



*Mike Jay convenes the RISCAuthority Security Group (formerly the IPCRes Group). The group monitors the property crime environment for its members, the great majority of UK's commercial insurers. It carries out research and publishes guidance documents on security issues of the day. In previous times its projects would have been taken on in an ABI forum.*

It goes without saying that the security of the keys to premises and intruder alarm systems is critical. The great majority of insurance policies operate on the basis that thieves must resort to force and violence to enter the premises. If, through some 'expedient', a possibility exists that the thief could gain access to the keys or codes, and thereby enter the premises without breaking in, most policies will not pay out. Even 'full theft' policies, which do not necessarily require there to have been a violent entry, can not be relied on if the policyholder has knowingly agreed to a situation whereby the thief was able to quickly and easily obtain the keys. Owners must exercise 'reasonable care' and act no differently from an uninsured owner if they are to avoid jeopardizing the insurance protection.

Traditionally, the security of keys has been taken for granted. The client has them in his pocket and takes them home after he's locked up. Or does he?

Recent developments in the response and keyholding market, and the BSI committee that sets its ground rules, are giving rise to concern in insurance circles. This comes at a time when insurers have for years been cooperating with clients - even encouraging them - to employ commercial keyholding services.

It seems these services, in their drive to be as efficient, competitive and profitable as possible, are arranging with their clients for premises keys and access devices/codes to be available to their crews in keyboxes outside the premises. Undeniably an efficiency gain, this enables the keyholding firm to deal with call-outs without first having to return to base to collect the keys or carry them on the vehicle.

But what exactly is a 'keybox' and how secure is it? There may well be an answer to this in other countries where keyboxes have been a feature for many years - chiefly with the aim of eliminating any avoidable delay in fire brigade intervention in an emergency. However it would seem that in this country the most you can say is that a keybox is 'a box for keys'. There does not seem to be a public standard for such a receptacle or its security. Neither do we know where it is to be located and fixed but we assume it is attached somehow to the outside of the alarmed premises in an accessible position.

When BS7984:2008 Keyholding and Response Services was revised recently a move was made to include reference to site key storage. However no new requirements were made other than to add a clause pointing out that such facilities may not be as secure as storage within a defined 'secure facility' and that keyholding operations should seek written acknowledgement and acceptance from a customer as to the potential security risks. There is also a clause requiring that written quotations make it clear that it is the customer's obligation to check with their insurer that use of site key storage is acceptable.

The security implications are obvious. Any intruder gaining access to the keybox - either opening it in situ, or removing it and opening it elsewhere - will possess the physical means both to unlock the premises entry door and unset the alarm. Once safely inside the premises, no longer protected by any security system, the amount of time intruders have to deal with any internal security and inflict theft or damage will be limited only by the arrival, at some point, of a keyholder - either to open for business or responding to a message from the ARC (assuming they receive and react to irregular opening times). Insurers are very concerned and presumably installers may not be too happy with the implications either.

Insurers are anxious that policyholders should not unwittingly find themselves unable to claim on their policies and the Security Group within the insurers' technical committee structure, now known as the RISCAuthority (formerly InFiReS-IPCRes), has recently circulated a bulletin to members on this subject. In it insurance surveyors and underwriters are reminded that policyholders who allow use to be made of a keybox put their insurance at risk. If a claimant can not show that force was used to break in or that he had exercised all normal care in the safe custody of keys he will probably be in difficulty. Especially so if his policy has an intruder alarm condition requiring that the insured:

- 'maintains the secrecy of codes and security of keys and setting/unsetting devices for the operation of the intruder alarm system'
- and that
- 'all keys and other setting/unsetting devices for the intruder alarm system must be removed from the premises when they are left unattended'

This is not to say that insurers have a dogmatic policy on keyboxes - there could well be circumstances in which an underwriter would accept their use. However such situations are more likely to be at lower levels of risk or in the household sector.

The RISCAuthority group speculates that the keyholding market could well find the attractions of keyboxes irresistible and roll them out across customers at all levels of risk. It is vital that customers enter into these arrangements knowingly and consider the implications. It will be essential for customers to refer proposals for the keybox solution to insurers. The group hope that SSAIB installers share their concerns and will help open customers' eyes to the issues.