Home
News Feed XML
Free Web Design Quotation
Add Your URL
Hosting
Domain Names
Job Search
Submit an Article
Directory
FAQ
Forum
Get our Logo
Webmaster Tools
Contact Us
Returns Policy
Search DMOZ

Articles & Tutorials

Latest Articles
ASP
Beginner's
C#
CSS
Topical
Databases
Design Tips
Dreamweaver
Flash
Net History
Hosting
HTML/XHTML

Revealing Facts

Posted on Wed 06 October 2004 by: **S,s Ramage**

By Sally Ramage Dabydeen, BA(Hons), MBA, LLM, MCMI, FFA.

The Computer and Internet Crime Conference 2004 which took place in Lon the 30th and 31st March was a very necessary and timely conference . Ed G Agent of the FBI and now at the US Embassy, gave a presentation , the ope address made by the Assistant Commissioner of the Metropolitan Police Tari Ghaffer.

Cybercrime such as internal and external hacking , spam and computer viru widely acknowledged. Hacking is a growing problem for businesses which st confidential client and customer details electronically. External hackers can confidential information, deface websites and steal financial company inform

Often, white collar crime is carried out by internal hackers but a larger prop through an outside source of security breaches. Employees can steal intelle property from their employers. Intellectual property theft includes theft of e address books, proposal documents used as marketing tools of solicitors, cli databases and contact information. An indication on how serious the proble white collar crime has become is the recent issue of "The Lawyer" which

JavaScript
Legal
Marketing
Networks
Perl
Photoshop
PHP
SEO
Security
Usability
XML

Other Resources

PHP Manual
PEAR Manual
SEO Tools

concentrated on the war on fraud and featured so many expert witnesses o collar crime.

In what way are hackers' activities illegal ? In the UK, it is a Data Protectio offence to send unsolicited e-mails. There is a new European Commission D introduced in 2003 which makes it a criminal offence to send unsolicited e-r the UK, this EC Directive has been implemented by the Privacy and Electron Communications Regulations 2003. Will these regulations deter the sending spam? Only if the source of the spam can be pin-pointed. Spam is particular sinister. At present spammers have created virtual countries' websites and banks even. Spammers can blackmail companies. Current anti-spam device filter spam. Spam also damage businesses by taking up valuable business ti dealing with them and also because they can carry malicious viruses which even more major disruption to businesses . Viruses in a business's compute are very costly in terms of data recovery, slow-down in productivity, necess software upgrades as well as loss of business, not to mention the lowering o morale and the damage to the business reputation . Internet filtering and e monitoring software, anti-virus software , backing-up of data, and systems policies are steps to controlling any potential damage. Staff policies must be place. The consequences of e-mail misuse must be set down in company po

If staff , for example, use e-mail to circulate ridicule about other staff memb would amount to gross misconduct and dismissal. Such e-mails would amou intrusions into employee privacy as per Article 8 of the European Conventio Human Rights.

When things go wrong, electronic documents, spread-sheets and e-mails ho relevant material for litigation. More and more in court cases, evidence is fo be exclusively in electronic format. Forensic technology therefore needs to t large part of the investigation. Forensic technology can recover, for example deleted material. Forensic techniques can recover multiple versions of the s document from traces left on electronic media. Small differences between th altered versions can be used to build up a picture of what changes were ma when. The time-line of document creation and differing versions can be use corroborate or disprove the chronology of events. Electronic evidence must the provenance of the material and the entire history of electronic material collated to produce robust evidence in court. The evidence must be collecte the UK evidence laws. Metadata is hidden within electronic files, examples o are entries in e-mails, dates embedded in documents and links to other files case of e-mails, a full audit trail does exist and can be retrieved.

It is now possible for forensic technology specialists to use forensic tools to volumes of material for electronic files and filter such material to reveal pot disclosable material. The volume of material in large businesses can be in te in size. This material can be sifted on live computer servers without disrupti business or alerting any suspects.

And when a fraud case comes before the courts, evidence is displayed in co large computer screens to the jury and the defence, rather than on paper. H most successful prosecutions rely on more than one stream of computer-de evidence. What is needed is more than one independent stream of evidence paper and computer-derived, which collaborate each other. There are cases e-mails have been forged and it is no longer the case that because it is in el form, it must be true. A recent case in the UK is R v Bhatt (unreported) Can Crown Court [2003]. During the trial, the defence illustrated to the court ho an e-mail is forged by simulating a link to the Internet to create and explair electronic communications can be manipulated in real time. The simulated e was "read" with a standard e-mail client, Microsoft Outlook Express and it a no different from the paper e-mails that the prosecution offered as "proof" t e-mail had in fact been sent by Bhatt. Only a full technical examination of th "headers" within Outlook Express system would have revealed the forgery, after a significant amount of network investigation.

So what can accounting departments do ? A fraud policy can be formulated. policy is a formal, written statement recording the company's attitude to fra should make clear that fraud is unacceptable and that all instances of suspe fraud will be treated seriously and dealt with swiftly. Staff should be require indicate their awareness of and compliance with the fraud policy on an annu The policy will serve a useful purpose as a deterrent. The company should a a contingency plan setting out the steps that should be taken in the event th is suspected. This plan should be known to all staff.

About the Author

Posted on Wed 06 October 2004 by: **S,s Ramage** at **ssk**

UNIVERSITY LECTURER, AUTHOR.