



## Case Communications June Newsletter

Greetings,

Welcome to the Case Communications June Newsletter

This month we look at security issues and a new initiative where prisoners are to be given IT Skill Training. Sadly Westell who made a number of voice gateways have ceased operating in the UK.

.....

### **SOCA releases e-crime increase warning**

In a report from SOCA it has been revealed that there is a market evolution geared at trading and exploiting data. The report said there are an increasing amount of gangs, usually containing an average of 30 specialists focused on areas ranging from phishing to data trading.

[More](#)

.....

### **IT skills to be offered to criminals**

Prisoners will be given training in networking and cable installation to help fill the skills gap.

According to Cisco, one of the co-founders of the initiative, demand for data and network cabling experts outstrips supply by 20 per cent in the UK – equivalent to 61,000 jobs.

[More](#)

.....

### **British Hacker fighting extradition to US**

Self confessed British hacker Gary Mc Kinnon, who is fighting extradition to the US, broke into more than 73,000 US government computers, including those of the US Army, Navy and Nasa, and deleted critical data, the House of Lords heard today

[More](#)

.....

### **The IT Industry is responsible for 2% of the Global Co2 emissions and its getting worse.**

Last month analyst group Gartner said that the IT industry is responsible for two percent of global CO2 emissions, the same amount as the airline industry

### **Case Communications June Newsletter**

#### **In this Issue:**

- [SOCA releases e-crime increase warning](#)
- [IT skills to be offered to criminals](#)
- [British Hacker fighting extradition to US](#)
- [The IT Industry is responsible for 2% of the Global Co2 emissions and its getting worse.](#)
- [WiMax is likened to Wi Fi on steroids](#)
- [A potential new way to prevent Internet worms.](#)
- [WESTELL TECHNOLOGIES SHUTS DOWN ITS UK OPERATION](#)
- [INTERNET OVERHAUL APPROVED](#)
- [AVG anti-virus software generating excess web traffic](#)

[More](#)

---

### WiMax is likened to Wi Fi on steroids

Wimax, often likened to Wi-Fi on steroids, has two advantages over LTE: it's available today, and is free from the hefty royalty charges required for 3G (third-generation) mobile devices and equipment. Mobile operators may be counting on LTE.

[More](#)

---

### A potential new way to prevent Internet worms.

The spread of Internet worms could be stopped early on by using a new method to watch computers for the behavior exhibited by infected hosts, according to research recently published in *IEEE Transactions on Dependable and Secure Computing*.

[More](#)

---

### WESTELL TECHNOLOGIES SHUTS DOWN ITS UK OPERATION

Westell Technologies has closed its UK operation and according to early reports withdrawn support contracts in the UK for its range of LiQ converter products. Last month the US parent company reported a significant loss in its fourth quarter and fiscal year 2008, ending March 31, 2008.

[More](#)

---

### INTERNET OVERHAUL APPROVED

A new era in the way websites are named was ushered in when the governing body for internet domain names announced a massive liberalisation on 26th June 2008.

[More](#)

---

### AVG anti-virus software generating excess web traffic

If you are using AVG as your anti virus system, you have probably noticed little green (or sometimes red) marks beside search results on Google. These appear to be handy, because it gives an indication that the site you might visit is free of any malware. However, there is a down side to this.

[More](#)

---

#### **Subscribe FREE**

Sign-up for the newsletter  
If you would like to subscribe or un-subscribe to this magazine then click on the link below.

[Subscribe/Unsubscribe](#)

#### **Feedback**

##### **Tell us your thoughts**

If you have something interesting to say or comments about the ezine, please feel free to email them to us:

[Email feedback/Enquiry](#)



## Case Communications June Newsletter

### SOCA releases e-crime increase warning

.....

In a report from SOCA it has been revealed that there is a market evolution geared at trading and exploiting data. The report said there are an increasing amount of gangs, usually containing an average of 30 specialists focused on areas ranging from phishing to data trading.

The gangs operate by stealing information through techniques such as phishing and key logging using malware sent via email. The stolen data is then used by the thieves for fraudulent purposes or sold to other cyber criminals over the web.

E-criminals are using increasingly diverse web-based technologies to access and exploit victims and conceal their activities, the report said.

"Each group will typically have an inner circle of more technically advanced and/or experienced members who control access to the attack tools and are responsible for dividing up the work," it said.

Soca said the tactics used by the criminals are also constantly updated to keep ahead of protection offered by software vendors.

### Case Communications June Newsletter

#### In this Issue:

- [SOCA releases e-crime increase warning](#)
- [IT skills to be offered to criminals](#)
- [British Hacker fighting extradition to US](#)
- [The IT Industry is responsible for 2% of the Global Co2 emissions and its getting worse.](#)
- [WiMax is likened to Wi Fi on steroids](#)
- [A potential new way to prevent Internet worms.](#)
- [WESTELL TECHNOLOGIES SHUTS DOWN ITS UK OPERATION](#)
- [INTERNET OVERHAUL APPROVED](#)
- [AVG Santi-Virus software generating excess web traffic](#)





## Case Communications June Newsletter

### IT skills to be offered to criminals

.....

All criminals who complete the training will then be given an interview with BeOnsite, a not-for-profit training company owned by scheme co-founder Bovis Lend Lease. Successful candidates will be offered employment once they are released from prison.

Speaking at the launch of the vocational learning academy, responsible for the management of the initiative, prisons minister David Hanson said: "Reforming offenders so they can positively contribute to society as well as being punished for their crimes by denying them their freedom is what prison is about and what both communities and businesses demand. "Initiatives like the academy at HMP Wandsworth are an inspiring example of how we can use the expertise and knowledge of both the private and public sectors to improve employment opportunities for prisoners on release so they don't return to a life of offending."

The academy is a public private partnership developed by Working Ventures UK and the London Employer Accord in partnership with Cisco, Panduit, Bovis Lend Lease and HM Prison Service (HMPS). It will be delivered by Cisco and HMPS Regime Services.

### Case Communications June Newsletter

#### In this Issue:

- [SOCA releases e-crime increase warning](#)
- [IT skills to be offered to criminals](#)
- [British Hacker fighting extradition to US](#)
- [The IT Industry is responsible for 2% of the Global Co2 emissions and its getting worse.](#)
- [WiMax is likened to Wi Fi on steroids](#)
- [A potential new way to prevent Internet worms.](#)
- [WESTELL TECHNOLOGIES SHUTS DOWN ITS UK OPERATION](#)
- [INTERNET OVERHAUL APPROVED](#)
- [AVG Santi-Virus software generating excess web traffic](#)





## Case Communications June Newsletter

### British hacker fighting extradition to US

.....

Self confessed British hacker Gary Mc Kinnon, who is fighting extradition to the US, broke into more than 73,000 US government computers, including those of the US Army, Navy and Nasa, and deleted critical data, the House of Lords heard today

The charges emerged at McKinnon's appeal against extradition, heard by five British Law Lords in parliament this morning.

Papers before the Lords showed that investigators traced the breaches to McKinnon's computer, which was seized by British police. McKinnon admitted responsibility in an interview and accepted a caution.

Mc Kinnon said that he started hacking in 1999, looking for evidence of extraterrestrial beings and technology, which he believed the US government was hiding.

Police from the former National Hi-Tech Crime Unit arrested McKinnon in 2002.

McKinnon's appeal is based on his contention that the terms of a plea bargain offered to him by US prosecutors were coercive and put "unconscionable pressure" on him to give up his right to an extradition hearing.

The terms offered a choice of "coming quietly" or "having the book thrown at him", said Edward Fitzgerald, acting for Liberty, the human rights watchdog.

The terms were to volunteer to appear and plead guilty in a US court. In return, the prosecution would ask that McKinnon serve between 37 and 46 months in a low-security prison. The would offer him repatriation to the UK after 18 months, and probable release under license after serving half his sentence.

If he did not waive his rights, the US would press for a sentence of at least eight to 10 years in a high-security prison, with no repatriation.

### Case Communications June Newsletter

#### In this Issue:

[SOCA releases e-crime increase warning](#)  
[IT skills to be offered to criminals](#)  
[British Hacker fighting extradition to US](#)  
[The IT Industry is responsible for 2% of the Global Co2 emissions and its getting worse.](#)  
[WiMax is likened to Wi Fi on steroids](#)  
[A potential new way to prevent Internet worms.](#)  
[WESTELL TECHNOLOGIES SHUTS DOWN ITS UK OPERATION](#)  
[INTERNET OVERHAUL APPROVED](#)  
[AVG Santi-Virus software generating excess web traffic](#)

David Pannick QC told the lords the offer was made in a letter from Ed Gibson, then special attaché to the embassy in London and currently special legal adviser to Microsoft in the UK, on behalf of the US Attorneys Office.

In questions to counsel, the Lords were concerned whether Gibson's offer was merely setting out "the facts of life" as Baroness Hale, put it, or whether the prosecutors exaggerated their influence over repatriation procedures, as these are handled by a different section in the US justice department.

The Lords will hear arguments for the US government later this afternoon. They are expected to take two weeks to deliver their judgement.





## Case Communications June Newsletter

### **The IT Industry is responsible for 2% of the Global Co2 emissions and its getting worse.**

.....

The Morse survey, carried out by Vanson Bourne a couple of months ago, questioned over 100 IT Directors in the United Kingdom. It found that 76 percent of companies have set no targets for reducing the IT department's power usage, and that 63 percent of organisations claim to have a strategy to become more environmentally friendly.

Yet according to Morse, ignoring the IT department's power use suggests that many of these green strategies are little more than hot air.

Sixty two percent of organisations said that green IT was not a top priority and only 24 percent of organisations said they are working towards a set energy reduction target.

"This survey is a realistic snapshot of the IT manager," said Tim Turquand, consultant at Morse. "IT managers don't have an idea of how much their data centre is costing them."

"The survey clearly shows that IT departments do not know about their electricity bills," he added. "Green IT strategies are just not aligned to any business strategy at the moment. For example, most businesses have recycle bins for printer cartridges and or paper, but they forget about their 20,000 square foot data centre which is the biggest pollutant."

"If they don't know what their power consumption is, how can they expect to reduce it?" Turquand asked.

The problem, according to Turquand, is that currently the electricity bill of a company is traditionally paid by the central facilities or operations group, which gives IT departments very little visibility into how much power their consume.

"Facilities departments normally pay electricity bills as part of their job," said Turquand, "but IT is going to have start realising what their costs are, and the amount of carbon being produced."

"Attitudes have to change," he said. "There can be no more heads in the sand, and IT managers have to stop paying lip service to green IT and do something about it."

### **Case Communications June Newsletter**

#### **In this Issue:**

[SOCA releases e-crime](#)

[increase warning](#)

[IT skills to be offered to criminals](#)

[British Hacker fighting](#)

[extradition to US](#)

[The IT Industry is](#)

[responsible for 2% of the](#)

[Global Co2 emissions and](#)

[its getting worse.](#)

[WiMax is likened to Wi Fi](#)

[on steroids](#)

[A potential new way to](#)

[prevent Internet worms.](#)

[WESTELL TECHNOLOGIES](#)

[SHUTS DOWN ITS UK](#)

[OPERATION](#)

[INTERNET OVERHAUL](#)

[APPROVED](#)

[AVG Santi-Virus software](#)

[generating excess web](#)

[traffic](#)

Turquand pointed out that IT managers need to be aware of the energy consumption of their entire IT infrastructure, and not just the data centre or server room. "He or she should gain visibility of the power being produced from all assets," he said.

Another problem comes from the fact that IT departments are often not the one making equipment purchases. "Purchases are normally made by projects and not IT departments," said Turquand. "The project is given a budget, and they go out buy the equipment they need, and then when the project is finished, they move to different project or even a different company."

"The IT department is left to pick up the pieces from projects, or more often or not they do not pick up the pieces, they just put their heads in the ground and ignore it," he said.

"That has to change, and IT managers need to get a grip on what is being brought and how power does it consumes." Turquand believes that control must be given back to the IT department so that it can investigate strategies which help the business to reduce its energy consumption. These could include using virtualisation to increase utilisation rates and turning the allocation of storage and server resources into a service offered to the business so that fewer devices are needed and they become easier to manage.

Turquand advocates that departments should be billed for their energy consumption in order to increase accountability. He accepts this is going to be difficult. "There needs to be culture change, and we need to drastically change how we work."

The Morse survey found that only 12 percent charge the IT department for the power used.

Another finding was that over half (53 percent) of the UK businesses surveyed, said that making their data centres greener would be too expensive.





## Case Communications June Newsletter

### WiMax is likened to Wi Fi on steroids

Mobile operators may be counting on LTE (Long-Term Evolution) technology to offer high-speed mobile data access in coming years, but WiMax services will arrive first, promising to shake up the wireless data market in the process.

WiMax offers high-speed Internet access over a wide area and comes in two versions, a fixed-wireless version and another for mobile. The technology, often likened to Wi-Fi on steroids, has two advantages over LTE: it's available today and is free from the hefty royalty charges required for 3G (third-generation) mobile devices and equipment. By comparison, LTE has another two to three years to go before it can be deployed and, because the radio uplink uses CDMA (Code Division Multiple Access), device makers will have to pay substantial royalties to Qualcomm.

"They charge a 5 percent royalty on the handset or devices, and that's on the retail side...Behind the door, they're charging anywhere from 15 to 30 percent on the chipsets," said Bill Rojas, director of communications research at IDC Asia-Pacific, adding that WiMax backers have agreed to a much lower royalty for using the technology.

While lower royalties and the earlier rollout of commercial services gives WiMax an edge over LTE, there are still obstacles that must be overcome before the technology can be widely deployed.

The immediate challenge WiMax faces is product interoperability. WiMax Forum, the industry group that oversees the certification process, has only approved the interoperability of a handful of WiMax products designed to operate in the 2.3GHz spectrum. This frequency is used in South Korea while most other markets expect to use the 2.5GHz to 3.5GHz spectrum bands.

In addition, the certified products are based on the Wave 1 version of WiMax, which does not support MIMO (Multiple-In, Multiple-Out) antenna technology, or other advanced features found in the Wave 2 version of WiMax that operators, including those in Korea, plan to deploy. As a result, the certified products announced by WiMax Forum are largely irrelevant to wider adoption of the technology.

WiMax Forum will not certify the interoperability of Wave 2 WiMax

### Case Communications June Newsletter

#### In this Issue:

[SOCA releases e-crime increase warning](#)  
[IT skills to be offered to criminals](#)  
[British Hacker fighting extradition to US](#)  
[The IT Industry is responsible for 2% of the Global Co2 emissions and its getting worse.](#)  
[WiMax is likened to Wi Fi on steroids](#)  
[A potential new way to prevent Internet worms.](#)  
[WESTELL TECHNOLOGIES SHUTS DOWN ITS UK OPERATION](#)  
[INTERNET OVERHAUL APPROVED](#)  
[AVG Santi-Virus software generating excess web traffic](#)

products until the second half of this year, at the earliest - nearly a year behind schedule and after Intel releases the first Centrino 2 products in June. That timing suggests that the number of Centrino 2 laptops that ship with WiMax this year will be relatively low, but nevertheless widespread availability of the technology is not far off.

Intel sees 2008 as the year when WiMax will start to appear in computers, such as a WiMax-equipped Asustek Computer Eee PC that Sriram Viswanathan, vice president of Intel Capital, the chip maker's investment arm, and general manager of the company's WiMax Program Office, showed off in Singapore.

"We have a variety of these devices. Not all of them will be launched on the first day, but the fact is during the second half (of 2008) you will see a plethora of devices," Viswanathan said in a recent interview.





## Case Communications June Newsletter

### **A potential new way to prevent Internet worms.**

.....

Although other methods exist to protect against worms, the new strategy is designed to minimize interference with users' normal work patterns, says Ness Shroff, a professor in the electrical-engineering department at Ohio State University, who was involved in the research. The researchers envision the technique being used in corporate networks, where it could identify computers that need to be quarantined and checked for infection.

Internet worms can be enlisted to launch denial-of-service attacks, which flood a website so that legitimate users can't access it, or install back doors that can be used to create botnets. Large numbers of infected computers could significantly slow Internet traffic, even if the worms do nothing more than spread.

The Purdue University and Ohio State method of preventing worms from spreading works primarily for a class of worms that scans the Internet randomly in search of vulnerable host machines to infect. One such worm was Code Red, which infected more than 359,000 computers in less than 14 hours in 2001, and ultimately caused an estimated \$2.6 billion in damages. Although this type of worm has been around for some time, Kurt Rohloff, a scientist in the distributed systems technology group at BBN Technologies says that it is still dangerous. These "are a very simple class of worms that's very easy to develop and program, but at the same time, they're not as easy to contain," he says. "If we could understand these fairly simple but still problematic worms, we could hopefully address the more so-called devious worms."

The researchers base their strategy on a new model that they designed for how worms spread. Many existing models are based on an analogy to the spread of epidemics, Shroff says, but they are more accurate at later stages of an infection. The researchers' model was particularly designed for accuracy in the early stages of infection, and it revealed that the key to whether or not a worm can spread successfully is the total number of times that an infected host scans the Internet in attempts to find new hosts to infect.

While other methods of containing worms have focused on monitoring computers for changes in the rate at which they scan the Internet from moment to moment, Shroff says that this can interfere with users' daily activities. "Scan rates fluctuate a lot, so

### **Case Communications June Newsletter**

#### **In this Issue:**

- [SOCA releases e-crime increase warning](#)
- [IT skills to be offered to criminals](#)
- [British Hacker fighting extradition to US](#)
- [The IT Industry is responsible for 2% of the Global Co2 emissions and its getting worse.](#)
- [WiMax is likened to Wi Fi on steroids](#)
- [A potential new way to prevent Internet worms.](#)
- [WESTELL TECHNOLOGIES SHUTS DOWN ITS UK OPERATION](#)
- [INTERNET OVERHAUL APPROVED](#)
- [AVG Santi-Virus software generating excess web traffic](#)

if you go online, you may scan a lot of times during a very short period of time, and then not scan at all," he says. "We felt that the scan rate was too restrictive and could interfere with the normal operation of the Network." By monitoring the volume of scans over a longer period of time, he says, it's possible to contain worms while keeping the threshold too high for ordinary users to raise alarms. Software could monitor the number of scans each computer on a network sends and quarantine any computers that exceed that number. Shroff hopes that changing the criteria for suspecting infection in this way will reduce the likelihood that legitimate scans of the Internet would be flagged as worm activity.

"In a sense, what we're doing is taking advantage of the fact that this worm is trying a lot of things and missing many times, and each time it misses, it's giving out some information," Shroff says. Although the system is designed for dealing with scanning worms that seek vulnerable hosts at random, the researchers have also adapted it for worms that target their attacks at specific local networks.

Shroff believes that the system could best be deployed on corporate networks, particularly in situations in which extra computers are available that could cover a workload while possibly infected computers are examined. It might not work as well for small businesses or on home networks, because taking a computer offline could be too large of a disruption for users, he says.

Rohloff says that he could imagine such a system being effective, but he cautions, "The bias, of course, would be that it would protect local networks from infections that are already present in the network. It wouldn't do as much for protecting networks from infections that come from the outside." He adds that while the researchers' model and initial simulations look good, he would be curious to see a more thorough analysis of how often the system suspects a computer of being infected with a worm when no worm is actually present.

The Purdue and Ohio State researchers suggest that future work could search for ways to adapt their tools for ever more targeted worms. Shroff says that while he and his colleagues are now concentrating on stopping worms at the level of host computers, another possible direction could be to make software that would allow routers to watch for suspicious traffic patterns. While such an approach could allow a relatively large number of computers to be monitored from a single point, it would also require significant changes to how routers operate. While they currently keep track of only the destination of Internet traffic, they would have to begin keeping track of its source as well.



## Case Communications June Newsletter

### WESTELL TECHNOLOGIES SHUTS DOWN ITS UK OPERATION

.....

Total revenue for the fourth quarter was \$44.7 million, a decrease from the \$60.0 million reported in the prior year period. Net loss during the period was \$61.5 million, or \$0.87 per diluted share, compared to net income of \$0.6 million, or \$0.01 per diluted share in the same period last year. Commenting on the news, Phil Sawyer, Managing Director of DXP, said: "There will be a huge hole in the market for DPNSS/Qsig/IP conversion product.

Westell was approved by Avaya, Cisco, Gamma and many others." In October last year Westell was selected for Gold membership in the Avaya DeveloperConnection program. Gold-level members develop products that are particularly complementary to Avaya's portfolio. The following month Westell's InterChange iQ (IiQ) 3000, a DPNSS to IP converter, passed Cisco's Interoperability Verification Testing (IVT) methodology. In January this year Reuters reported that Westell Technologies would axe 58 jobs, saying that the job cuts would result in annual cost savings of \$6 million.

According to Datamonitor, Westell Technologies recorded revenues of \$260.1 million during the fiscal year ended March 2007, a decrease of 8.2% compared to 2006. The operating profit of the company was \$11.6 million during fiscal year 2007, a decrease of 47.8% compared to 2006. The net profit was \$8.7 million in fiscal year 2007, a decrease of 32.3% compared to 2006.

The Illinois-based company has 898 employees and a turnover of \$260m.

### Case Communications June Newsletter

- In this Issue:**
- [SOCA releases e-crime increase warning](#)
  - [IT skills to be offered to criminals](#)
  - [British Hacker fighting extradition to US](#)
  - [The IT Industry is responsible for 2% of the Global Co2 emissions and its getting worse.](#)
  - [WiMax is likened to Wi Fi on steroids](#)
  - [A potential new way to prevent Internet worms.](#)
  - [WESTELL TECHNOLOGIES SHUTS DOWN ITS UK OPERATION](#)
  - [INTERNET OVERHAUL APPROVED](#)
  - [AVG Santi-Virus software generating excess web traffic](#)





## Case Communications June Newsletter

### INTERNET OVERHAUL APPROVED

.....

The body that oversees the internet's structure has approved a "land grab" for new web addresses that will allow people to apply for any top-level domain name — but it will cost them at least \$100,000 to do so.

Scripts other than Latin — for example Chinese, Japanese, Arabic and Cyrillic — will also be allowed, opening up the internet to many millions in the Middle East and Asia.

Until now top-level domain names— the .com or .uk at the end of a web address — have been restricted by the Internet Corporation for Assigned Names and Numbers (Icann), the international not-for-profit body set up in 1998 to to oversee the structure of the internet and maintain its stability. Icann regulates the way web addresses are assigned to ensure that computers can communicate with each other.

The free-for-all agreed in Paris earlier in June this year is seen as a great leap forward akin to the privatisation of telecommunications in the Thatcher era. Icann is not being forced to act because of there are not enough name options, but because it wants to open up the system to increase consumer choice.

Most web addresses in Britain have the suffix .uk. The most popular top level domain name in the world is .com and there are about another 20 possibilities such as .org or .net. Every country has a country code domain name such as .de (Germany) and .fr (France). Now the possibilities are endless and the new names could range from place names to commodities.

Paul Twomey, the chief executive of Icann, said: "It's a massive increase in the real estate of the internet. It will allow groups, communities and businesses to express their identities online."

Experts are divided on how many new domain names will come into existence. Sceptics argue that some of the more recent additions such as .name introduced in 2000 have failed to take off. But several categories of suffix, such as those relating to cities, are sure to prove popular. It is easy to imagine addresses ending in .london or .paris. City authorities could apply for use of the domain name and then group services and companies under

### Case Communications June Newsletter

#### In this Issue:

[SOCA releases e-crime increase warning](#)  
[IT skills to be offered to criminals](#)  
[British Hacker fighting extradition to US](#)  
[The IT Industry is responsible for 2% of the Global Co2 emissions and its getting worse.](#)  
[WiMax is likened to Wi Fi on steroids](#)  
[A potential new way to prevent Internet worms.](#)  
[WESTELL TECHNOLOGIES SHUTS DOWN ITS UK OPERATION](#)  
[INTERNET OVERHAUL APPROVED](#)  
[AVG Santi-Virus software generating excess web traffic](#)

the .london umbrella.

Another top-level domain name likely to attract attention is .web. Experts also predicted that regional names such as .scot for Scotland would be snapped up.

It was not clear last night how many big name companies would want to change their well-established web addresses to take advantage of the new opportunities. Some were asking whether, for instance, Microsoft would want to stop residing at [www.microsoft.com](http://www.microsoft.com).

Dr Twomey said he did not expect there to be thousands of applicants, mostly because of the cost, but added: "We hope there will be a broad range of applications. The key principle is that it is open to all to apply."

But there is the potential for large sums to be won — and lost — amid fears that "cybersquatters" would cash in on the liberalisation to register hundreds of new web addresses created within each new suffix, and seek to sell them on to companies or organisations that want to claim them.

Big companies already spend millions of pounds buying up web addresses similar to their own to protect their brands. At the other end of the scale, those with money to burn might register their own personal domains.

Would-be applicants are advised that the process is different from registering a regular website. Top-level domains require significant equipment — including servers, routers, and databases — to run. "These new names are not going to be for mom-and-pop businesses," Dr Twomey said.

Icann said it would begin taking applications for new domains in April, with the first expected to be in operation by the end of 2009. The system is open to anyone, but applicants have to show they have a "business plan and technical capacity". Disputed domains will be auctioned to the highest bidder, though in some cases intellectual property law may help a company to secure a name. Icann also reserves the right to reject a domain on "morality or public order" grounds, in which case the matter may go to an international arbitration committee.

One area of dispute will be domain names useful to the sex industry. Icann has in the past rejected the .xxx domain name on the grounds that it would be forced to become a content regulator. Whether .sex or .hot may be now allowed remains unclear.

Asked why registering a domain was so expensive, Dr Twomey said that the fees would cover the \$10 million Icann is having to spend developing the domain name system to accommodate new

domains and languages.

The largest top-level domain is .com, with 71 million addresses, followed by .de — the country code for Germany — with 11.2 million and .net, with 10.6 million. The fastest-growing is .cn, for China, which has 10.5 million addresses and grew by 31 per cent in the past three months alone.

But most commentators believe the dominance of the .com suffix will make it hard for new domain names to establish themselves. As one blogger put it: "Adding more skimmed milk to the mix will not stop the cream from rising, and that cream is .com."

Dr Twomey did not expect there to be thousands of applicants, mostly because of the cost, but he said: "We hope there will be a broad range of applications.

They key principle is that it is open to all to apply." He did, however, expect some vanity applications. Countries that do not use Latin script were very keen to start using their own domain names, he said. Russia has already requested to use the Cyrillic script for the Russian Federation suffix. Such requests will be fast-tracked. But it may take years to establish a full list of country code domain names in local scripts.

Story from Timesonline 27th June 2008





Case Communications June Newsletter

**AVG anti-virus software generating excess web traffic**



**Anti virus ups Internet traffic**

If you are using AVG as your anti virus system, you have probably noticed little green (or sometimes red) marks beside search results on Google. These appear to be handy, because it gives an indication that the site you might visit is free of any malware.

However, there is a down side to this. In order to make this assessment, AVG visits every site shown on the results page to check it out. As a result, internet traffic increases and you might suddenly find that you are getting many more visitors to your site than before. Except, of course, these are not real visitors. I

f you are paying for bandwidth on your web site, you could then be out of pocket. What can you do about it? The simple answer is nothing. AVG are aware this could be an issue and looking at their system. However you do at least have the satisfaction of knowing that your pages have appeared in someone's search result.

**Case Communications June Newsletter**

- In this Issue:**
- [SOCA releases e-crime increase warning](#)
  - [IT skills to be offered to criminals](#)
  - [British Hacker fighting extradition to US](#)
  - [The IT Industry is responsible for 2% of the Global Co2 emissions and its getting worse.](#)
  - [WiMax is likened to Wi Fi on steroids](#)
  - [A potential new way to prevent Internet worms.](#)
  - [WESTELL TECHNOLOGIES SHUTS DOWN ITS UK OPERATION](#)
  - [INTERNET OVERHAUL APPROVED](#)
  - [AVG anti-virus software generating excess web traffic](#)

