Understanding and Transforming Organisational Culture

D. Lacey

Abstract

Since the introduction of computers, information systems and data have been repeatedly undermined by design flaws, weak passwords, lost media, social engineering and numerous other bad practices. These risks continue to grow with the increasing complexity and connectivity of modern business systems. But actions by people are not only the cause of incidents, they are also the means to prevent, detect and resolve them. People design, implement, operate, use and abuse information systems. And in the process they make mistakes or create weaknesses that enable criminals to steal, corrupt and manipulate information assets. Addressing these risks cannot be done through technology and process alone. It requires an understanding of the principles for understanding organizational culture, creating awareness, and changing attitudes and behaviour. This paper presents a range of observations about the nature of organizational culture, as perceived by an experienced information security director, as well as a set of practical techniques, based on psychological principles, that have been found to be effective in helping to achieve desired changes in human security behaviour.

Keywords

Information Security; Risk Management; Security Awareness; Organizational Change

1. Why contemporary awareness campaigns fail

A spate of well-publicised data breaches in recent years has prompted demands by a range of stakeholders to improve security culture in organizations that handle sensitive personal information. This should be a source of good practice but, unfortunately, the approach adopted by most remedial initiatives suggests that little impact will be achieved. In practice, most security awareness campaigns turn out to be little more than token gestures, based on a handful of hackneyed slogans, a few gimmicks (such as customised mouse mats) or a tough-sounding warning from top management. Such awareness campaigns fail because they are built on the best endeavours of security managers rather than the fundamentals of psychology and marketing communications. And some campaigns, especially those following a major incident, can turn out to be counter-productive, as they encourage a damaging blame culture that is far from conducive to good security behaviour.

The root cause of this situation is an ignorance of the key requirements for an effective change campaign, such as an understanding of psychology, experience of marketing communications, and the use of proven methodologies to change human behaviour. Indeed, it is rare to witness a security awareness or behaviour change

programme that is actually based on fact-finding, research or scientific principles. The consequence is that many security professionals conclude that education campaigns are not very ineffective, leading to a loss of appetite for investment in projects expected to deliver a minimal improvement. The answer is to design organizational change programmes that are based on a better analysis of the problem space, and that draw on best practices from psychology and marketing communications. The starting point for this approach is an understanding of the nature of organization culture, as well as the key principles for achieving changes in people's attitude and behaviour.

2. What is organizational culture?

There are many descriptions that attempt to explain the essence of organizational culture. It might be thought of as the attitudes, values, beliefs, norms and customs of an organization. Or it can be seen as the outcome of conversations and negotiations between members. Or perhaps just a pattern of basic assumptions that has worked well enough in the past to be considered valid. Statements such as these are worthy of attention as they suggest some of the things we might consider in order to understand how to influence organizational culture. Influencing discussions across social networks would, for example, be an obvious starting point.

But identifying and understanding organizational culture is never easy, especially if you're a part of it. Much of the culture that shapes our actions is an invisible "madness" that surrounds us, a peculiar set of customs and habits that we've all unconsciously elected to adopt for selfish reasons, such as greed, fear, survival or success. We rationalise such conformist actions to ourselves as "normal" behaviour in order to survive an otherwise alien corporate environment. The result is that we're rarely conscious of the hidden fog of organisation culture. In fact, it generally takes an outsider to see it for what it really is.

Influencing organization culture requires us to understand, sympathise and compensate for the circumstances, limitations and aspirations of staff, as well being alert to the politics of the day. The starting point is good relationship management, an ability to observe and listen, supported by patient diplomacy. Unfortunately these are skills that are becoming harder to practice in an increasingly demanding, competitive and fast-moving business environment.

3. The nature of security culture

When it comes to deciding what style of security culture we are seeking, we have a spectrum of possibilities. We can design it around negative motivators, such as fear and paranoia, or around positive ones, such as openness, trust and empowerment. But pride and joy will always be more effective motivators than fear and greed. Reward is more powerful than punishment, and inspiration is a better lever than authority. In reality, however, the tone for a security culture is generally shaped by top management's reaction to damaging security incidents. In particular, the political climate associated with the aftermath of a damaging or embarrassing incident will set

the tone for the consequential remedial security programme. Top management will wish to deflect the outrage expressed by citizens and stakeholders towards a suitable scapegoat. They will demand urgent change and visible action. Heads will be expected to roll. And managers will be expected to be held more accountable in future. Unfortunately, such actions will not correct the underlying causes of the incident. On the contrary, they will generate a smoke screen that masks the real problems. There are further factors that serve to reinforce such a negative response, such as a belief that fear, paranoia and punishment are the basis of a healthy security culture. This misconception is often encouraged by a contemporary management style that has become increasingly brutal and unforgiving, reinforced by a corporate rewards system that makes it easier to sack people than to promote them. A culture of fear will have some impact in making employees more cautious in managing information, but it will not eliminate the honest mistakes that are caused by poor process design.

Experience in the safety profession has demonstrated that the most major safety incidents are blame-free, i.e. no particular individual can be considered directly responsible. Security incidents are likely to follow a similar pattern. If this is the case, then identifying a scapegoat will only serve to deflect remedial action from the true underlying causes of the incident. It will also promote a damaging "blame culture", which will undermine future cooperation, discourage risk taking and prevent honest reporting of factors that might contribute to further incidents. In fact, a blame culture is no less than a culture of lies, deception and avoidance of responsibility. Such a security culture should not be regarded as a healthy business practice.

4. Addressing the root causes of incidents

The vast majority of mistakes that cause major security incidents are caused by human factors that are not associated with bad behaviour. Factors such as stress, lack of training and supervision, and bad system design often lie behind many contemporary breaches. We should not blame individuals for mistakes and omissions without first investigating the reasons for their errors. In practice, it's often found that the best performers make most mistakes because they tend to work harder, faster and are more empowered. The sensible response to an incident is to address the root cause of the incident, rather than focus on the trigger or the person who pulled it. But such a response is neither obvious nor easy for most managers, as it demands a level of enlightenment and a degree of confidence (e.g. to challenge top management) that is rarely encountered in most organizations.

The safety field has long understood this problem and employs a defence-in-depth approach (or "Swiss cheese" model as they prefer to call it). Aviation safety practice, for example, is underpinned by regular inspections and root cause analysis of minor incidents, including near misses. The BS7799 security standard was designed to deliver a similar defence-in-depth approach, but contemporary information security management remains weak in monitoring near misses and conducting root cause

analysis of minor incidents. Security managers also place less emphasis than their safety counterparts in building preventative measures in new system developments.

A further problem is the heavy reliance on risk management in the security field to determine preventative measures. In particular we need to understand and accept human limitations for assessing risks. Risk assessment is a subjective blend of logic and gut feeling, generally with the latter dominating the former. In theory, risk management appears to be a very simple process. But, in practice, people turn out to be astonishingly bad at both assessing and managing risks. Our perception of risks is shaped by many personal factors, including experience, current agenda, personality, gender, age, culture and religion. Risk management is far from a perfect science. Neither future events, nor their full business impact, can be predicted with any certainty. And the process of reducing complex risks to simple, short descriptions and scores limits its value as a decision-making technique. In fact, risk management should be seen as a decision-support tool. Business managers will not make big decisions on complex issues based on the output of a risk assessment exercise. But they will use that output to support decisions based a richer set of considerations. The risk management process is no more than the supporting evidence that a structured method has been applied to examining the potential impact of known hazards and potential future risks. It is far from being a reliable method for preventing future security incidents.

5. Planning an effective campaign

Changing how people operate in a working environment is not as difficult as most people imagine, but it requires a good understanding of human behaviour and best practices in marketing communications. Change programmes need to be based on a clear strategy, a good understanding of key problem areas, thoughtful analysis of the root causes of incidents, and an appropriate program of corrective actions. It is important to differentiate between the need for changes to *knowledge, attitude* and *behaviour* because the most appropriate initiatives are quite different. Conveying knowledge is a relatively straightforward task. It simply requires good, compelling communications. Changing people's attitudes is much harder. It requires a personal journey of discovery for the audience. Changing behaviour is the hardest challenge of all. It requires careful attention to a wide range of underpinning enablers and blockers.

Before we can design an effective campaign, we need to find out what people know and think about the security, as well as how they behave in practice. Questionnaires to measure this are not difficult to develop, and they also provide a good deal of useful information to help shape future security policy and to set priorities for security initiatives. Questionnaires also raise awareness and help gain staff involvement, which is a major factor in achieving "stickiness" in security campaigns. In addition, they provide a valuable set of metrics that can be repeated after a campaign, both to demonstrate an improvement, as well as to identify areas that require further intervention.

For maximum impact, security messages should be related to known business and personal issues. Images should be chosen that will resonate with people in the organization. Analogies help, as they will aid people's understanding and memory. Engagement is a powerful vehicle, e.g. using interactive methods such as games, quizzes or competitions. Professional support also helps, whether from professional writers, marketing experts or behavioural psychologists. Information security consultants rarely possess the necessary skills and their day rates are much higher than most other specialists. Modern channels, such as blogs, social networks and podcasts, should also be considered as they help to disseminate information in a real-time, interactive fashion.

Changing people's attitudes requires a self-discovery process, e.g. through vehicles such as games, stories or exercises. The choice of method is a matter of taste, imagination and budget. Films and case studies are excellent vehicles. Scenario planning is also a powerful method for changing mental models, encouraging managers to consider situations they would never otherwise have contemplated. On a lower budget, creative workshops or crisis exercises are also effective. People will generally be prepared to suspend their disbelief when confronted with an imaginary situation. They will cease arguing and become less defensive.

Transforming behaviour is much harder than changing attitudes. It requires attention to a much broader range of cues, capabilities and motivators that might serve to block or enable particular types of desired or unwanted behaviours. People's behaviour is influenced by many factors such as recent experiences, perceived roles, actions of colleagues, authority of management, local environments, and the cues and controls in systems. The most powerful impact is generally the perceived consequences of their actions, especially the ones that are *personal*, *immediate* and *certain*. Rewards always beat punishments, but in practice it's generally easier to sack people than promote them. Fear is therefore easier than inspiration to embed in the workplace. Environments also help to shape behaviour. People are influenced by the behaviour of people around them, as well as the sights they see. Groups of people will also behave differently according to the shape and size of their physical environment. And cyberspace itself has a major influence, encouraging many people to behave very differently than in the physical world, perhaps taking more risks, exploring darker subjects such as pornography, or becoming more hostile.

6. A new kind of information security

The BS7799 standard was a major breakthrough in its day. But it's a vehicle conceived more than fifteen years ago, reflecting the nature of information security management for a process-driven business world. And that world is changing. We need a more radical new approach for a real-time generation that operates in a nomadic, networked, script-free information society. It requires a progressive shift in emphasis from processes and procedures towards people, relationships and information flows. We need less focus on formal procedures and corporate dogma, and better engagement with people. And this needs to be more of a two-way, emotional, communications process, one that aims to harness the efforts of everyone

in the corporation, including customers and business partners. We need to exploit this collective vision and perception to understand the real causes of incidents and gain better visibility of events and their context.

The hardest of all issues to solve is the need for better information systems that make allowances for human error to help eliminate unnecessary mistakes, accidents and breaches. Good security design can only be achieved through closer observation of and engagement with users. We need to spend longer learning to appreciate their culture, requirements, likes, dislikes and expectations. Attention to detail is crucial when drawing up specifications because, in practice, the difference between a design that works and one that fails is often no more than a small detail or two.

7. References

Lacey, D. (2009), Managing the Human Factor in Information Security, John Wiley, London, ISBN: 978-0470721995