New cybercrime law is too vague to protect UK businesses from malicious hackers

Submitted by: Pleon
Thursday, 22 February 2001

Internet security consultancy @stake claims new legislation highlights general misunderstanding of corporate security

New anti-terrorism laws that came into force on Monday 19 February 2001 under The Terrorism Act 2000 c.11 will mean that criminals face arrest and prosecution if the cybercrime is found to be motivated by religious, political or ideological beliefs. According to Part I, section 2E of The Terrorism Act, terrorism can be defined as an action, "designed seriously to interfere with or seriously to disrupt an electronic system".

Royal Hansen, practice director Europe @stake, commented, "Although, the new legislation highlights the Government's growing realisation that e-security is a real threat to the bottom line of UK businesses, companies cannot rely on the act for protection. It is not sophisticated enough to react to the crime and not sufficiently well known to act as a deterrent. Hacking is a valuable skills set for developing new security technologies, but when these actions are malicious they can also cause real losses to business. The seriousness of the problem is highlighted by recent figures showing that criminal hackers cost European businesses $4.3 billion in the last year - on average 5-7 per cent of revenue to each company. These threats demand real-world solutions."

Hansen continued, "While no company's data can be completely secure, businesses should look to evaluate their individual security requirements. Rather than relying on a legislation that will be difficult to enforce, each business must identify the risk of security exposure, together with the cost of implementing a solution, and assess the level of security needed to protect their sensitive data."

About @stake

@stake works where business and technology intersect, because that is where security is most powerful. The firm integrates technical and business expertise to build security solutions that look beyond the network to the security of applications and data, and future business goals.

@stake couples vertical industry expertise in three areas-- financial services, communication service providers and e-markets-- with pioneering research, to design and build strategic security solutions that enable the

electronic business initiatives of its Global 2000 clients. Amidst other providers for whom security services are a way to sell products or drive the sale of broader service offerings, @stake stands out with its dedicated focus on security consulting services and the unmatched calibre of its people.

@stake security consultants and research scientists built their expertise at premier organisations including the L0pht, Cerberus Information Security, DERA, the National Security Agency, Axent, BBN, Deloitte & Touche, Open Market and RSA. @stake matches its unparalleled security talent with equally strong vertical industry and business expertise drawn from Sapient, Cambridge Technology Partners, Arthur Andersen, Fleet, Fidelity, Exodus, Nortel and Interpath.

Contact Brodeur Bfour

Matthew Ward/Lena Ahmed

mward@brodeurbfour.com

or lahmed@brodeurbfour.com

Telephone +44 (0) 1753 44 8875/8861