THE FUNDAMENTAL IMPORTANCE OF AN INFORMATION SECURITY CULTURE

When Even the Best Technology Cannot Provide Full Information Security

Really effective information security has never been something that can be "bolted onto" an organisation. True, technology exists today for dissimulating or blocking access to information electronically. However, not only insufficient as a solution to the overall challenge of information security, technology is also aggravating the problem. Current trends confirm this. BYOD (Bring Your own Device) computing is an example, in which members of an organisation use their own computing devices for work and for leisure. The cohabitation of organisational and personal data, and the mobility and vulnerability of that data outside corporate confines has given rise to yet more automated measures of security. However, they each share the same fundamental limitation.

The Human Factor at the Heart of the Problem

Why can technology alone not provide all the answers to the problem of information security?

Simply because members or employees in an organisation still need access to information. Computer saboteurs and data thieves know that the easiest way to get what they want is often via people, not software hacking. They exploit the ignorance of human beings, or their carelessness in using the very technological tools that are supposed to protect them. In fact, the more the information of an organisation is protected by the latest and most advanced technology, the greater will be the temptation for its members to assume that they have no further need for caution when handling organisational information.

The Risks of Serious Damage through Compromised Data

An organisation whose employees are offhand in their approach to handling information can suffer the impact of an information security problem in several ways. Sensitive product data that finds its way to competitors, customer data that is exposed to cyber-criminals and negative publicity leading to an image of carelessness that can adversely affect relationships with partners are all possibilities. In extreme cases or through knock-on consequences, any one of these can ultimately force an organisation to cease functioning.

Fixing What Needs to be Fixed – the Information Security Culture

Considerable study has been made of the customs, beliefs and unwritten rules of organisations – in short, their culture. It is this culture that influences how its members think and act at work. This includes their attitude and behaviour concerning the information they handle. While culture has often featured in discussions concerning areas where the human factor is obvious, such as sales or customer services, it has frequently been neglected when technology is more present, for example in information processing. Yet it is of vital importance and must be nurtured, repaired and developed as required.

Approaches for the Orientation and Evolution of Behaviour

Working to appropriately shape or transform organisational culture is the way to fulfil effective information security. Between the proven theory and the constraints of the workday in an organisation, a way has to be found to encourage and develop the behaviour required to keep data secure. Experts and pioneers in this field, such as TreeSolution Consulting, have designed methodologies to produce positive changes in information security awareness, behaviour and culture that are not only measurable, but also durable.

Developing the Pay-Off, as well as Preventing the Problems

The right information security program does not just help an organisation avoid the disasters of information leaks, thefts and damage. In its application to different groups in an organisation, a program can also lead to higher productivity and improved teamwork, thanks to optimised procedures and levels of information access. This cost-effectiveness can be maintained in the same way in additional or subsequent refresher programs.

Keeping the Information Security Culture Alive and Well

The importance of an information security culture is also in its permanence. For such a culture to be durable and to continue being effective, organisations also have to pay attention to the frequency of appropriate awareness campaigns, and how the message is communicated. Once a high level of awareness has been achieved and the right behaviour is apparent within the organisation concerning information security, follow-on effort may be less than in the initial campaigns, but cannot be zero. Times change, threats alter and, quite simply, people also forget. Continuing and visible management commitment to an information security culture, as well as correctly adapted levels of internal publicity and participation, are two axes along which an organisation can continue to prevent information security problems and benefit from program payoffs.

About TreeSolution Consulting GmbH

TreeSolution is a consulting company specialised in information security awareness and behaviour, with a unique focus on information security culture and technology. The company can be contacted by phone at +41 (0)31 751 02 21, by email at contact@treesolution.ch or by using the contact form on the website of the company at http://www.treesolution.ch.