

# Comment

## CAUSE OF FALSE ALARMS

### Cable standard for a reason

**There's a cable standard for a reason – so don't let the cable be the weakest link in your system, warns distributor ADI-GARDINER's Intruder Product Manager Yvonne Butterworth.**

Because if it is, a fault is very difficult to find – and expensive to put right, she adds. We are all quite correctly obsessed with meeting the tighter specifications for intruder systems and products, as most recently is the case with PD6662, yet we seem to ignore that most universally used product in all installations, good old security cable, says Yvonne. "Cable is cable, one is just as good as another" is one of the most repeated phrases I hear among installers. Not only do I doubt that was ever true, but it is certainly not the case now! There is a cable standard for a reason." BS4737 Part 3 is designed to approve a cable with the minimum of resistance, and therefore ensure the effectiveness of the system and reduce the incidence of false alarms due to signal drop. Security cable might not appear to be the most sophisticated of components, yet its characteristics are absolutely vital to the efficiency of the installation, and if inferior product is used, it can easily be an unwelcome cause of false alarms, she reports. □



#### UNHAPPY

**'No matter how well defined, tested and understood the security policies, and no matter how well the technology is doing its job, there is always the human element.'**  
**Enemy at the Water Cooler (Syngress), a study of insider threats by Brian T Contos.**

All this page's articles were, in full, added to the Professional Security site [www.professionalsecurity.co.uk](http://www.professionalsecurity.co.uk) in December and January

### Risks of technology

**Organisations face serious security risks and tough legal penalties if they fail to bring employee communications under control, warns Nick Kingsbury, chief exec of Chronicle Solutions.**

Today's employees are highly empowered and have unprecedented power to access and compromise systems, infrastructure and confidential data across the organisation, potentially leading to serious, irrecoverable damage to the business interests of the organisation. These issues cannot be ignored for they now form part of the regulatory compliance requirements for most large

### Approved firms stand to benefit

**Late as I was for the SIA approved contractor forum on November 10, 2006, I was impressed none the less with the content of the well presented seminars, writes Essex-based AA Security director Wilson Chowdhry, pictured.**



Directors that espouse the SIA ACS scheme stand to benefit significantly from major alterations to the licensing remit that will include electronic applications by companies via a basic spreadsheet or linked to their HR systems. One question unanswered is a poignant concern about the callous selection of rogue security providers; that are continuing to breach SIA legislation; by clientele that are in their awareness of this breach conniving with miscreant company. This collusion should be met with abhorrence by our

sector, the SIA and Government. The wheel is turning and our industry is definitely the better for licensing not many could argue with this. However, the SIA must increase the level of incentivisation for good practice especially in respect to ACS contractors that are actively promoting compliance and subject themselves to the highest scrutiny within the industry. The professional organisations have settled into the sphere of regulation with consummate ease, the initial

panic spurred 280 companies into entering an elite quorum. It is now up to the others to match or exceed this achievement. Cost benefit analysis is the order of the day! I can confirm that my company AA Security has more than doubled in turnover since the fateful day that we achieved our ACS. Furthermore, the conniving companies still financing the rogue element within our industry, may be obtaining security on the cheap at this stage. However long term implications do not look so favourable now that this debate is out in the open! □

### From A to BC: Steven Garrod, of Garrison Continuity suggests writing business continuity plans step by step.

Be it an art or a science, writing a business continuity plan on a blank piece of paper is almost impossible to get right. Yet this is what many people set out to do when they begin to develop a business continuity plan for their business. The work of writing a plan should start way back, thinking about the risks faced by your business and the scope and scale of any impacts that may result. If you don't have a clear idea of what you are trying to protect – and what you are trying to protect it from – how can you know what to put in the plan and what to leave out? □

Garrison is among exhibitors at Business Continuity - The Risk Management Expo 2007 at London's Excel, Docklands on March 28 and 29. Visit [www.businesscontinuityexpo.co.uk](http://www.businesscontinuityexpo.co.uk)

organisations. And if they haven't yet hit home then they shortly will, as new compliance demands have an inevitable tendency to be rapidly cascaded across jurisdictions, business sectors and supply chains. But the traditional fixes will not work in today's new business environment of empowered, streetwise, mobile employee. Clear 'acceptable use' policies supported by ongoing education campaigns are essential to steer employee behaviour in the right direction. But these softer processes alone are not sufficient. They need to be reinforced by smart use of special purpose technology. □ Chronicle is exhibiting at the Infosecurity Europe 2007 information security event, from April 24 to 26 in the Grand Hall, Olympia, London. Visit [www.infosec.co.uk](http://www.infosec.co.uk)