Audit Committee follow-up

Bennetts End Adventure Playground Theft.

Members will recall that at the last meeting of the Audit Committee on 8th December there was an action for me to request a meeting of the OSC Chairs and Vice-Chairs to discuss their Risk Registers. Whilst it is important that OSC should be fully aware of their Risk Registers, following a discussion between Cllr Tiley and me it was felt that in this particular case it would be more beneficial to meet with the Chief Executive, Daniel Zammit, to inform him of the interest that members had shown regarding this situation and to affirm that the appropriate actions had been taken both to minimize any effect of the break-in and to protect the council against the consequences of a similar situation occurring in the future.

I duly met with Daniel Zammit on 5th January 2012.

The break-in was effected through a number of locked and secured elements and various items were stolen, including a computer. Immediately this theft was known, a meeting was convened with all relevant operational managers and IT managers, both to review the nature and level of sensitivity of information which had been stored on the computer and to assess whether any data handling was contrary to policy and operational procedures. It was confirmed that some supporting personal information had been stored on the computer at a local level. The relevant contacts for those whose data was stored on the database were written to but it should be noted that there was very little response from them to this incident.

At the same time, the Assistant Director (Legal, Democratic & Regulatory) advised the Information Commissioner of the incident setting out the background and advising the security arrangements. The Police, investigating the incident, confirmed that the physical protection to the property was reasonable and adequate.

Within 48 hours of the theft, steps were also taken to ensure that all data is no longer kept locally at Adventure Playgrounds but is up-loaded to the central DBC server where it is stored securely. Access to it from a local point is via password protected encryption.

Internal Audit was requested to carry out an audit, the results of which were reported to the Audit Committee on 8th December 2011. This recognised that policy procedures had not been adhered to correctly and the Assistant Director wrote immediately to all staff of the data storage arrangements and the need for a high level of vigilance at all times including the requirement to correctly follow the policy procedures.

I believe that the policy procedures are now in place to minimise the risk of any such loss occurring in the future.

Terry Douris