Creating an Intentional Culture of Security

Jo Stewart-Rattray, MEdStud (Psych), CISA, CISM, CGEIT, CRISC, FACS CP

It has been said that organisations have two assets that are more important than any other and there is some debate as to the order in which they should be ranked. They are: people; and information.

It therefore follows that if information is so highly ranked then its protection should become part of the culture of the organisation. However, recent research[1] shows us that organisations do not generally have effective information security cultures particularly those where the intentionality of the culture is embedded into the day to day operations and practices of the organisation.

So how does this differ from our current view of Culture?

ISACA's Business Model for Information Security defines Culture *as "the pattern of behaviours, beliefs, assumptions, attitudes and norms in an organisation".*[2] Culture is not simply limited to what the Executive mandates! (Although Executive buy in is incredibly important to embedding the appropriate values into the culture of any organisation.)

Culture is not just about the rules or the social and organisational norms that have been created over time but rather culture should be seen as how 'stuff really gets done' in organisations.

Embedding this deeply rooted type of security culture into an organisation's corporate identity is not a quick fix but rather requires a longitudinal approach. It must be learned and it must be supported by senior management in order to give the required degree of comfort across the board. There are other factors too that should not be downplayed when considering developing an intentional culture of security and these include geographic location, political, ethnocentric and economic climate, to name just a few.

The importance of the component parts of a shared culture is often under-estimated. For instance, there are the assumptions people make and the beliefs that exist throughout the organisation that combine to create the organisation's culture. Assumptions and beliefs often evolve into a shared history and assumptions become behaviours which in turn become the norm, or the unwritten rule.

It is interesting to look more deeply at 'how stuff gets done'. Take for example, the written procedures an organisation has in place for something as simple as password resets. The procedures are of no use if everyone bypasses them because there is a shared belief that

[1] ***The Business Model for Information Security,*** (2010) ISACA, Rolling Meadows, Illinois, USA
[2] ***Creating a Culture of Security,*** (2011) ISACA, Rolling Meadows, Illinois, USA

the real way to get a password reset quickly is to bypass the written process and go directly 'Fred in IT' and ask him to do it!

If this norm were to be modelled to a new employee an expectation would be set and the behaviour exhibited by the long term employee would be the behaviour that is transferred. Therefore, the norm has been embedded in to the daily practices, and therefore into the culture, rather than the desired behaviour.

Once norms have been established in this way they are usually hard to break or indeed to change them at all. Human beings are naturally resistant to change!

Commitment to an intentional culture must be modelled throughout the organisation. For example, if the rules say that all staff must undertake security awareness training online but the managers do not ask employees to do so, or they ask them in a way that does not emphasise the importance of undertaking such training therefore staff are likely to think that security is not important.

For a culture of security to be effective it must be strong and strongly supported by senior management, well-organised, aligned with corporate goals, be consistent and contribute to the overall governance posture of the organisation.

The level of security employed to protect an organisation's information assets must be considered and should be commensurate with the value of the information and in line with the business context of the organisation and the environment in which it operates.

In the first instance all of these elements are consciously included when building the intentional security culture but over time that same culture will become unintentional or instinctive as it becomes part of the organisation's DNA. Organisations need to have security engrained so deeply into its DNA that people do not have to think about doing something securely – they just do it.

Sometimes security is viewed negatively because it is perceived to be oppressive and constraining. In reality, no-one is actually opposed to security; who could possibly favour the notion of insecurity? There is often a vague and sometimes naive element of trust within organisations. There is a belief that someone else is doing something about security but whereas security is actually the responsibility of every individual in the organisation and it is this seed that needs to be planted to enable the security culture to move from intentional to instinctive.

Successful creation of an intentional culture of security depends on all or at least most stakeholders accepting and wanting to promote security as something of benefit to themselves as well as the organisation. It necessitates creating an image of security as an essential contributor to business and not a necessary, but unwelcome, burden for an organisation to carry.

Cultural changes can and do happen but they will take time. Small intentional changes can have ripple effects across an organisation. For example, increasing collaboration between groups can increase trust and bring people together to achieve a common goal.

Often times, once people begin to work together they begin to share experiences which will help to improve relationships and attitudes. Being prepared to deal with change is an essential part of the process of moving toward the preferred future state of security.

Perceptions are important. The security professionals within the organisation must show that security is not an obstacle but an enabler and other people need to be able to accept that. And Information security professionals must speak the language of business if they hope to enshrine security principles into every employee's every day practices to create an instinctive culture of security.