

DON'T LET YOUR BUSINESS GO DOWN WITH THE FLU BUG

Ten tips to keep your business going in a pandemic

by Ian Kilpatrick, chairman Wick Hill Group, IT security specialists

If a flu epidemic really does take hold in this country, will your business be able to survive minus large numbers of staff? Ian Kilpatrick, chairman Wick Hill Group, specialists in IT security, gives ten key actions companies can take and explains how business can continue if staff are able to work from home.

1. Check your insurance. You're probably not going to be covered for business losses if a pandemic strikes, so you need to plan to minimise the impact.

2. Get the plan in place NOW. If you need to implement any new equipment, you don't want to be doing that during the first or second wave of flu. And staff may not be available at your suppliers or onsite to carry out any installations.

3. Identify key staff. Pinpoint IT, management and administrative staff who will need remote communications access, so they can carry on working from home. Determine what level of access is required, confirm home and mobile phone numbers are current, and confirm home addresses. If you want staff to access the computer network remotely, confirm whether they have home PC access, that the line speeds are OK and that they are running current anti-virus!

4. Confirm by testing that these staff are able to access and use the relevant systems remotely. Unless you're already using IPsec, you will need SSL, a system which allows staff to easily access company networks remotely and securely. If you already have SSL, you should check whether it allows full network access, as some SSL systems don't do this. And, of course if you haven't got SSL in place, now is the time to install a system. Comparatively low-cost SSL systems are available from companies such as Barracuda Networks, Check Point and WatchGuard.

5. Check whether your phone system is capable of delivering remote switchboard capabilities for calls and conferencing, and test that capability. If it isn't, there are a range of solutions from companies such as Samsung that can integrate with your existing phone system to quickly and inexpensively upgrade its capability, so that remote users can continue to operate in a work environment.

In addition, there are hosted services that can provide central telephony facilities for remote users. Set-up for this can be rapid, but needs to be implemented before staff become home-based.

6. Ensure that setting up remote access doesn't compromise your business security. Simple password access is insecure and two factor authentication is much, much safer.

This typically involves a PIN number and a changing password generated by a hardware token or from the system onto your mobile phone. Companies such as VASCO and CRYPTOCARD have a range of solutions in this area. They also provide hosted authentication solutions, which make administration and deployment even easier.

7. If business critical information is being accessed remotely, ensure that it is adequately protected. Encryption solutions are available that protect data in motion and stop it being downloaded on to USBs, if that is your policy. If downloading to USBs is allowed, make sure the data is encrypted. Solutions such as Check Point End Point Security can easily provide these facilities

8. Ensure that home PCs are secured. Consider an end point package, such as those from Kaspersky Lab, which protect against viruses and spyware on home machines accessing the network

9. Ensure that key suppliers have contingency plans in place, that you are happy with them and that you have access to key emergency numbers.

10. Ensure that you communicate your plans to all relevant staff well in advance.

ENDS

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

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 Times 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.