

Contributors

Lynda King Taylor
Business Continuity journalist

Rik Turner
Information Technology journalist

special report publishing

Publisher
Miles Allen
Editor
Andrew Baker
Design & Production
Benn Withers
Print & Distribution
The Telegraph Group Limited

www.specialreportpublishing.com

For more information about future reports distributed exclusively with the Daily Telegraph please contact Special Report Publishing on 020 7629 7080

Copyright Special Report Publishing ©

The latest online threats

Since 2003, the threat landscape has been dominated by crimeware, i.e. malicious code created to make money illegally. There have been few global epidemics and many more localised, targeted, small-scale attacks, with malicious code spammed directly to victims' machines. The number, and types, of Trojans (the weapon of choice for cyber criminals) have grown steadily: they account for around 70% of all malware. It's no surprise, therefore, that they consistently dominate the Kaspersky Lab top twenty. There are many types of Trojans, all designed to carry out a specific function: Backdoor Trojans (often with built-in keylogger), Trojan Proxies (for spam distribution or conducting DDoS attacks), Trojan Spies, etc. Many are geared towards identify theft: i.e. capturing logins, passwords, PINs and other personal information and using it to steal money. Unlike the malware of the 1990s, today's threats are less obvious (cyber criminals have a vested interest in our up-time), but much more insidious.

Source: Kaspersky Lab
For top 20 latest viruses go to www.viruslist.com/en/analysis?pubid=204791936

The enemy within

The threat of portable storage devices is growing all the time. But the diligent IT manager can find solutions.

The uncontrolled use of portable storage devices by employees is a very real threat to the security and stability of any business. Unfortunately, many businesses are unaware of, or ignore the threat until something actually happens.

According to research findings announced by GFI Software at InfoSecurity, 65% of 370 UK companies underestimate the security threat posed by devices such as USB sticks, PDAs and Blackberrys. Although 49% are concerned about data theft, 65% do not consider these devices to be a threat. At the same time, 79% have no clue what data is being transferred from the network to the device and vice versa. And here lies the biggest threat for network administrators. The uncontrolled use of portable storage devices coupled with data theft techniques such as 'pod slurping', can lead to major security breaches. And while data theft from the loss or theft of laptops is a growing concern for IT managers, there are even more serious threats closer to home than many realize – "the enemy within".

Portable storage devices are a major threat because companies have no record of what files are being transferred from the network to the device and vice-versa. An employee with a grudge against his employer can easily copy commercially sensitive information off the network or upload a virus that could cripple the system. While a few counter-measures that corporations

can adopt to prevent unauthorized portable device use exist, they are not the perfect solution. Banning portable storage devices on the corporate premises, the physical blocking of computer access ports, or using Windows Group Policies are common practices, yet they also restrict those who depend on these devices from doing their jobs effectively.

The only effective solution to counter portable device threats is to deploy a software solution that allows you to discriminate between legitimate and illegitimate use of devices, in compliance with the custom security policies set up by the corporation. What administrators must also realize is that managing risk is always more cost effective than having to react to breaches or incidents. In an ever-growing networked environment where risk is becoming a major concern, administrators have to be ahead of threats and not passively reacting to incidents. Apart from immediate financial repercussions such as business loss, there is the enduring stain of embarrassment and loss of credibility. For a company that prides itself upon protecting its customers' data, a single breach could have irreversible repercussions. All it takes to prevent this happening is a small investment in a comprehensive endpoint security solution – such as GFI EndPointSecurity! ▶

Andre Muscat, Director, Network Security Division GFI Software.
www.gfi.com



Q What is Information Availability and why should I care?

A Keith Tilley
UK MD and Snr Vice President Europe, SunGard Availability Services

Information Availability is a holistic approach towards ensuring business availability, which identifies an organisation's mission critical information and ensures its underlying infrastructure meets its business requirements, in all situations and gives a considerable ROI. Information is the lifeblood of an organisation and businesses cannot function without access to their data. Organisations that experience downtime do not simply lose revenue; they lose customers directly to their competitors, not just today but forever.

Information Availability goes further than simply sustaining IT systems. It helps organisations understand information flow throughout its organisation to staff, customers and suppliers. Therefore, understanding Information Availability helps organisations streamline business processes and actually is an investment that can provide significant returns. Given its importance to continued operations of an organisation, Information Availability goes beyond the remit of the CIO or IT director, all the way to the Board. Many CEOs are now recognising the importance of Information Availability by bringing together the separate disciplines of risk management and business continuity, an acknowledgement that Information Availability concerns more than simply IT but actually impacts upon every area of an organisation.

Q In your opinion, where is the 'big challenge' in achieving UK business continuity?

A Mike Osborne
Managing Director of ICM Business Continuity Services

Government and industry need to focus on the risk that exists within the supply chain and in particular the SME businesses that are such a feature of the UK economy. The problem being that business continuity planning is seen by many as a black art: complicated and expensive. As a consequence many SMEs simply bury their heads in the sand, rather than grasp the concept and implement a solution. The result is that SMEs who, by their very size, do not possess the inherent resilience achieved as a consequence of both size and diversity are actually left exposed. Also, as many of them do not fall under the same regulatory or corporate governance, the lack of a solution can be allowed to continue unchecked. Via public sector preparedness and commercial regulation such as the Civil Contingencies Act, Government has set out to ensure the UK has both a resilient economy and resilient communities. Until both educational and financial support is provided to SMEs at a local level, then these aims will not be achieved. By the time the payout comes, no customers and no staff means that the business is in start-up mode again. Hence the much quoted statistic that 80% of businesses that have a disaster without a business continuity plan in place go out of business within 18 months. It would not be unreasonable to assume that all had insurance.

Q Should the flu pandemic take hold in the UK is there secure, reliable technology available that meets the requirements of financial institutions, enabling employees to work seamlessly from home?

A Graham Chick
Chief Executive, GemaTech

According to the government's chief medical officer, it is a matter of when, not if, a flu pandemic develops over the next few years. Financial institutions will have to implement flexible working strategies to ensure 'business as usual'. In their recent six week exercise into dealing with a 'flu pandemic crisis' the FSA found that whilst a significant number of participants decided to adopt flexible working, home working was not extensively utilised. This is a view I totally concur with. Should a flu pandemic arise, employees will invariably decide where they feel safest working, if they feel fit to work at all. To embrace flexible working, financial institutions not only need to be able to re-route incoming calls to remote workers, but also voice record all calls, including outbound calls made by remote workers. Specialist telecoms vendors can now seamlessly recover 100% of incoming calls to office based individual geographical DDIs by intelligently re-routing them to any number, anywhere in the world. Additionally, both the re-routed inbound calls to remote employees and any subsequent outbound calls they make can be recorded – all using reliable, tried and tested, traditional fixed line telephony. However, a word of warning for those who believe VoIP will deliver an acceptable service during a pandemic – forget it! Whilst the technology itself is evolving, becoming more resilient and more secure, the Broadband connectivity over which it travels is simply not up to the job, resulting in unacceptable delays during conversations.

Healthcare Connections

Businesses not prepared

Pandemic influenza could be a global killer:

- Global economic losses could be \$2 - 4.4 trillion
Source: World Bank and Lowry Institute, Australia 2006
- Government anti-viral stockpiles are limited (20-25% is likely not to be enough to mitigate impact)
Source: Roche, Tamiflu Media Briefing 2007
- Workplace planning is only truly effective if you include the right medication and make sure you are delivering in the best way
Source: Alison Brown, Healthcare Connections Ltd CEO, 2007

If a pandemic influenza hits it could spell disaster for your business, we can help you prepare.

As leading providers in pandemic preparedness we are working with many large corporations to create the right occupational health solutions for the **workforce**, the **supply chain** and their **family members**.

Our unique service offering was created by our own need for an effective health scheme and since then we have stockpiled in excess of 700,000 courses of medication for our clients.

Speak to the pandemic professionals:
call: 08456 773005 **fax:** 08456 773006
click: www.hccpandemic.com

we help you care

All Rights Reserved

First, run your exercise... then write the plan?

It's traditional to get things the wrong way round in Business Continuity. First, you have a crisis, then everyone starts talking about a crisis plan – and wants to know why you didn't have one before. At Steelhenge, we specialise in looking at things a different way. As the leaders in exercise planning, we can 'stage' your crisis, to help you validate your plan – before it actually happens. **Now that is the right way round.**

steelhenge

the uk's experts in
organisational resilience

0845 094 2117
www.steelhenge.co.uk