

Data control and management lacking in virtualisation technology 10

Phishers using financial crisis for e-mail scams 12

Intel says slowdown won't harm tech development 14

Better storage management key to success 16

Green IT still a priority says Gartner survey 17

November 2008

ComputerScope

DEFINING TECHNOLOGY FOR BUSINESS

Report says that CFOs are more concerned with tech value than cost

IT value challenge



Ciaran Kelly, Terry Retter and Pat Kelleher of PwC, with Niall Barry, Department of Social and Family Affairs, at the launch of a report indicating that a large number of CFOs in Ireland are unconvinced of the value of IT

IRISH chief financial officers (CFO) are more concerned that IT is not producing real value for the business than they are with the cost of the technology. That is one of the core findings of a new survey from

PricewaterhouseCoopers (PwC) entitled "IT Technology Value".

A top concern cited by CFOs in the survey was that IT was not reactive enough to the needs of business. Other concerns were that it was

"unclear as to what contribution IT makes to the bottom line in terms of reducing costs or increasing revenues".

Of the participating CFOs, 43% felt that IT had not been a significant factor in reducing

costs in the previous year, while over two thirds (68%) of CFOs stated that recent IT investments played no part in terms of increasing revenues. The poor perception of IT by CFOs seemed compounded by another finding from the survey that, while 86% of organisations indicated that a business case was required for significant IT investment, only half went on to assess whether the stated benefits were achieved.

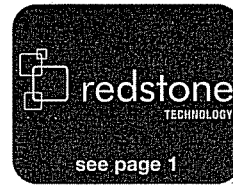
"Given the current challenging operating environment, it is even more critical for business to get the best value from its IT function and to use it to control costs, reduce complexity and enhance revenue where feasible.

"The two key areas needed to address the perception of a lack of value for money among CFOs are to ensure that IT strategic plans are clearly aligned to current business objectives and to

formally measure that IT investments deliver the expected benefits to the business," said Ciarán Kelly, partner, Advisory, Performance Improvement, PwC.

Pat Kelleher, director, Advisory, Performance Improvement, PwC suggested that there was a strong correlation between those organisations where IT is represented by a person at the highest level and better perceptions of IT value. In many Irish organisations the

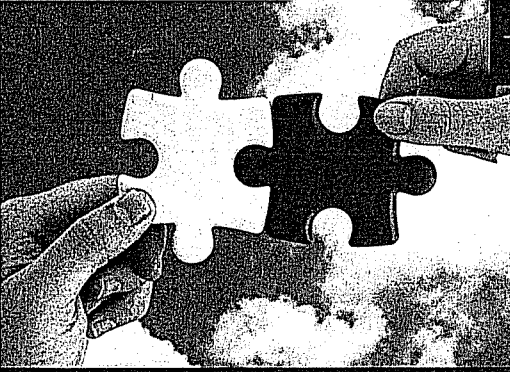
Continued on page 14 >



OFFICE CIRCULATION LIST

Read ComputerScope and pass on

- 1
- 2
- 3
- 4





TRUST TOPSEC FOR ALL YOUR SYMANTEC NEEDS

Topsec are Symantec's Strategic Security Partner in Ireland.

Topsec Technology and Symantec, the perfect fit for all your Security, Availability, Compliance and Performance requirements.

Topsec Engineers are fully certified to carry out Symantec product deployments and upgrades, as well as providing first rate telephone and email support for all our customers.

The IT Security and Communications Specialists

SOUTH COUNTY BUSINESS PARK, LEOPARDSTOWN ROAD, D.18. WWW.TOPSECTECHNOLOGY.IE TEL (01) 240 1000 FAX (01) 240 1001

"drive-by" scenario, where malware is downloaded from a website that the victim visited while surfing.

Deployment - Once the malware is delivered, the criminals strive for it to remain undetected for as long as possible. Malware writers use a number of technical strategies to maximise the lifespan of each piece of malware.

As a primary strategy, the malware writers depend on stealth not only for delivery, but also for survival. The less visible their malware is to antivirus early-warning radar systems and law enforcement agencies, the longer the malware can be used to provide access to infected machines and to harvest data. Common stealth techniques include rootkit technologies, suppression of system error messages, concealed increases in file size, many and varied packers, and suppression of antivirus warning messages.

Malware authors are also relying heavily on obfuscation techniques to avoid detection. Polymorphism is an obfuscation technique that was popular in the 1990's and then virtually disappeared. Today, malware writers have returned to polymorphism, but rarely do they attempt to morph code on victim machines. Instead, there is a distinct trend of server-side polymorphism - the re-

compiling of code on web servers with "do-nothing instructions" that vary over time, making it significantly more difficult to detect the new malware residing on the server. In fact, today, there are websites where bots re-compile malware as often as every five minutes.

Attacking security solutions

Another common technique used in malware is the sabotage of security programs, to prevent detection and extend shelf-life. Malware sabotage often occurs through the termination of security processes, deletion of code, or modification of the Windows hosts file to prevent antivirus program updates. In addition, malware often removes malicious code that is already installed, not for the user's benefit, but to ensure "ownership" and control of the victim machine exclusively for its own benefit. This active competition between malicious programs highlights the rich opportunities that are available to malware writers and the criminals that sponsor them.

The human factor

Ultimately, any security system is only as effective as the weakest link. In the case of online security, the weakest link is always the human

factor. As a result, social engineering techniques are a key element in malware dissemination processes used today. Techniques are often as simple as sending links purportedly from a friend via e-mail or instant messaging (IM). These links are crafted to look as if they lead to interesting online resources, but in reality, these links lead to infected web resources.

Today, e-mail messages can contain scripts that connect to infected websites without any user interaction at all. Even the educated, highly cautious person who never clicks on unsolicited links is in danger of infection by a "drive-by" download. The inclusion of current events in such campaigns occurs today with alarming speed, yielding astonishingly effective results. Phishing continues to be a major source of infection despite efforts by banks and other organisations that conduct online financial transactions to implement countermeasures. Too many innocent victims can still be convinced to explore interesting links and to accept official-looking communications as legitimate.

Final thoughts

In order to manage cybercrime, we need to develop and implement a number of protection strategies. Naturally, anti-malware software and risk

management strategies are vital at all levels.

However, I have stated this before and continue to believe that in addition to appropriate protection strategies, a successful anti-cybercrime strategy requires a community effort. There must be a functional Internet-Interpol and ongoing consumer education, much like that conducted to encourage seat belt usage. There should be legal measures requiring people to behave in a secure and legal fashion online, as well as legal consequences to support enforcement efforts. Just as with seat belts, unrelenting long-term education is needed to gain widespread acceptance for these measures.

While I don't believe we will ever abolish cybercrime any more than we have abolished crime in the physical world, I do believe that we can make the Internet a safer place. It will take more than the measures listed above, more than a single company, and more than a single government. We need a united community of individuals that each do their little bit for online security ... a community like this can and will succeed in winning against cybercrime most of the time. And most of the time is a goal worth striving for.

... Eugene Kaspersky, is founder and CEO of Kaspersky Labs

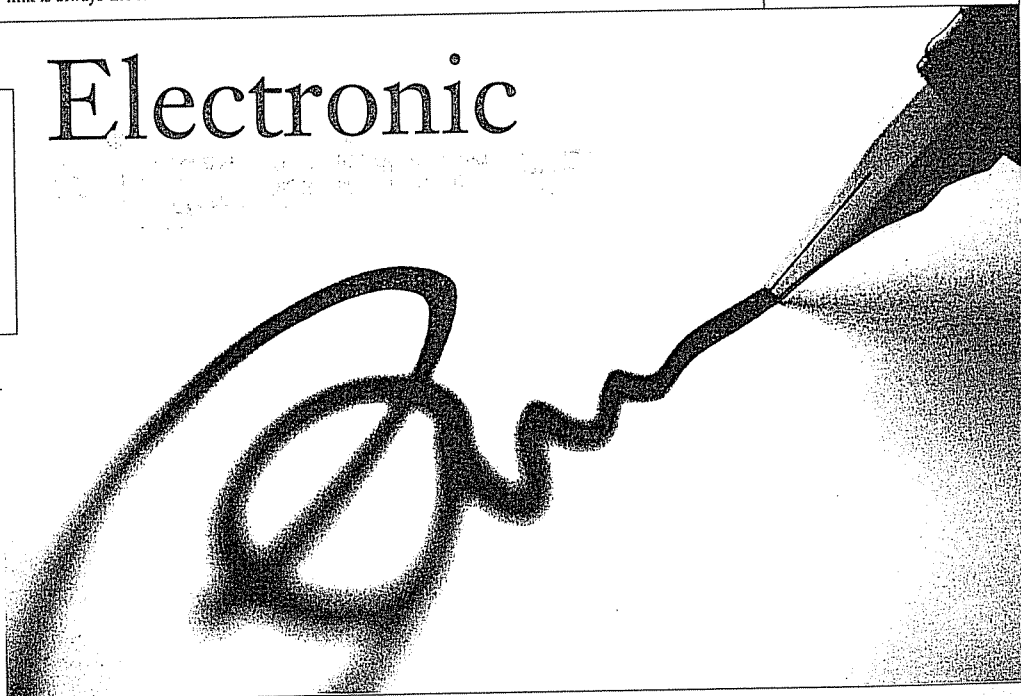
While I don't believe we will ever abolish cybercrime any more than we have abolished crime in the physical world, I do believe that we can make the Internet a safer place'

PAUL FOLEY makes the case for the next generation of your John Hancock

Electronic

According to a report issued by the UK Office of Fair Trading in a March 2008 report, internet retailing is growing at about 30% each year.

In the non virtual world, a paper based signature can provide evidence that data originated from the signer that the signer intended to

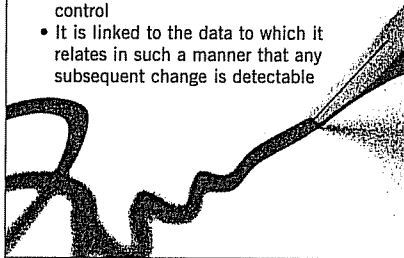


Signature types

Basic electronic signature – This means data in electronic form which are attached to or logically associated with other electronic data and which serve as a method of authentication. The term "authentication" encompasses any legal purpose or function that the signature is considered to fulfil in each national jurisdiction.

Advanced electronic signature – This is an electronic signature that meets the following requirements:

- It is uniquely linked to the signatory
- It is capable of identifying the signatory
- It is created using means that the signatory can maintain under his sole control
- It is linked to the data to which it relates in such a manner that any subsequent change is detectable



adhere to the document on which the signature is written and that the signed data has not been altered after signature.

One of the issues that constantly arises in the context of internet retailing is to provide for an electronic signature system which could replicate a paper based signature.

The EU recognised this issue some time ago and in 1999, an EU system for the regulation of electronic signature based products and services was adopted as the Electronic Signatures Directive 1999/93 ("Directive").

Directive issues

There have been a number of issues with the Directive. Firstly, the Directive is very technical and indeed, arising from a recent report published for the Commission, judges still struggle with understanding the different levels of electronic signatures (basic, advanced and qualified) and how to assess the fulfilment of the technical criteria for creating a legally valid electronic signature.

Secondly, there is a lack of definition of the whole set of electronic signature products, a lack of referenced standards outside the standards related to Annex II(f) (trustworthy systems and products) and III (requirements for secure signature creation devices)

of the Directive and a lack of formal standards in the area of electronic signatures.

eSignature related standards that are referenced in the Official Journal are not necessarily harmonised standards but in some cases are based on CEN workshop agreements.

Indeed the Commission report referred to, recommended that the Commission update by way of decision the list of generally recognised standards which ensure compliance with Annex II (f) and Annex III of the Directive and further that the Commission issue a mandate to the European Standardisation

Organisations asking them to draft a guidance paper on the use of relevant standards including their legal relevance in the context of the Directive.

As mentioned above, the Directive defines three different types of electronic signatures, an electronic signature (ie a basic electronic signature), an advanced electronic signature and a qualified electronic signature (QES).

Qualified

What is particularly important about an electronic signature which is a QES is, that it is the only type of electronic signature which the Directive states must be recognised as having the same legal value

An EU system for the regulation of electronic signature based products and services was adopted as the Electronic Signatures Directive 1999/93

as a handwritten signature. In the case of a basic or advanced electronic signatures, Member States cannot deny their legal effectiveness and admissibility as evidence in court, solely on the ground that they are in electronic form or are not based on a qualified certificate etc. However the exact legal effect of an electronic signature in a particular context would be a matter for a court to decide in a given case.

The mandatory requirements for accepting a signature as a QES are i) that the electronic signature is an Advanced Electronic Signature, ii) the signature is supported by a Qualified Certificate and iii) the

It is clear from the definitions (see panel) of an electronic signature, that it gives an entity seeking to rely on it very little comfort.

Case study

In a recent case in the UK, a director of a company the subject of a winding up petition, asked a member of staff to send an e-mail to the solicitors acting for the plaintiff, to consider adjourning the winding up petition for one week in return for a personal guarantee. The e-mail itself was not signed, but the head of the e-mail showed that it came from the employee's address. There was no further reference to the e-mail sender's name in the body of the e-mail. The

judges still struggle with understanding the different levels of electronic signatures'

signature is created by using a secure signature creation device. The Qualified Certificate ("QS") is an electronic attestation which links signature verification data to a person and which confirms the identity of that person. The Directive lays down detailed requirements for the contents of the QS and also in relation to the service provider who will provide the QS.

Accordingly, the first thing to be considered, whether you are a supplier, or a customer (such as a government department), or, for example, a provider of a financial service over the Internet, is whether the law mandates the use of a QES in context.

Usage

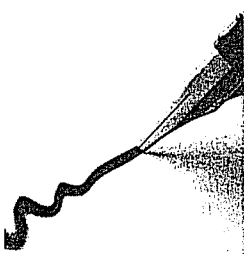
However, even if the law does not mandate the use of a QES, the parties may decide to use a QES where the use of the QES is essential to prevent the occurrence of serious legal risks (for example the level of transactions involved in the application supported by an electronic signature mechanism is considerably high).

In these circumstances, it is not so much the higher legal value of the QES that is important, but rather the security and functional guarantees that are inherent from the creation of the QES that are important.

proposal was accepted but then the employee did not honour the guarantee. The judge held that the e-mail message satisfied the statutory requirement of writing, but could not be classified as a signature. It was not possible to hold that the automatic insertion of an e-mail address was intended as a signature.

Planning

In the context of a closer user group, the parties may decide that a QES is not necessary and instead accept that members of the group will be bound by an electronic signature or an advanced electronic signature. However, the structuring of the closed user group will require careful planning from a systems perspective and also will require that the parties agree on a comprehensive set of terms and conditions, so that the risks in context are properly managed.



Paul Foley is a partner with McKeever Rowan

Enter the

THE rise of Enterprise Resource Planning software in the 1990s revolution in the way businesses work. Re-published research by Andrew McAfee of Business School uses data from Fortune 1000 over the decade from 2000 through 2005 underpinning a claim that the success of ERP is demonstrating a clear shift in competitive advantage. McAfee believes that ERP is the next big opportunity for technology to deliver shift in competitive advantage for business. This is to explore why this

Diminishing returns

ERP software automates business process, releases people from the equipment, cutting costs and speeding operations. Further optimisation may yield additional benefit – this is a sum of diminishing returns. Enterprise optimises these gains by taking a new approach. Where ERP has driven away from the process exacerbated by trends in globalisation, mobility, flexible working, Enterprise steps in to reconnect our workforce with 'problem solvers', or to step in when an error occurs – Enterprise businesses provide tools with the tools to enable problem solving more efficiently, through more effective collaboration with information and colleagues to speed up business process.

Web 2.0 technology as social networking sharing have achieved success in consumer and their collaboration makes them perfect

YOU IS NO L

At Hosting365, we can host sophisticated IT infrastructures. Important things, like Log on www.hosting365.com