



PLANNING FOR A SECURITY REVIEW?

You breathe a sigh of relief – you’ve finally sorted out the security contract and now have an accredited Security Industry Authority (SIA) provider in place. You’ve built a good relationship with the provider and all the necessary Service Level Agreements (SLAs) and Key Performance Indicators (KPIs) are in place. Even the finance director is happy with the cost of the service. You can now sit back and leave it to them...or can you?

You might have total confidence in your security provider to provide you with up-to-date, appropriate solutions to your particular needs but it is still worthwhile reviewing your company’s security requirements with them on a regular basis.

In their July 2007 survey the Security Industry Authority (SIA) found that many companies do regularly scrutinise their security contracts.¹

WHY REVIEW IS IMPORTANT

Regular reviews are built into any contract lifecycle in order to check that the provider is meeting client needs. However, contract review time can also be an opportunity for the company to reassess its security requirements and to discuss them with the provider. In these days of changing technology and increased potential threats it is important that your business is effectively protected, even when cash is tight. John Saunders, former Chief Executive of the SIA has said that security should not be purchased on a **“buy the very least from the very cheapest”** basis.²



Instead, companies should work with security providers to ensure that security expenditure is based on sound, verifiable business requirements. It is therefore crucial that you have an awareness of the security challenges facing your business, and that you keep that awareness up-to-date. Things change, new threats and vulnerabilities become apparent and effective security should reflect this.

A security review might be triggered by a scheduled 6 monthly contract re-negotiation or in response to business environment changes. The latter could include new threats to your type of business or your location, changes in legislation or insurance requirements, or new technological developments. You might initiate a security review if acquiring or extending premises, as it will be cheaper and more effective to consider security at the planning stage than to add measures later. It is also worth noting that many of the security precautions typically used to deter criminals are also effective against terrorists. So, before you invest in additional security measures, review what you already have in place. The National Counter Terrorism Security Office (NaCTSO) also recommends that you review the effectiveness of your security:

- after a security incident within your business.
- after a security incident in your neighbourhood.
- after a change in your business practices;
- when information is received about threats.

Frequency of Security Contract Review	% of Companies
0-6 months	36%
7-12 months	32%
Every 2 years	15%
Every 3 years	12%
Every 4 years	5%

CATALYST FOR REVIEW

It is important to review all your security measures regularly to ensure that they continue to support the needs of your business.

25 years of expertise providing total security solutions



WHAT TO REVIEW

To some extent what you review will be determined by what is in your current security contract, particularly if you are working in conjunction with a provider who has Approved Contractor Scheme (ACS) accreditation, as they will already be formally committed to reviewing the quality of their provision. Suggested areas to cover and questions to ask include the following:



TRAINING

Is security training taking place?
Do personnel understand it?

Are regular reviews and rehearsals taking place and are these recorded (eg fire drills)?

Is training planned and documented?



RISK ASSESSMENT

Have your risk assessments been conducted? Are there potential new threats to your particular industry/business sector? Crime prevention measures are only effective if they are targeted correctly and are based on evidence. There should be crime prevention and security measures in place that are appropriate to the company based on an analysis of the risks. 'In order to ensure that an organisation is secure, the risks it is exposed to need to be understood. To demonstrate this, senior managers need to be able to describe the risks posed to the organisation and explain how the risks and incidents are recorded, monitored and analysed. Senior managers should also be able to explain how the information collected is used to create a secure working environment. Managers need to be able to explain the importance of reporting to create a secure environment. Employees should be able to explain what they need to do to report an incident and provide examples of when they have done this.'

Source: ACPO 6 Principles of Secured Environments.

SECURITY PLAN

Is the plan understandable?

Is it site-specific?

Who has responsibility for it?

Are they ensuring the plan is implemented?

Does the plan have breadth, i.e. does it cover not just premises but employees, information, suppliers, customers and the maintenance of the company's good reputation?

Is supporting documentation accessible, clear and up-to-date?

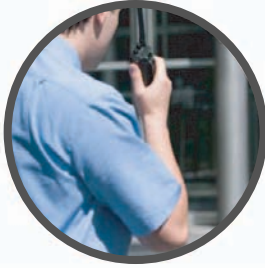
In order to create a secure environment the organisation needs to have a plan in place to achieve its aims and objectives. All security measures should be proactively managed, this means that security measures should be planned.

IN-HOUSE PERSONNEL ISSUES

Do management demonstrate their commitment to security? Are personnel aware of relevant security issues? Are meetings on security held regularly? Are personnel security checks carried out, both as part of recruitment and as an on-going process?

SECURITY PROVIDER PERSONNEL

How are their personnel selected for work? Have they the relevant qualifications? Have they the right to work in the UK? Concerns from the UK Border Agency over the scale of illegal working in the UK private security industry led to the revocation of 7,700 licences between 2007 and 2008.³



SECURITY PROVIDER

What price are they charging? Are they ACS accredited? What do they offer your company over and above other providers? Security measures can be expensive and it is important to track these costs to enable effective budgeting. You need to show that you know what resources (e.g. people, time, money and technology) are used within the company to create a secure environment and that this is an efficient use of available resources.



USEFUL WEBSITES

www.the-sia.org.uk

www.crimereduction.gov.uk

www.nsi.org.uk

www.mi5.gov.uk

www.acpo.police.uk

www.cpni.gov.uk

www.bsia.co.uk

www.nactso.gov.uk/documents/secure-in-the-knowledge.pdf

www.gbsg.co.uk

SUGGESTIONS FOR REVIEW IMPLEMENTATION

- Discuss review areas with security service provider.
- Canvass opinion from security stakeholders, management and staff, other businesses, Business Crime Reduction Centre, the local authority and police.
- Take a walk around the premises to check physical assets.
- Collect relevant documentation, reports, advice from web sites.
- Discuss potential for more integrated systems with a suitable supplier; ideally a 'one-stop-shop' to ensure compatibility and co-ordination.
- Consider what is available from alternative security providers.
- Develop an action plan for security in conjunction with your selected security provider.
- Brief management on developments.
- Monitor provision of security service in accordance with standards agreed.
- Keep up-to-date with security developments in your geographical and business area.

SUMMARY

It is essential that crime prevention initiatives and security measures are assessed to determine whether they are effective. This may occur in a number of ways, for example through testing existing security measures and processes, or through auditing and evaluating systems. Your company may use one or all of these methods depending on the size of the company and its security risks. But whatever method you use you need to be able to explain how security measures and crime prevention methods are monitored and evaluated, and how the findings are fed back into the security strategy. You need to be able to explain how a crime prevention initiative or security measure has been improved based on the findings from an evaluation. By regularly reviewing security requirements and contracts you can ensure that security complements the critical parts of your business and supports day-to-day running.

If you require more information concerning the integration of costeffective technology into your company's security systems please visit www.gbsg.co.uk. For more general advice please refer to the useful website section.

REFERENCES

- 1 SIA Research Findings: The Impact of Licensing on Door Supervision and Security Guarding July 2007, p57. SIA.
- 2 Spotlight on Security November 2005, p4. COR/05-06/10 CBI.
- 3 Vernon Coaker Under Secretary of State for Crime Reduction: SIA Annual Report and Accounts 2007/08.
- 4 Professional Security Magazine Online: Retailer's Savings, 02 March 2006.
- 5 SIA: Mind the Gap, SIA Corporate Update England and Wales, Spring 2007.



PHYSICAL MEASURES

Are appropriate physical measures such as locks, alarms, CCTV surveillance, complementary lighting and glazing protection in place? Is Visitor Access controlled?

ELECTRONIC SECURITY MEASURES

Are they working? How regularly are they maintained? Do they cover essential business and security assets? Could some physical assets be replaced by electronic ones? The dramatic increase in the sophistication of the technology of security systems solutions has resulted in huge benefits for the business community. When configured together as an integrated solution the benefit of the whole is greater than the sum of its parts.

Typically an integrated solution can involve some or all of the following: CCTV, Automated Gates/Barriers, Access Control, Perimeter and or site Intruder/Fire Alarms, Process Control, Temperature Control, Building Management and other Alarm Systems and Remote Control/Monitoring of some or all of the above devices. In 2006, GBSG installed integrated systems on two of Pinguin Foods Ltd's (a food company) sites, consisting of CCTV, Access Control, Gates and barriers, and interactive Monitoring. The company made annual savings of £100k+ over the two sites compared to their previous manned guarding contracts.

MFI furniture company went to IP (internet protocol) and they have saved approximately **£110,000** yearly on guarding at two sites.⁴

Some electronic measures can have a wider application than just security: for example, smart cards, tokens or fobs are easier to control than keys. Lost cards or fobs can simply be deleted from the system, and a new ones issued to a legitimate user. Electronic tracking of such devices could also be used to help you locate staff more easily, or record their times of entering and leaving the building. Tagging all equipment also makes a computerised inventory of the entire business simple to set up and manage.

COMMUNICATION AND AWARENESS OF SECURITY ISSUES

Are you a member of a local Business Watch or a similarly constituted group? Do you know your local community police officer or community support officer? Do you speak with neighbouring businesses on issues of security and crime that might affect you all? Are key security stakeholders aware of which assets are critical to business success and the security measures in place to protect them? Do personnel know who to contact regarding security? 'Last year, the SIA conducted an in-depth study of corporate attitudes to security, in conjunction with the readers of leading business publications Facilities Management Journal, Security Management Today and Financial Director. The results were revealing. The study suggested that more than three quarters (78 per cent) of financial directors, those who control the budgets for corporate services have little idea about how their companies buy security. Furthermore, over half (55 per cent) didn't know the name of their security supplier, and believed that the majority of their board members would be similarly un-informed.⁵

INFORMATION SECURITY

Are regular information back-ups conducted? Do you lock away all business documents at the close of the business day? Are all your computers password protected? Do you have computer firewall and anti-virus software on your computer? Do you regularly update this protection? For today's companies the potential threat and impact of your computer system crashing is much greater than a leak of confidential commercial information, as shown below.

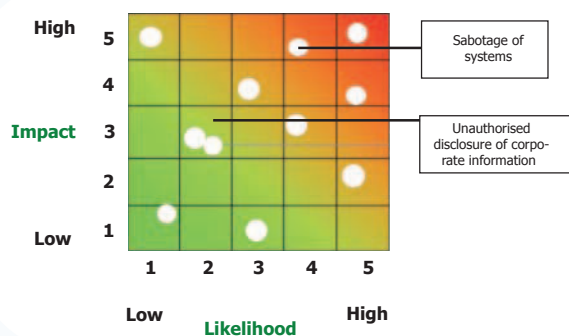


Diagram: Illustrative use of a risk matrix showing how the sabotage of IT systems is a greater risk to a hypothetical organisation than the unauthorised disclosure of specific corporate information.