all starts with the *CISO* taking every opportunity to create an opportunity to cultivate the organizations ideas about securing information.

And what gets in the way of opportunities for people to learn about information security? Autry and Mitchell tell us:

There's just one thing that collapses that space: expectations. *When people are talking with the boss, they are always aware of hierarchy, so they measure their words and actions, assuming that they are constantly being judged. This is, in fact, most often the case, and the added self-*

consciousness can stifle someone's best ideas. But if people feel that they can be themselves, that they aren't being judged against the boss's preconceptions, then they can become liberated to do their best work. When you act in this way to support people and ideas, you will be creating an atmosphere that gives birth to high morale and productivity.

And even though the CISO isn't the boss, when he talks to people about information security, he is the authority, acting in the role of judge. When people think they are being judged they become fearful. When they become fearful, they become defensive. And when they become defensive, learning shuts down. And the CISO loses an opportunity to impact the culture.

Therefore, to be successful at creating culture change, the CISO must not judge. This is reflected in the very first of Deming's highly influential 14 points of quality improvement: "Drive out fear."⁹

With the above as prelude, the following are some verses from the *Tao* that are particularly germane to the challenge of embedding information security into the organizational culture.

*The ancient Masters
Didn't try to educate the
people,
But kindly taught them to not-
know.*

*When they think that they
know the answers,*

*people are difficult to guide.
When they know that they
don't-know,
People can find their own
way.*

*The Master doesn't talk, he
acts.
When his work is done,
The people say, "Amazing:
We did it, all by ourselves!"*

*Intelligent control appears as
uncontrol or freedom.
And for that reason it is
genuinely intelligent control.
Unintelligent control appears
as external domination.
And for that reason it is
really unintelligent control.
Intelligent control exerts
influence without appearing
to do so.
Unintelligent control tries to
influence by making a show
of force.*

*If you want to shrink
something,
You must first allow it to
expand.
If you want to get rid of
something,
You must first allow it to
flourish.*

*Giving birth and nourishing,
having without possessing,
acting with no expectations,
leading and not trying to
control:
this is the supreme virtue*

⁹ *Out of the Crisis*, pg 23, W. Edwards Deming, MIT CAES, 1986.

Ethical Persuasion: Changing Culture Means Building Relationships

If you would win a man to your cause, first convince him that you are his sincere friend. Therein is a drop of honey that catches his heart, which is the high road to his reason, and which, when once gained, you will find but little trouble in convincing his judgment of the justice of your cause, if indeed that cause be a just one.

*Abraham Lincoln
16th US President*

Changing a culture requires changing people; changing how people perceive, think, and feel about information security problems. In effecting cultural change, the *CISO* must win everyone to the cause of information security. And to do that, as Lincoln reminds us, requires the *CISO* to be a sincere friend.

If the *CISO* is to change people, the *CISO* must engage in what is known as *ethical persuasion*, the honest attempt to induce people to change their behavior. To persuade ethically — to catch the heart which is the high road to reason — the mode of persuasion needs to be direct and honest, it needs to be respectful of people, and it must be without manipulation.

Recent work in the behavioral sciences has discovered six specific *persuasion triggers* that the *CISO* can use to influence the extent to which people will open themselves up to being persuaded.¹⁰

Trigger 1: *Reciprocity: People feel obliged to give to people who have given to them.*

¹⁰ *Harnessing the Science of Persuasion*, Robert Cialdini, Harvard Business Review, October 2001.

This trigger is, perhaps, at the core of human interaction and relationship building. It appears to be invariant across all human cultures. Besides instilling obligations, the reciprocity trigger is an inducement to build relationships. The trigger is activated by gifts and concessions. The key is to provide a gift or a concession as a way of getting a relationship started.

The reciprocity trigger is a testament to the power of the Golden Rule: *Give unto others as you would have them give unto you.* First you give. Then you get.

The most important gifts a *CISO* can give are the gifts of friendship and respect, the gift of recognizing that coworkers have needs and challenges and responsibilities of their own, and accepting that these can get in the way of people's information security obligations. This doesn't mean abandoning information security standards, but it does mean giving people flexibility in meeting the standards.

The *CISO* should also seek out opportunities to apply information security standards to helping people do their jobs. To most employees, information availability is more important than information confidentiality. The *CISO* who gives employees the gift of information availability can reciprocally trigger employees to better protect information confidentiality and integrity.

Trigger 2: *Social Proof: People follow the lead of similar others.*

An information security bandwagon is forming as society increasingly recognizes the need to secure sensitive information. Laws are being passed requiring whole industries to implement information security safeguards. Legal duties of due care are

being established in the courts, by the FTC, and by several Attorneys General. Business organizations, including the influential *Business Roundtable*, are recommending that information security become a matter for attention by a company's Board of Directors. Joining the bandwagon are all those employees who see their productivity suffer from spam, viruses, and the other digital detritus that finds its way into their information systems.

An effective *CISO* can use this emerging bandwagon to trigger *social proof*. By gently demonstrating how this bandwagon is growing, by sharing with personnel how others are coming to think, feel, and act differently about information security issues, the *CISO* can influence people to join the bandwagon.

To amplify this trigger the *CISO* can demonstrate how ubiquitous information security concerns are becoming, how the entire society is becoming concerned about information security matters. Building a bandwagon inside the company adds additional amplification as people tend to be more strongly influenced by people who are like them.

People are particularly prone to doing what others do when they find themselves in unfamiliar situations where they are not quite sure what they should do. As information security requires employees to act differently, the effective *CISO* will always be on the lookout for opportunities to share information that illustrate effective security practices.

Trigger 3: Authority: *People defer to experts who provide shortcuts to decisions requiring specialized information.*

As a general rule, people tend to rely on those with superior knowledge, expertise or wisdom for guidance on how to behave. This trigger illustrates the difference in influence between being *an* authority and being *in* authority.

CISOs can naturally tap into this trigger as people typically respond to the *trappings* of authority. A *CISO's* title, the fact that she has her *CISSP* certification, the diplomas on the wall, the books on the shelf, even the ability to speak geek, these are the trappings that establish the *CISOs* authority. Where the *CISO* sits in the organizational hierarchy can add or detract from the *CISO's* trappings of authority. That's a big reason why it's important for the *CISO* to have a seat at the management table.

While people will generally respond to the trappings of authority, research has shown that the most effective authority is the authority who is perceived as *credible*. Two factors dictate the extent to which people will deem the *CISO* as a credible authority: her expertise and her trustworthiness.

This is one reason why the *CISSP* certification is so valuable. It is not only a trapping of authority, it serves also to demonstrate expertise. It serves notice that the *CISO* is not just an empty suit.

Trustworthiness is the second amplifier of the authority trigger. Trustworthiness means being honest with people about the realities of information security. It means not trying to frighten senior management into budget increases or employees into meek compliance with horror scenarios having a 0.00001 percent chance of occurrence. Trustworthiness means being brutally honest about the strength and robustness of one's information security controls, neither

making them out to be stronger nor weaker than they really are.

Trigger 4: *Consistency: People fulfill written, public and voluntary commitments.*

Consistency is a very powerful trigger for the *CISO* who knows how to use it. But it also has the capacity to seriously backfire if misused.

For this trigger to succeed, it is important that the commitment be voluntary. An involuntary commitment is at best neutral towards inducing behavioral change. At its worst it is downright dangerous, often acting to produce exactly the opposite effect from what is desired.

So while an organization may be obligated, for legal reasons, to require every employee to sign a statement agreeing to abide by the organization's information security policies, this involuntary commitment is unlikely to serve to change people's behaviors.

Far more effective is for the *CISO* to understand people's values and behaviors, linking desired information security behaviors to behaviors the employee has already committed to.

If, for example, the organization values a strong "chain-of-command," the *CISO* can link desired information security behavior into this chain-of-command. In this circumstance, employees will secure information as a way of fulfilling their commitment to respect the organization's chain-of-command.

Alternatively, if the organization publicly values a looser less restrictive more autonomous environment, then it is important for the *CISO* to link information security behaviors to people's personal

responsibility to "do the right things" for the organization.

Trigger 5: *Scarcity: People value what's scarce.*

Since information security is about protecting the organization from loss, this trigger is a natural tool for the *CISO*.

To understand the value of this trigger, it's important to recognize that several psychological studies have shown that people are more likely to expend money and energy to avoid loss than to achieve gain.¹¹

Consequently, by discussing information security in the language of loss, the *CISO* is far more able to induce people to take action to limit the potential for loss. The *CISO* can increase her effectiveness even more by making a point to couch the loss in terms that are meaningful to the hearer.

Consider, as an example, the impact of an open honest discussion about how an information security breach can result in lower revenues and how lower revenues translate into fewer jobs. (Choicepoint provides a good starting point for the discussion.) This kind of discussion provides an opportunity for employees to link their jobs to the security of information. And as people are typically very risk-averse towards losing their jobs, this well-positioned link to scarcity can serve to induce people to pay more attention to their information security actions.

Trigger 6. *Liking: People prefer to say "yes" to people they perceive like them.*

¹¹ *Judgment Under Uncertainty: Heuristics and Biases*, edited by D. Kahneman, P. Slovic, and A. Tversky, Cambridge University Press, 1982.

I know we're taught how important it is that people like us; that our success depends in part upon how well we are liked. And, to some extent it's true. But like all great truths, there is another, deeper, perspective.

It turns out that even more important than people liking us ... is us liking them. People like, and are inclined to follow, leaders who they perceive as liking them. If people perceive the *CISO* likes them, they are more inclined to say yes to the *CISO*.

What a golden opportunity for the *CISO*! The *CISO* needs to go out of his way to find legitimate opportunities to demonstrate to the people he works with that he really truly likes them.

Add the *liking trigger* to the other five persuasion trigger and the *CISO* has a sure-fire winning strategy for changing the organization's culture, changing how the organization *perceives, thinks, and feels in relation to information security problems*, and supporting the organization's becoming *skilled at creating, acquiring and transferring knowledge about information security, and at modifying its behavior to reflect new information security knowledge and insights*.

A thoughtful *CISO* can use the liking trigger in so many different ways. Rather than the *CISO* imposing information security requirements on people — a clear signal that she doesn't respect them enough to solicit their input — a better strategy is to ask their opinion about how best they can secure information — thereby clearly demonstrating that she values their opinion; that she likes them.

To influence people, win friends. An effective *CISO* will always be on the lookout for opportunities to establish

goodwill and trustworthiness, to give praise, and to practice cooperation.

To the extent the *CISO* shows she likes the people in the organization and to the extent she shows that she shares their concerns and problems, to this extent will people provide her with opportunities to change the culture.

A Warning. Ignore at Your Own Peril:

Integrity and honesty are absolutely vital in the application of these persuasion triggers. The six triggers have been shown to work in persuading people to act in ways desired by the persuader. Obviously, this power can be used for both good objectives and cynical ones. *To be effective as a change agent, however, the CISO must take pains to use his power of persuasion ethically.* If people perceive a lack of moral or intellectual integrity on the part of the *CISO*, they will not only not follow him, they will become even more cynical about the attempt of the information security organization to force change upon them. Instead of embedding information security concerns in the larger culture, the larger culture will reject the embedding attempt.

Summary

The effectiveness of an information security program ultimately depends upon the behavior of people. Behavior, in turn, depends upon what people know, how they feel, and what their instincts tell them to do. While an awareness training program can impart information security knowledge it rarely has significant impact on people's feelings about their responsibility for securing information, or their deeper security instincts. The result is often a gap between the dictates of information security policy and the behaviors of our people. It is the role of culture to close this gap.

It is the *CISO*'s responsibility to provide the organizational leadership required to change how the organization *perceives, thinks, and feels in relation to information security problems*, to embed the information security subculture into the dominant culture of the organization. Meeting this responsibility requires the *CISO* to evolve an *information security learning organization, one skilled at creating, acquiring and transferring knowledge about information security, and at modifying its behavior to reflect new information security knowledge and insights*.

At a deep strategic level, the *CISO* can only do this in harmony with the basic principles of real power, seeking to create the spaces in which information security learning can take place. Tactically, *the CISO has available six specific persuasion triggers* that taken together open up the spaces in which information security learning can take place. By ethically applying these persuasion triggers over and over and over again, day-in and day-out, the *CISO* has the opportunity to win the hearts and minds of the people, making information security come alive, so that everyone in the organization, from the CEO to the receptionist, can evolve an *information security mindset*.