

## TEN TIPS TO KEEP IT SECURITY COSTS DOWN IN THE RECESSION

By Ian Kilpatrick, chairman Wick Hill Group, specialists in secure infrastructure solutions

### 1. Move to UTMs (unified threat management systems)

UTMS save money over multiple point solutions. They can cost just a quarter of the price of multiple solutions.

With UTMs you have fewer devices, so you can save on energy costs, rack space and air-conditioning. If you deploy multiple UTMs throughout an organisation, and use centralised management and reporting, you can significantly reduce the time spent on admin and management. There are also fewer ongoing management costs from factors such as training, maintenance and upgrades. And you only have one dedicated platform to support. Companies such as Check Point, WatchGuard and NETGEAR have solutions in this area

### 2. Beef up your web filtering

List-based web filtering security tools don't provide effective control against proxy anonymisers, which allow staff to browse restricted sites undetected by many web filtering systems. Consider moving to solutions that provide protection against anonymisers, so you can significantly increase productivity, as well as improving security. Marshall8e6, Barracuda Networks and Finjan are among the companies who offer products here.

### 3. Close down the bad guys

Close down the areas that you weren't too happy about but may have ignored in the past. For example, P2P, streaming media and IM. Not only do they represent a significant security risk, they also have an extremely high cost in wasted staff time. Solutions are available that let you manage these areas, alongside traditional web risks. They include those from Marshall8e6 and Barracuda Networks.

### 4. Deal with non-work related emails

Inappropriate and non-work related emails not only carry major legal risks for organisations but also have a huge security and productivity cost. Yet many organisations are completely blind to the level or nature of the activity. Solutions are available that allow you to manage non-work related emails and increase productivity, without upsetting staff or disrupting business.

### 5. Deploy encryption

The lack of encryption can lead to data being viewed by unauthorised people, both inside and outside an organisation. The cost of dealing with such data leakage incidents is massively larger than the cost of preventing them in the first place. In a recession, the damage to reputation can be even more expensive. We are all too painfully aware now, that data leakage is not an isolated thing and can strike all sorts of companies. Encryption used to be expensive and disruptive to install, but this is no longer the case, and most companies can afford to use it. Solutions are available from Check Point (Check Point Endpoint Security) and HP.

### 6. Two factor authentication

The cost of managing passwords can be extremely expensive in terms of helpdesk resources. And weak passwords put your business at risk. Two factor (soft or hardware) tokens cost only a few pounds, less

than the price of one helpdesk call. They can secure your business effectively, particularly where you have a lot of remote and mobile users. Suppliers include CRYPTOCARD and VASCO.

#### 7. Hosted security

For some companies, hosted security can be a more cost-effective option than handling all security needs yourself. It can cover any type of environment and includes office based systems, remote locations, home offices and mobile laptops. You can host all or just some of your security needs. Cost savings can come from areas such as not having to pay all the costs associated with installing and managing hardware and software. There are many companies in this area including Kaspersky Lab and CRYPTOCARD.

#### 8. Compliance

The burden of proving that your IT security is compliant to an ever-increasing range of laws and regulations can take up costly manpower. Solutions are available which can automate the collation of security data from devices and systems across your organisation, and make it readily available when you are called upon to prove your compliance. They save on manpower and on the possible cost consequences of not being able to prove you are compliant. These include solutions from ArcSight and LogLogic.

#### 9. Bring staff on board

Using your own staff is a major way to secure your systems. Retrain staff and remind them that data security is their responsibility and crucial to the survival of the business. In tough times, the message is more likely to strike home and be appreciated.

#### 10. Review AV.

Many anti-virus and end point solutions create a large load on PC resources with big updates and processor intensive scans. With budgets under threat, desktop refreshes are being delayed. Using efficient low footprint anti-virus extends the life of PCs and laptops. Kaspersky Lab is proven to have one of the lowest system footprints of any anti-virus

Bio - Ian Kilpatrick

Ian Kilpatrick is chairman of value added distributor Wick Hill Group plc, specialists in secure infrastructure solutions. Kilpatrick has been involved with the Group for more than 30 years. Wick Hill is an international organisation supplying most of the Time Top 1000 companies through a network of accredited resellers.

Kilpatrick has an in-depth experience of computing with a strong vision of the future in IT. He looks at computing from a business point-of-view and his approach reflects his philosophy that business benefits and ease-of-use are key factors in IT. He has had numerous articles published in the UK and overseas press, as well as being a regular speaker at IT exhibitions.

END

For further press information, please contact Annabelle Brown on 01326 212130, email [abpublicrelations@btinternet.com](mailto:abpublicrelations@btinternet.com). For reader queries, please contact Wick Hill on 01483 227600, web [www.wickhill.com](http://www.wickhill.com). For pic of Ian Kilpatrick, please contact Annabelle Brown or download from <http://www.wickhill.com/company/press/pictures.php>