Understanding and transforming organizational security culture

David Lacey
David Lacey Consulting Ltd, Guildford, UK

Received 30 September 2009
Accepted 1 October 2009

Abstract

Purpose – The purpose of this paper is to examine the practical issues, techniques and learning points associated with information security awareness and organizational change programmes.

Design/methodology/approach – The paper is based on the findings and conclusions of research, observations and projects carried out in large organizations over the last two decades. It highlights failings and critical success factors in contemporary approaches to transform organizational culture. It draws on theory and research from the industrial safety field, and discusses its relevance in the information security field.

Findings – The paper identifies the primary reasons why many contemporary enterprise security awareness programmes are ineffective. It discusses the nature of the problem and solution space, identifying the practical issues and opportunities, and gives recommendations on how future programmes can be improved.

Research limitations/implications – The paper identifies gaps in current research, including the need to confirm whether or not certain findings about incidents in safety field might be applicable to security incidents. It calls for a new approach to information security management that incorporates theory and techniques drawn from psychology and marketing.

Practical implications – The paper is intended to educate students and researchers working in the information security field on issues and techniques associated with information security awareness and organizational change programmes. It also provides practical advice for business organizations on how to design and implement such programmes.

Originality/value – The paper takes a fresh approach to the subject, examining the relevance of theory and techniques adapted from other fields and drawing new conclusions about the requirements and approach for effective information security awareness and organizational change programmes.

Keywords Data security, Risk management, Organizational change

Paper type Research paper

1. Introduction

Ever since their introduction, the security of information technology systems and platforms have been repeatedly undermined by design flaws, weak passwords, lost media, social engineering and numerous other human failings. These risks continue to grow with the increasing complexity and connectivity of modern business systems.

Actions by people, however, are not only the cause of incidents; but they are also the primary means to prevent, detect and resolve problems. People design, implement, operate, use and abuse information systems. They make mistakes and create weaknesses, enabling criminals to steal, corrupt and manipulate information assets. But people are also the heroes that prevent a major security breach or turn an escalating crisis into a media marketing opportunity.

Addressing these risks and opportunities cannot be done through the traditional security focus on policies, processes and technology. It demands new interventions to change human awareness, attitudes and behaviour. This paper examines the nature

Information Management &
Computer Security
Vol. 18 No. 1, 2010
pp. 4-13
© Emerald Group Publishing Limited
0968-5227
DOI 10.1108/09685221011035223

of organizational culture, as perceived by an experienced systems analyst and former security director, as well as outlining a set of practical techniques that have been found to be effective in helping to achieve organizational changes in human security behaviour.

2. Why many contemporary campaigns fail

A spate of well-publicised data breaches in recent years has generated widespread citizen outrage and executive board demands for a more responsible security culture in organizations that handle sensitive personal information. In the UK, for example, the Poynter (2008) review of called for major changes in security awareness and behaviour following the loss of over 20 million personal records by HM Revenue and Customs (HMRC).

From a security management perspective, this new climate of stakeholder enlightenment provides an unprecedented opportunity to drive through long-overdue changes in the security attitudes and behaviour of staff. The outcome should be a wave of good security behaviour cascading across business sectors and supply chains. Unfortunately, in practice, we are unlikely to realise the sought-after step change in improvement. The reason for this pessimism is the approach adopted by security professionals towards the design of security awareness campaigns. Aside from a handful of well-funded campaigns triggered by high-profile breaches such as TK Maxx and HMRC, most campaigns are little more than token gestures, based on small budgets, weak content and *ad hoc* initiatives that do not deliver sustainable change.

Unfortunately, best practices in this solution space are more often judged by the forcefulness of management intent or the novelty of the interventions selected, rather than by the appropriateness of their design and the effectiveness of their impact. Some campaigns, especially those following a major incident, might even turn out to be counter-productive, as they encourage the establishment of a damaging blame culture which is not conducive to honest reporting of near misses and minor incidents. Most analyses of subsequent incident levels will also show that the initial impact of any campaign quickly fades, leaving little or no lasting effect on staff behaviour.

Contemporary awareness campaigns fail because they are built on the best endeavours of managers, rather than on sound principles of psychology and communications. The reason for this is that few security practitioners appreciate the key requirements for an effective change campaign: a basic understanding of psychology; experience of marketing campaigns and use of proven methodologies for changing human behaviour. Indeed, it is rare to witness a security awareness or behaviour change programme that is genuinely based on fact-finding, research and scientific principles.

An unfortunate consequence is that an increasing number of security professionals now conclude that awareness campaigns are ineffective, leading to a loss of appetite for further investment in people-oriented initiatives. Many streetwise security managers prefer to invest their scarce budgets and resources in security technology or process improvement. This is reflected in the relatively low levels of spending and staffing for security awareness in large organisations. Yet, the experience of organisations, such as the UK Royal Mail Group, that have actually measured the impact of targeted security awareness drives on incident levels, is that substantial financial and operational benefits can be achieved through carefully planned, relatively low-cost campaigns.

The solution advocated by this paper is to design organizational change programmes that are based on three critical success factors. First, a thorough analysis of the problem space, including a clear definition of the knowledge, attitudes and behaviour to be introduced, as well as an insight into the mindset of the audience. Second, a set of interventions that is consistent with basic psychological research and theory. And third, a selection of themes, images and messages that draw on best practices from advertising and marketing communications. The starting point for developing such an approach is an understanding of the nature of organization culture and the key principles for achieving changes in people's attitude and behaviour.

3. The nature of organizational culture

There are many descriptions that attempt to explain the essence of organizational culture. It might, for example, be viewed as the attitudes, values, beliefs, norms and customs of an organization. Or it could be seen as the outcome of conversations and negotiations between members. Another popular description is that it is a pattern of basic assumptions that has worked well enough in the past to be considered valid. Statements such as these might seem obvious or irrelevant to campaigns, but they are in fact more worthy of attention than they might initially appear. Their usefulness is in the fact that they point to some of the key things we might aim to influence in order to understand to change the organizational culture.

But understanding organizational culture is not an easy task. In practice, it can prove to be an elusive, evolving phenomenon that is difficult for both insiders and outsiders to grasp. A large part of it is impenetrable to outsiders, and at the same time, invisible to the participants themselves. Organizational culture is a major influence on thinking and perception that is hard to differentiate from one's own natural judgement and personality. It is, in effect, an invisible cloud of insanity that surrounds staff, something they have progressively and unconsciously absorbed, in the interests of their own success or survival, and often against their better, initial judgment. Organizational culture is an insidious, corrupting influence. Many people might set out to resist it, but it will gradually creep into their thinking and lifestyle, slowly shaping their outlook into a corporate or community perspective and influencing everyday views and behaviour.

New aspects of organizational culture are continually emerging and evolving, often combining in unpredictable ways to create varying influences across different groups of employees. Globalization of business units generates a cross-fertilisation of different perspectives and working practices. Mergers, acquisitions and recruitment drives introduce successive vintages of staff with new experiences and attitudes. Many local cultures might not survive through such a constantly changing environment, but they can endure for long enough to be an important influence that serves to block or support the successful execution of a security policy or programme.

The most significant emerging influence on organisation culture is the increasing exposure of staff to external interactions through social networking. This is a phenomenon which injects fresh perspectives on events and thinking, largely at the expense of local dialogues with nearby working colleagues. Many young employees now spend more time interacting with remote, networked contacts than with colleagues seated across the desk. The office is becoming an increasingly anonymous place, with responses to new issues shaped by external conversations, rather than internal debate.

Any attempt to change culture will need to take account of the constraints and opportunities offered by social networking.

Recognising organizational culture is never easy, especially if you are a part of it. Much of the culture that shapes our everyday views and reactions is a hidden filter that shapes our perception of events, reinforced by a set of customs and habits that have been unconsciously adopted for reasons of fear, survival or success. We will instinctively rationalise such conformist actions as normal behaviour in order to survive an otherwise dissenting, corporate environment. The result is that we are no longer conscious of this hidden fog of organisation culture. In fact, it generally takes an outsider to appreciate the true nature of an organization culture.

Identifying the factors and triggers that shape organizational culture, however, is a more straightforward task. Staff behaviour is influenced by many factors, including their immediate environment; the behaviour of peers; the demands of management; as well as perceived roles; past experiences; cues and prompts in systems and processes; and, most importantly, the perceived consequences of actions.

As mentioned earlier, useful vehicles for change can be found in the classic definitions of culture given at the start of this section: attitudes, values, beliefs, norms and customs; the outcome of conversations and negotiations between members; and patterns of basic assumptions that have worked well enough in the past to be considered valid. Changing organisational culture therefore requires an engagement with staff through social networks, and a convincing argument that existing assumptions are no longer valid.

As we shall see later in this paper, changing attitudes cannot be achieved merely by convincing, confrontational arguments. It requires a process of self-discovery on the part of the target audience. We have to present the case for change in a compelling form that people can consider, discuss and absorb on their own terms. Individual behaviours can be influenced by the introduction of specific motivators, but attitudes and culture are absorbed through a more subjective process, generally over a longer time period.

Influencing organization culture requires us to understand, empathise with and compensate for the circumstances, limitations and aspirations of staff. It is also vital to be alert, as far as possible, to the politics of the day. The starting point is to apply good relationship management skills, including the ability to observe and listen objectively, supported by a large dose of diplomacy. Unfortunately, these are rare skills that are becoming harder to find and apply in an increasingly demanding, competitive and fast-moving business environment.

4. The nature of security culture

Many security practitioners would like to introduce a better “security culture” into their organizations, but few can define precisely what that actually means. In practice, security culture means different things to different people. To some people, for example, it implies a disciplined approach to applying security controls. To others, it conjures up a mindset that is cautious and suspicious. In fact, when it comes to deciding the style of security culture we would prefer to encourage, we have a broad spectrum of possibilities. We can, for example, design it around negative motivators, such as fear and paranoia, or around positive ones, such as trust and empowerment. We can enforce discipline through fear of punishment, or through a promise of reward, but at the end of the day, pride and joy are likely to be more virtuous and lasting motivators than fear and greed.

Inspiration is a more powerful, compelling and longer lasting lever than authority, but, in practice, the nature of most security cultures is largely determined by senior management reaction to major security incidents. In particular, the political climate in the aftermath of a damaging or embarrassing incident will set the tone for any consequential remedial programme. Top management will generally wish to deflect the outrage expressed by angry citizens following a major security breach towards a suitable scapegoat. Executive boards will demand urgent change and visible action. They will expect to see heads roll and other managers held more accountable for their actions in future.

Unfortunately, such initiatives rarely address the true causes of incidents. Experience in the safety profession, for example, has indicated that most safety incidents are blame-free, i.e. no particular individual can be considered to have been directly responsible. Security incidents are likely to follow a similar pattern, resulting from a combination of factors rather than a single person's action. If this is the case, then identifying a scapegoat will only serve as a smoke screen of activity that deflects remedial action away from the underlying causes of the incident.

A further factor that serves to reinforce this negative response to breaches is the widespread belief that fear, paranoia and punishment are the basis of a healthy security culture. This perception is probably founded on an old-style, military approach to security, but it has also been encouraged by a contemporary management style that has become increasingly brutal and unforgiving. This approach in turn is often reinforced by a corporate rewards system that makes it easier to sack people than to promote them. A culture of fear will certainly have some impact in making employees more cautious in managing information, but it will not eliminate the honest mistakes that are caused by overworked executives, inadequate checks and controls, and poor process design.

Over time, a security regime based on fear and punishment is likely to encourage the development of a "blame culture" that undermines future cooperation, discourages risk taking and prevents honest reporting of factors that could contribute to further incidents. A blame culture is dangerous because it promotes an ethos of lies, deception and avoidance of responsibility. Such a culture can by no means be regarded as an acceptable business practice. In contrast, a healthy security culture is characterised by an informed awareness of security risks; a willingness to report incidents or weaknesses; frankness in assessments of security compliance; and a degree of empowerment to enable staff to take remedial action.

5. Addressing the root causes of incidents

If the blame for an incident cannot be attributed to a single individual, where might the fault actually lie? In fact, it is interesting to observe that the vast majority of mistakes that cause major security incidents are caused by human factors that are not associated with bad behaviour (Lacey, 2009). Factors such as stress, lack of training or supervision, and bad system or process design often lie behind many contemporary breaches. Management should not therefore seek to punish individuals for mistakes and omissions without first investigating the reasons for their errors.

In practice, it is often found that the best performers make the most serious and glaring mistakes because they work harder, faster and are more empowered. The logical response to a major breach is to investigate what went wrong, rather than who is to blame. The focus should be on identifying and addressing the underlying reason, rather than on the trigger of the incident, and the person who pulled it. But organizational responses are largely political, rather than logical, and such a response is neither obvious, nor easy, for most business managers. It demands a level of enlightenment on the nature of incidents, as well as a degree of confidence to challenge the instinctive corporate desire for a convenient scapegoat.

Security managers investigating the causes of incidents would do well to study the lessons learned in the safety field. Back in the 1930s, Heinrich (1932), an American industrial safety pioneer, published observations on the root causes and statistics behind major safety incidents in industry. Amongst other things, his research showed that as many as 95 per cent of all workplace accidents were caused by unsafe acts, and that almost nine out of ten accidents were caused by human failure. Further, he discovered that, on average, for every major incident in which someone died or was seriously injured there was an average of 29 minor incidents, in which someone is slightly injured, and as many as 300 near misses. Lurking behind these events we are likely to find thousands of bad practices.

The safety field therefore employs a defence-in-depth approach (or "Swiss cheese" model) that aims to collectively prevent a major incident by incorporating controls across a series of layers. Aviation safety practice, for example, is underpinned by regular inspections and root cause analysis of minor incidents, including near misses. These measures are intended to prevent the occurrence of a more damaging major incident. In contrast, the security posture of many organisations is shaped by knee-jerk reactions to major incidents that occur unexpectedly after years of neglect in maintaining controls and a failure to probe below the tip of the iceberg of visible incidents.

The BS7799 security standard was designed to deliver a defence-in-depth approach towards controls and compliance, similar to that applied in the safety industry. But contemporary information security management remains relatively weak in monitoring near misses and conducting root cause analysis of minor incidents. Security managers also place less emphasis than their safety counterparts in specifying and incorporating preventative measures into the designs of new systems and processes. And when they do apply preventative measures, they are more likely to be based on theoretical risk assessments rather than lessons from real-life incidents.

Risk assessment is a subjective, unpredictable blend of logic and gut feeling, generally with the latter dominating the former. On the surface, risk management might appear to be a simple, straightforward process. But in practice, people turn out to be astonishingly bad at both assessing and managing risks, and they are rarely equipped with the knowledge and skills to carry it out. Perception of risks is shaped by many personal factors, including experience, current agenda, personality, gender, age, culture and religion. It must be concluded that risk management is likely to remain a flawed and inconsistent management technique. Neither future events, nor their business impact, can be predicted with any degree of certainty. And the process of reducing highly complex risk scenarios to single paragraph descriptions and scores based on coarse scales will limit its value as a reliable indicator.

Risk management is best employed as a decision-support tool, rather than a decision-making one. Business managers cannot be expected to make big decisions on complex issues based on the output of a simple calculation. But such assessments will help to support decisions based on a richer set of considerations. Risk management provides valuable supporting evidence that a methodical analysis of known hazards and future risks has taken place.

Risk assessments cannot be regarded as a reliable method for predicting and preventing future security incidents. That can only be achieved by a real-time appreciation of the wide range of factors that contribute lead to unsafe acts and incidents. And many of these are human failings, such as a lack of knowledge or supervision, or the absence of appropriate instructions or cues on how to operate systems securely. Such failings might not be visible to management until checked or tested, but they can be corrected, at least partly, by an organizational change programme.

6. Planning an effective change campaign

Changing how people operate in a working environment is not as difficult as most people imagine, but it does require a good understanding of human behaviour and some appreciation of best practices in marketing communications. Change programmes will also need to be based on a clear strategy, a good understanding of key problem areas, a considered analysis of the root causes of incidents, and an appropriate set of remedial interventions.

It is important to differentiate between the need for changes to knowledge, attitude and behaviour because the interventions required 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, because it requires careful attention to a wide range of underpinning motivating factors.

Before we can design an effective campaign, we ideally need to find out what members of the target audience know and think about security, as well as how they behave in the everyday execution of their duties. In fact, questionnaires to measure this are not difficult to develop, and they are a valuable source of useful information to help shape future security policy and to set priorities for other security initiatives. Questionnaires also raise awareness and gain staff involvement, which is a major factor in achieving "stickiness" in security campaigns. In addition, they provide a valuable set of metrics, enabling the status of security awareness and behaviour to be measured before and after a campaign to demonstrate its impact and identify areas that require further intervention.

For maximum impact, security themes and messages should be related to known business and personal issues. Images should be chosen that are likely to resonate with the target audience. Analogies help, as they aid understanding and retention of information. Motoring, for example, is a popular and effective theme, as security measures can be explained through a comparison with the numerous checks and controls applied to car transport: design features such brakes and safety belts; infrastructure controls such as traffic lights and warning signs and governance measures such as driving tests and traffic police. Such analogies help people to appreciate why existing controls are necessary and why further levels of controls might be necessary.

User engagement is a powerful vehicle, which can be achieved through a variety of interactive channels such as questions, games, quizzes or competitions. Professional support helps enormously, whether from professional copywriters, artists, marketing experts or behavioural psychologists. In fact, information security consultants rarely possess the necessary skills for such work, and their day rates tend to be higher than journalists, artists and media specialists. Electronic channels, such as blogs, social networks and podcasts, should also be exploited as they help to disseminate information in a real-time, often interactive fashion.

Changing people's attitudes requires a self-discovery process, through vehicles such as games, stories, debates or exercises. The choice of media is largely a matter of taste, imagination and budget. Films and case studies are good vehicles. Scenario planning is also a powerful method for changing mental models or encouraging managers to consider "unthinkable" situations which they might never otherwise have contemplated. Creative workshops or crisis exercises are also effective. The use of fictional stories is especially useful in changing attitudes, as people are generally prepared to suspend their disbelief when confronted with an imaginary situation. In such cases, they will tend to refrain from arguing their own viewpoint, and become less defensive towards new ideas and perspectives.

Transforming behaviour is considerably harder than changing attitudes. It requires attention to a much broader range of cues, capabilities and motivators that block or enable particular types of desired or unwanted behaviours. Employee behaviour is influenced by many factors such as recent experiences, perceived roles, actions of colleagues, the authority of management, policies and instructions, the immediate environment (both physical and cyberspace), and the cues and controls in business systems and processes.

All of the above factors are worthy of attention, but the most powerful impact is generated by the perceived consequences of individual actions, especially the ones that are personal, immediate and certain. Any attempt to shape new behaviours should therefore commence with a review of perceived consequences, including those that encourage a desired action, as well as those that discourage an undesired one.

Consequences can be divided into positive outcomes, such as rewards or negative ones, such as punishments. In practice, the impact of rewards will generally beat that from punishments, as they are generally more welcome, intrinsic and longer lasting. In many organizations, however, it is easier to sack and discipline staff than to promote or reward them. Fear has therefore become easier than inspiration to embed in the workplace. And unfortunately, this tendency is reinforced by the growing numbers of aggressive personalities, including bullies, control freaks and potential sociopaths, that have risen up through the ranks of competitive organizations.

Environments also help to shape behaviour. People are influenced by the behaviour they observe in the people around them, as well as the sights they see. In fact, no security campaign will be effective if the desired behaviour is contradicted by the actions of colleagues within line of sight. Groups of people also behave differently according to the shape and size of their physical environment. A crisis team, for example, positioned in a large room will tend to break into smaller groups. Yet, the same team in a smaller room will remain as a single team.

Cyberspace itself also has a major and worrying influence on behaviour, encouraging many people to behave differently and adopt a different persona than when interacting with other people in the physical world. In particular, many people are inclined to take greater risks, explore darker subjects, such as pornography, and become more hostile to other people. Ordinary computer users can, on occasions, be tempted to generate aggressive e-mails that could not possibly be repeated in a face-to-face confrontation.

Suler (1996), a researcher on the psychology of cyberspace, calls this the "online disinhibition effect". On the internet, people relax, become more open, and are less inhibited. Several factors contribute to this effect. First, there is the feeling of anonymity that cyberspace encourages. Second, there is a false confidence generated by a delayed response to user actions. A further factor is the merger of fantasy and reality, which is reinforced by our perception that the imaginary characters we have created might actually exist, perhaps in a make-believe world that does not demand the same responsibilities as the real world. The consequence is that ordinary users can adopt rules and norms that are different to those they might apply in the physical world. In effect, they become imaginary people carrying out acts that have no real consequence on the physical world.

There are many factors and layers that lie behind a person's identity and personality. People are complex and different. But it is clear that many can be inclined to develop online identities and personalities that are markedly different from physical, face-to-face ones. And the behaviour associated with such online identities tends to be more open, less inhibited and increasingly daring.

Addressing user behaviour in cyberspace is difficult, as it is harder to incorporate cues and interventions for desired behaviours across a portfolio of online systems. In a normal working environment, interventions such as posters, signs and leaflets can easily be introduced. In contrast, it can take substantial time and effort to introduce changes to commonly used platforms and information systems. The messages, however, will be largely the same as the audience rather than the media will dictate the nature of the required intervention.

7. Preparing for a new kind of information security

The BS7799 standard was a major breakthrough in its day, but it is a vehicle conceived more than 15 years ago, perhaps reflecting the nature of information security management for a process-driven business world. And that world is changing. BS7799, and its successor ISO27001, were designed primarily for a business environment in which repeatable processes dominated the value chain. Implementing security required controls to be embedded in business processes, procedures and infrastructure. In contrast, we now need an approach that matches a more dynamic business environment that is less constrained by repeatable processes. Implementing security now requires more attention to people, rather than processes or infrastructure.

This implies the need to develop a different approach to security management: one that caters for a real-time generation of users, operating in a nomadic, networked, and increasingly script-free, information society. Achieving this goal 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 more on genuine engagement with people. This demands a two-way, emotional, communications process, and one that aims to harness the efforts of everyone in the corporation, including customers and business partners. We will need to exploit this collective vision and perception in order to understand the real causes of incidents and gain better visibility of events and their context.

Perhaps, the hardest of all issues to solve is the need better information systems that make allowances for human error in order to eliminate unnecessary mistakes, accidents and breaches. But good security design is expensive and time consuming to develop. It can only be achieved through a closer observation of human behaviour and greater engagement with users. We need to spend a greater deal of time learning to appreciate our users' culture, requirements, likes, dislikes and expectations. We must also practice greater attention to detail when drawing up user 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.

Achieving these goals requires us to re-think both the essence of security management and the nature of the knowledge, skills and organization demanded by this changing business environment. In a future world in which citizens are fully connected and services are delivered from within an internet "cloud", the major thrust of security functions will not be to articulate legalistic policies and technical architecture, but to change the perception and behaviour of thousands of managers, staff and customers. Responding to this challenge demands a greater emphasis on the "softer" skills of psychology, education, marketing, communications and change management. Preparing for that change should be the major priority of information security training, education and business functions across the world.

References

Heinrich, H.W. (1932), *Industrial Accident Prevention: A Scientific Approach*, McGraw-Hill, New York, NY.

Lacey, D. (2009), *Managing the Human Factor in Information Security*, Wiley, London.

Poynter, K. (2008), *Review of Information Security at HM Revenue and Customs*, available at: www.hm-treasury.gov.uk/d/poynter_review250608.pdf

Suler, J. (1996), *The Psychology of Cyberspace*, January, available at: www.usr.rider.edu/~suler/psycyber/psycyber.html