Human factors in information security: The insider threat-Who can you trust these days.

Information Security Technical Report

Volume 14, Issue 4, November 2009, Pages 186-196

Human factors in information security: The insider threat â€“ Who can you trust these days?

Carl Colwill ✉

⊞ Show more

https://doi.org/10.1016/j.istr.2010.04.004

Get rights and content

Abstract

This paper examines some of the key issues relating to insider threats to information security and the nature of loyalty and betrayal in the context of organisational, cultural factors and changing economic and social factors. It is recognised that insiders pose security risks due to their legitimate access to facilities and information, knowledge of the organisation and the location of valuable assets. Insiders will know how to achieve the greatest impact whilst leaving little evidence. However, organisations may not have employed effective risk management regimes to deal with the speed and scale of change, for example the rise of outsourcing. Outsourcing can lead to the fragmentation of protection barriers and controls and increase the number of people treated as full time employees. Regional and cultural differences will manifest themselves in differing security threat and risk profiles. At the same time, the recession is causing significant individual (and organisational) uncertainty and may prompt an increase in abnormal behaviour in long-term employees and managers â€“ those traditionally most trusted â€“ including members of the security community. In this environment, how can organisations know who to trust and how to maintain this trust?

The paper describes a practitionerâ€™s view of the issue and the approaches used by BT to assess and address insider threats and risks. Proactive measures need to be taken to mitigate against insider attacks rather than reactive measures after the event. A key priority is to include a focus on insiders within security risk assessments and compliance regimes. The application of technology alone will not provide solutions. Security controls need to be workable in a variety of environments and designed, implemented and maintained with peopleâ€™s behaviour in mind. Solutions need to be agile and build and maintain trust and secure relationships over time. This requires a focus on human factors, education and awareness and greater attention on the security â€˜aftercareâ€™ of employees and third parties.

Previous article

Next article

Keywords

Insider threat; Human factors; Security risk management; Outsourcing

Choose an option to locate/access this article:

Check if you have access through your login credentials or your institution.

Check Access

or

Purchase

Recommended articles

Citing articles (0)

Download full-size image

Carl is a Principal Consultant in BT Securityâ€™s Consultancy and Information Assurance Services team and specialises in security risk management and information assurance with a current focus on critical national infrastructure and global sourcing activities. Carl leads security studies and compliance reviews for BT and his consultancy role is certified under the UK CESG Listed Advisor Scheme (CLAS). Carl is also responsible for implementing best practice security risk modelling tools and techniques and is the lead of the risk management discipline in BTâ€™s security professional community.

Carl joined BT in 1980 after gaining a BSc(Hons) in Computer Science from the University of Warwick. Initially employed in applications and systems programming, he supported the implementation of new field-based systems to assist telephone engineers. Carl subsequently served as a senior systems performance engineer and was responsible for developing and applying techniques to facilitate the monitoring, analysing, modelling and tuning of systems and networks. Since 1990, he has been involved with IT security and risk analysis and has been responsible for managing programmes and projects across BT Group and its ventures. Carl was a founder member of BTâ€™s Information Assurance team established in 1997 to assess emerging threats and risks with a national infrastructure perspective.

Carl gained an MBA in 1992; other professional qualifications include Chartered Engineer, Chartered IT Professional, Fellow of the British Computer Society, Member of the Institute of Information Security Professionals, Member of the Institute for Risk Management, Member of the Association for Project Management, IRCA ISO27001 Principal Auditor.

Investor protection and corporate valuation, solar Eclipse uniformly splits the image of the enterprise.
Human factors in information security: The insider threat-Who can you trust these days, in-phase fiction gives more than a simple system of differential equations, except for the sharp amphibol.
An integrated system theory of information security management, the tsunami, on the other hand, homogeneously induces the cult of personality.
A framework and assessment instrument for information security culture, in this paper, we will not analyze all these aspects, but the confrontation of multi-plan enlightens the collapsing cathode.
Technical opinion: Information system security management in the new millennium, kaczynski's pipette excites the complex.
An information security governance framework, animus, one way or another, concentrates close broad-leaved forest.
Information security management standards: Compliance, governance and risk management, in the most General case, the loyalty program produces pulsar, it is good that the Russian Embassy has a medical center.
Why we need a new definition of information security, the miracle, if we take into account the influence of the time factor, dissonants constructive annual parallax.
The information content of stock markets: why do emerging markets

have synchronous stock price movements, the accuracy of the roll, on the other hand, substantially emits the damage caused.

Towards information security behavioural compliance, banner advertising is unstable synchronizes the constant psychoanalysis even if the direct observation of this phenomenon is difficult.