Wake-up call to business: Tighten up on information security

June 30 2008

According to the Department of Trade and Industry there are 4.5 million businesses in the UK of which 99.3% are small to medium sized enterprises (SMEs), employing 0-49 employees. These comprise 58.9% of the total workforce of 24.4 million and account for 51.9% of the £2,600 billion UK turnover. Bruce Hallas, a specialist in information security, said "SMEs are particularly prone to poor or even non-existent information security. As awareness of the importance of information security increases, the SMEs stand to lose competitiveness, potentially losing contracts with existing clients and suffering the financial consequences that are increasingly arising from information security incidents."

An over reliance on Information Technology (IT) has developed over recent years. According to Hallas, this is the result of confusing Information Technology with Information Security (IS). With 'insufficient' money to invest in expensive information security expertise, many SME's are investing heavily in IT in the mistaken belief that IT will ensure IS.

"Yet the largest business drivers for security investment are contractual, regulatory, market pressures from consumers, corporate clients and the public sector. Not the typical domain of IT. The biggest security vulnerability lies with people," Hallas says. "Security is about managing the risk from people, both known and unknown, interacting with your information and information systems. It is more about people management than technology."

Tyler Moore of the Computer Laboratories, University of Cambridge expanded, "Information security is now a mainstream political issue, and no longer the province of technologists alone," he said. "People used to think that the internet was not secure because there was not enough of the right technology, not enough sophisticated cryptographic mechanisms, authentication or filtering etc. so advanced encryption, public key infrastructure and firewalls were added. The internet did not get any safer," he added. "In 1999 it became clear that even the latest and greatest technology will not solve all our problems if those who protect and maintain them are not sufficiently movitated. The issue is one of incentives."

The impact of an under-incentivised workforce can have devastating consequences in business such as denial of service attacks allowing viruses to infect the IT system, hospitals putting access to data above patient privacy, bank customers suffering phishing attacks by poorly designed banking systems.

"Economics can explain many of the failures and challenges in a new way" Tyler Moore said. "As companies are beginning to realise the value of good information security practice so security measures are being used not only to manage the evils of the attackers but also to support the business models of companies."

Now that the Achilles heel of the information security problem has been identified, companies, especially banks, often fight shy of divulging information about attacks, whether they have been successfully repelled or not because the information concerned may be sensitive.

Help is at hand in the form of a new report "Security Economics and the Internal Market" which outlines police options regarding the economic problems in providing IS.

The report's first recommendation is for the EU to issue a comprehensive breach notification law to notify consumers when their details have been compromised so they can protect themselves.

Source: Economic & Social Research Council

Citation: Wake-up call to business: Tighten up on information security (2008, June 30) retrieved 26 April 2024 from https://phys.org/news/2008-06-wake-up-business-tighten.html

This document is subject to copyright. Apart from any fair dealing for the purpose of private study or research, no part may be reproduced without the written permission. The content is provided for information purposes only.