1240/5(1979)

QUESTIONS TO BE ASKED OF THE PRESIDENT OF THE POLICY AND RESOURCES COMMITTEE ON TUESDAY, 4th NOVEMBER 2003 BY THE DEPUTY OF ST. JOHN

Question

Would the President inform members –

(a) how many different computer systems are believed to be operated by the States?

(b) whether the Committee has any plans to centralise all these systems under the control of one department and Chief Officer?

(c) of the number of occasions on which the States I.T. systems and websites have been infected by computer viruses and state what action, if any, is being undertaken by the Committee to prevent this from happening in the future?

Answer

(a) In total, the States operates approximately 250 computer systems comprising a mixture of corporate applications used by many departments (financial management, word-processing, e-mail, etc.) and line-of-business applications operated by departments to carry out specialist functions (e.g. clinical systems used by the department of Health). Service delivery to end customers is provided by a mixture of these.

Whilst a very limited number of the line-of-business applications have automated links with others, the vast majority were developed as stand alone systems, not intended to share information or make use of other information sources. This presents a considerable challenge as the States works towards becoming a customer focussed organisation. The technology building blocks, for which funds were agreed in 2002, will provide the infrastructure to improve this position in the future, but the underlying problem of discrete systems remains and will need to be dealt with over time.

(b) The Committee has been aware of the need to take a more corporate approach to the provision of IT across the States. The IT Director has proposed a structure for the organisation of IT across the States based upon a hybrid model in which some functions are centralised and some remain departmental responsibilities. This distributed approach is proposed within a wider structure that identifies an IT ‘Head of Profession’ to whom all States of Jersey IT staff will report (either directly or indirectly) for various matters, such as job descriptions, job families, policy and standards, compliance, succession planning, use of resources, etc.

The proposal is intended to find an efficient mix of centralised and departmental IT activity, to minimise duplication, maximise user support, and ensure that specialist requirements of the business are met by those most able to do so. The proposal has been circulated to members of the Corporate Management Board for their consideration before wider distribution.

(c) The States’ network is constantly assaulted by viruses and network attacks. During September 2003, the main corporate Internet gateway stopped 760 e-mail borne viruses and 5,600 unsolicited (SPAM) messages - typically these figures increase month by month. In the past three years, of the many thousands of attacks, only three viruses have penetrated the network and resulted in downtime for States’ systems, preventing some staff from being able to carry out work as desired. None of the attacks affected core data or systems or resulted in any long-term problems with the States’ IT infrastructure.

The most recent attack (the ‘Blaster’ worm) affected many businesses both locally and globally, and many were very severely affected. Only some 20 per cent of States of Jersey desktop computers were affected (no servers), caused, it is believed, by a failure of an unknown individual within the States network to comply with States security policy. This attack highlighted the need for a change in security procedures, and as a result, the Computer Services Department has reviewed and tightened virus protection and software update procedures, and has followed an industry trend towards securing not only the corporate internet gateways, but also the core network itself.

As reliance upon IT to deliver key services increases the risk and impact of virus attack will increase. Furthermore, the States of Jersey needs to ensure that it is not the source or unwitting carrier of viruses to others and so, in common with all other organisations who use IT, the States has no choice but to maintain robust defences.