HOTEL ENGINEER

PP 319986/101

Volume 22, Number 2

AUSTRALIAN INSTITUTE OF HOTEL ENGINEERING INC.
AIHE

Official Publication of the Australian Institute of Hotel Engineering

independent SECURITY AUDIT

SIMON HENSWORTH I BSC (SECURITY SCIENCE) ICCP (ADVANCED)

How do you know if your security is effective? Do those responsible for providing your security effectively manage your security risk? Is the security of your assets of concern to those who maintain your security arrangements or is it just another job? If these questions instil even the slightest of doubt about the effectiveness of your security then please read on.

Many organisations outsource the security function to external contractors. This can be a way to minimise permanent employed staff and reduce costs but it also has the potential to degrade the effectiveness of security in a number of ways. The following sections outline a few.

DEDICATION OF PERSONNEL

Those at the coal-face of operational security such as security officers, if outsourced, do not directly work for you. Therefore there can be outside factors that motivate their performance. If there is an issue with the level of service provided, rather than losing their employment, they may simply be moved to another client with little real impact to them personally. This may have an impact on their motivation and loyalty, which are important factors for those given the responsibility of managing your security risk.

LACK OF RISK MANAGEMENT

Organisations can sometimes assume that a security contractor is providing effective security that will address relevant security risks. If the contractor is technically based, such as an Alarm, Access or CCTV technician they may not get involved in security risk management at all. Their primary role may be to ensure the electronic security systems are functioning. It is very different to ensure that the security systems are effectively managing the organisation's security risk.

Contractors can often assume that a client is happy with the level of security provided if they are not informed of issues or require improvements by the client. These assumptions can lead to a situation where each party (contractor and client) assumes that security risk is being managed by the other, but in fact is not being managed by either.

If a rare but significant security risk is one day realised, the impact generally only affects the organisation. There is generally no impact on the contractor other than the potential to sell further products/services following a raised perception of risk.

INCENTIVES IN SECURITY'S LACK OF PERFORMANCE

Whilst most security service providers are upstanding citizens with a genuine interest in providing top level service, it should be noted that some may see a lack of security performance as a way to sell more of their products/services. If their performance (or lack of performance) results in security failures that appear to be outside of their control they may end up selling their client more security.

LACK OF DOCUMENTATION IN ORDER TO BUILD RELIANCE

When security is outsourced, contractors can sometimes limit the level of documentation on security systems as a way to maintain their control of the facility and make it difficult for a competing contractor to replace them. The contractor can often become the only one who knows anything about the security systems that are managing the organisation's security arrangements. This can build a reliance on the contractor to make even the most simplest of changes to the system. This can be exacerbated by contractors who deliberately withhold information and/or documentation regarding security systems in order to develop a position of total dependence.

EXTERNAL SECURITY EXPERTISE AND KNOWLEDGE

When knowledge of the organisation's security only resides outside the organisation, an organisation can lose sight of whether security arrangements are effective, efficient, or even operational. This can make security risk management very difficult for the organisation.

INDEPENDENT SECURITY AUDIT

The above issues can be overcome by either employing the security function internally within the organisation, retaining a limited internal security role to oversee and manage contractors such as a knowledgeable fulltime Security Manager, or ensuring a sufficient independent security audit is carried out to verify the effectiveness of security service and performance.

INDEPENDENT SECURITY RISK ASSESSMENT

If it cannot be conducted internally, an independent security risk assessment can be conducted. Even though independent, the security risk assessment will rely heavily on input and involvement by personal within the organisation who can provide details regarding organisational risk criteria, operations, criticality of assets, potential threats and vulnerabilities and their likely impacts. An independent security risk assessment can provide advantages over an internal assessment due to an external perspective which may bring fresh ideas and solutions to the process.

CONTRACTUAL CONTROLS

Elements of an independent security audit should be incorporated into contractual documentation. For example, when new security systems need to be implemented, the scope of work for the project should be clearly documented and stipulate requirements for deliverables which assist in auditing security and the contractor's performance. This may include the provision of As Constructed documentation, independent inspections by the project Superintendent during testing and commissioning, and final inspections prior to the end of defects liability.

VERIFICATION OF INSTALLATIONS

Following the installation of a security system, independent verification of the conformance of the installation to the contractual documentation is vital. Without independent verification contractors can miss details or even intentionally underperform to save costs.

During such inspections it is not uncommon to find omissions such as installation of products that are inferior to those specified and priced, failure to correctly configure security resulting in ineffective performance, failure to program systems to client's requirements or even missing out whole elements from the scope of work.

VERIFICATION OF DOCUMENTATION

Review of As Constructed documentation and manuals as part of an installation of new systems is equally important as physical inspections. Documentation often misses the detail required for effective ongoing management of systems and should be carefully assessed to ensure accuracy and suitable level of detail.

SCHEDULED AUDITS

Scheduled audits of security arrangements should also be considered to assess effectiveness and highlight areas where improvements may be required. This can be very important if such a review has not been conducted for a number of years and the security function has not been critically assessed as to whether it is effectively managing the organisations security risk.

SUMMARY

While outsourcing can appear to be the simplest and cheapest option to maintain a security function, the reduction in security risk management, service and performance should be factored into the equation. Organisations need to be mindful that managing security risk should be in the hands of those who have a personal interest in the organisation's risk minimisation, and not managed by a party who could benefit from a security failure. Depending on the risk profile of the organisation the right balance of in-house security, outsourcing and independent testing needs to be carefully weighed and decided.

NOTE:

The issues discussed in this publication are of a general nature for the purposes of increasing Security Awareness throughout industry and the wider community. It is recommended that organisations undertake their own security risk assessments in order to determine the most appropriate action and arrangements to minimise loss and maximise their security performance.

ABOUT THE AUTHOR.

Simon is a Senior Security Professional with Engineering Technology Consultants – ETC. Simon has over 13 years' experience in providing security advice, design and consultancy services for a range of clients with major assets in Western Australia. He is a registered Security Professional on the Australasian Security Professionals Registry and one of 10 CPTED practitioners certified by the International Crime Prevention Through Environmental Design Association (ICA), worldwide. Simon is involved in all aspects of Security Management, security design and documentation, CPTED and promoting Security Awareness.