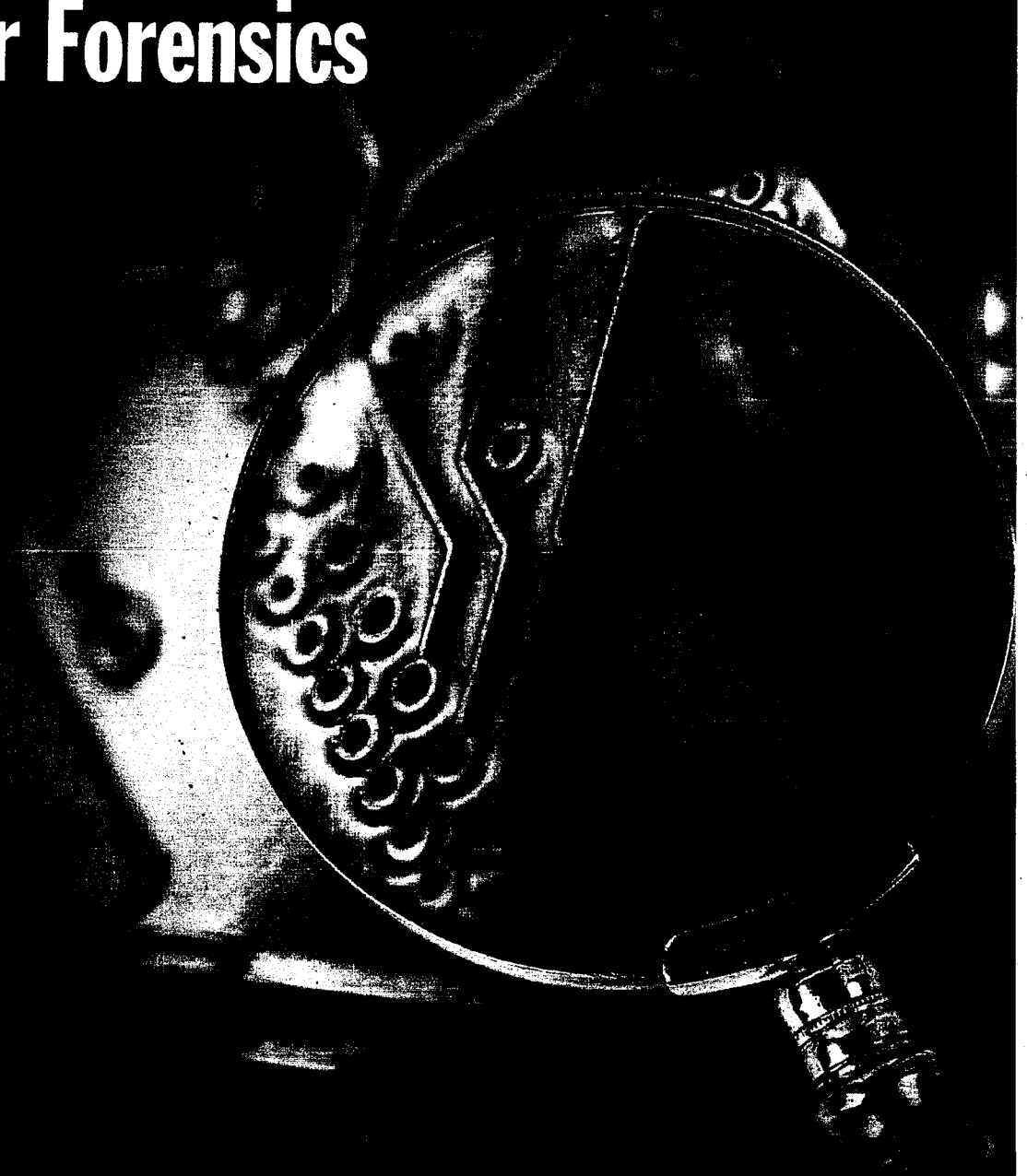
Information Systems
# Control
JOURNAL
VOLUME 6, 2005

# Computer Forensics



Best Practices for Computer Usage

Identity Theft and Cybercrime

Cyberforensics

*Gather and preserve evidence successfully.*

WWW.ISACA.ORG

# Security and Ownership of Personal Electronic Devices

*By Richard A. Bassett, DPS, Rita Mack, Jason Foster and Andrew Swiatlon*

In this age of instant communication, there are all sorts of wonderful and amazing gadgets. People can talk to anybody, anywhere, at any time, receive electronic messages anywhere at anytime and access all kinds of stored information. In addition to satisfying the desire for "instant" everything, these devices actually have become a need. Depending upon the profession, there can be expectations that employees will always be available for immediate communication or have the most current data available. The medical profession, service functions such as systems programmers and analysts, people in financial industries, marketing practitioners and others are expected to be instantly available at all times with the answers at their fingertips.[1]

So, how do people manage? Many have personal electronic devices (PEDs) to help them. These are familiar as the ubiquitous cell phones, Blackberries, laptop and tablet computers, personal digital assistants (PDAs) and, lately, little devices popularly known as flash drives. All of these items make information portable, and, except for the flash drives, they can also interact with the Internet and each other. The flash drive can only store data with no interactive ability. What all of these devices have in common is their ability to carry confidential information that could cause financial, corporate and personal problems if the data were mishandled.[2] These compact portable devices have become so commonplace that one rarely stops to think of what would happen if they were misplaced, lost or broken down and in need of repair.

## Risks

Numerous risks result if these devices and the data they contain are not secured. **Figure 1** illustrates some of these risks and the kinds of data available on the devices.

Cell phones contain phone numbers, e-mail addresses and other information related to one's personal and corporate lives. Many people cannot remember the last time they physically dialed a phone number. The cell phone knows all, and people feel lost when it loses its charge or breaks. If the data on a cell phone were available to another person with a lack of scruples, the owner might suffer significant consequences. In spite of this, many people still fail to secure their phones with a password. They are equally cavalier with the data on their Blackberry and PDA. These devices can also hold e-mails with personal or confidential data. Quite often, it is corporate information that has no business being made public.[3] As with cell phones, most people fail to secure their Blackberry or PDA with a password.[4] The same goes for portable PCs. There is quite often information on them that has no business being in the public domain and could conceivably cause great damage if it were made known. This might include customer lists, corporate projections and figures, research results, patient information for those in the medical arena, client information for the legal industry, or any other information that requires confidentiality. Because these devices are used in an interactive manner through the Internet, all of these devices run the risk of being co-opted by hackers if they do not have security programs that are maintained on a regular basis. With the increase in Bluetooth-enabled devices, attacks such as bluesnarfing, bluejacking and bluebugging will only become more common. These attacks normally occur over short distances; however, there are now devices called Bluetooth rifles that extend that range to a mile.[5]

**Figure 1—Devices, Types of Data and Risks**

| Device | Types of Data | Risks | Sample |
|---|---|---|---|
| Cell phones | Phone number<br>E-mail addresses | Loss<br>Stolen<br>Improper disposal<br>Viruses |  |
| PDAs | Phone numbers<br>E-mail addresses<br>Mailing addresses<br>Contact information<br>Patient information<br>Financial information<br>E-mails<br>Databases<br>Spreadsheets | Loss<br>Stolen<br>Improper disposal<br>Viruses<br>Unauthorized access |  |
| Blackberries | Phone numbers<br>E-mail addresses<br>Mailing addresses<br>Contact information<br>Financial information<br>E-mails | Loss<br>Stolen<br>Improper disposal<br>Viruses<br>Unauthorized access |  |
| Flash drives | Documents<br>Images<br>Spreadsheets<br>Databases | Loss<br>Stolen<br>Improper disposal<br>Unauthorized access |  |
| Tablet PCs | Any information that could be found on a PC | Loss<br>Stolen<br>Improper disposal<br>Viruses<br>Unauthorized access |  |
| Laptops | Any information that could be found on a PC | Loss<br>Stolen<br>Improper disposal<br>Viruses<br>Unauthorized access |  |

An unprotected device is vulnerable to an immense library of viruses, Trojan horses, worms, etc., that can make data available to unscrupulous persons.[6] Depending upon the information in question, unsecured data can lead to lawsuits. In the medical field, for instance, regulations exist for the protection of patient data that mandate strong fines for those who do not protect the data properly.[7] Data management has similar protections in the financial arena.

Another major risk is the loss of personal data leading to identity theft. Identity theft is a very real threat, and having unsecured data and devices that hold the data is not simply careless, but also dangerous. Identity theft can lead to untold problems, including ruined credit and one's name being used for unscrupulous purposes. The only devices that are somewhat free of these problems are the flash drives. As they are not interactive, they can be the bearer of viruses if loaded with an infected file but cannot be directly infected by malicious activity unless they are docked. The risks inherent in losing them and their data are the same as with the other PEDs.

## Statistics on Scope of Problem

Examination of key benchmark statistics illustrates the size of the problem that owners and users of PEDs face. In 2001, in London, UK, the following devices were left in cabs: 62,000 cell phones, 2,900 laptop computers and 1,300 PDAs. In the same time frame in the US, the following items were lost: 350,000 laptop computers, 35,000 handhelds (PDAs/Blackberries) and 232,000 cell phones.[8] In 2002, in the US, more than 250,000 PDAs alone were lost.[9] According to a recent survey,[10] 33 percent of PDAs have no password protection enabled, 57 percent of PDAs contain unencrypted sensitive corporate data, 85 percent of devices contain sensitive business-related data, and 25 percent of PEDs are lost or stolen.[11] Only 25 percent of the lost devices are returned.

Examining the monetary side of the equation, Gartner estimated in 2001 the average cost for a lost portable device, including loss of data, to be between US $2,500 and US $3,000.[12] The number of PDAs (not including smart phones) shipped in 2004 was 12.3 million devices.[13] Based on these numbers, the impact, not including identity theft and corporate divulgence, is between US $490 million and US $588 million just for PDAs shipped in 2004. These are astounding, mind-boggling numbers. Given the amount of lost data and the financial impact to owners and corporations that these numbers represent, one can begin to understand the truly enormous scope of the problem faced not only by the owners of PEDs but also those whose corporate, personal, medical or financial data were lost.

*A device that uses biometrics is safer than one that uses only a password.*

## In the News

Here is just a small sampling of recent news clips relating to stolen laptops:

- 5 April 2005—A laptop owned by copier maker Ricoh Co. was stolen when an employee fell asleep at the train station. The laptop contained data on more than 18,000 customers.[14]
- 28 March 2005—Two laptops were stolen from the San Jose Medical Group when thieves broke into the administrative offices. The laptops contained personal information, including Social Security numbers and confidential medical information, on 185,000 patients.[15]
- 11 March 2005—A laptop that contained personal information on almost 100,000 alumni, graduate students and past applicants was stolen from a University of California, Berkeley (USA), office. According to Joanne McNabb, chief of the state's Office of Privacy Protection, 58 percent of security breaches recorded by California officials are the result of loss or theft of computers or other devices containing personal information.[16]

## Security Overview

Ensuring the security of these devices is essential, as their very size and portability are what makes them so vulnerable. They are easy to misplace, which makes them easy to steal. There are also risks if they need to be sent out for repair. While the service facility might be trustworthy, what if the device is lost in transit? The cost of destroying the device against having it repaired must be weighed, and these costs are not just monetary.[17] It becomes apparent that, while people take all this connectivity and instant information for granted, they must pay close attention to how they handle the security risks inherent in the media. Just as people would not leave a house, car or other valuables unsecured, so they must recognize that information is also valuable and learn to secure not only the access to their PEDs but also to the data.

## Security Measures

Measures can be taken to provide a more secure environment for a user of a handheld device. These measures can be broken into three levels: physical security, data security and network security.[18]

## Physical Security

Physical security involves the protection of the actual device from being lost, stolen, damaged or accessed. This is the best measure one can take to have the most secure device, because if physical security is sustained, the other measures are not as necessary.[19] The most common method for physically securing a PED is to carry it safely. Owners of these devices should carry them in a way that a thief cannot see it or it would be very difficult for him/her to steal it. This can be accomplished by keeping it in a front pocket or a locked briefcase. It should also be kept in a protective case so that if it is dropped, it is less likely to break.

Another way to physically secure a device is to prevent access to it if it does get lost or stolen. This involves setting a basic power-on password that must be entered to use the device. A strong password is recommended for better security. Some pocket PCs offer four-digit numeric passwords, and others offer stronger alphanumeric passwords of seven or more digits.[20] Others have more advanced protection measures, such as biometrics, which involves a fingerprint scan. Some of these devices even have the capability of using both biometrics and password protection. Biometrics is starting to evolve into a more widely used protection method, and a device that uses biometrics is safer than one that uses only a password.

One final way of physically securing a device is to make sure it can be properly identified if it is lost or stolen. There are different approaches to this depending upon your personal preferences. One way is to write or engrave the owner's name on the back of the device or attach a business card to the back instead of permanently keeping the owner's information on it. For people who do not like to disclose their identity by putting their names on the back, labels with confidential code numbers can be bought and placed on the device.[21] People who find a lost device with one of these labels attached can call the toll-free number located on the label. The number is for a third party who then informs the owner of the missing device. Another way is to use a feature that is usually available in all devices, especially PDAs; it allows the owner to enter his/her name and phone number under a tab called "owner" within the preferences section.[22] If the device is locked when the owner loses it, this information will still be shown whenever the device is turned on.

## Data Security

After taking physical security measures, the next level of security is to protect the data from unauthorized access. A number of methods can be used in this quest. One way is to encrypt sensitive data, which involves converting the data into a form that cannot be easily understood by an unauthorized user. Many different types of encryption programs (such as Ccrypt and PointSec) are available to help protect data from being accessed.[23] Some antivirus software allows data to be automatically wiped from the device if there are too many unsuccessful login attempts.[24] An increasing number of viruses (such as SYMBOS_SKULLS.A and SYMBOS_CABIR.A)[25] target PEDs, and as PEDs become more popular in business and even personal environments, there will be more incentives for hackers and crackers to sabotage the devices.

Another way to protect data from being accessed is to store any sensitive data on a memory card. When the device is not in use, the memory card can be removed so the sensitive data are not left on the device. This is also helpful if the device breaks and has to be sent out for repair. The owner will not have to worry about someone copying valuable information without approval.

*Store any sensitive data on a memory card.*

Also important to securing an electronic device's data is to regularly back up the data. This may not prevent the data from being accessed, but at least the owner will be able to report exactly what is at risk and inform any necessary people that their information is vulnerable.

## Network Security

The measure to take to have the highest level of security for a PED is securing its network. If the device has Wi-Fi or Bluetooth, it should be disabled when not in use. This helps minimize the chance of unauthorized users accessing the device. There are monitoring and notification programs, such as System Security Monitor for Pocket PC,[26] that are available with the ability to track and detect hidden activity on a PED.[27] These can be very helpful because sometimes it is not apparent that the data are being accessed. In addition, there are now firewalls designed for PDAs and other PEDs that help protect the devices from being accessed over a network. Finally, if the device is going to be hooked up to a company's network, a virtual private network (VPN) should be used. This uses encryption in the lower protocol layers to provide a secure connection over an insecure network such as the Internet.

If these security measures are taken for a PED, there is a better chance of preventing access to important data by an unauthorized user. Each person must educate himself/herself on what these risks are and what can be done to minimize the chance of becoming a victim.

## Legal/Ethical

In determining risks and the steps necessary for their mitigation, legal and ethical implications cannot be ignored. There are ramifications of not implementing the appropriate measures to ensure confidentiality of consumer data. Several instruments of note include the Council of Europe's (CoE) 1981 "Convention for the Protection of Individuals with Regard to Automatic Processing of Personal Data," the Organization for Economic Cooperation and Development's (OECD) "Guidelines Governing the Protection of Privacy and Transborder Data Flows of Personal Data," and the European Union Data Protection Directive of 1995.[28]

CoE's Article 7, regarding data security, states, "Appropriate security measures shall be taken for the protection of personal data stored in automated data files against accidental or unauthorised destruction or accidental loss as well as against unauthorised access, alteration or dissemination."[29] Article 10 directs that each party determine appropriate measures to address violations of the Convention.

The OECD "Guidelines Governing the Protection of Privacy and Transborder Data Flows of Personal Data" also has a provision for the security of personal data. Section 11 specifies, "Personal data should be protected by reasonable security safeguards against such risks as loss or unauthorised access, destruction, use, modification or disclosure of data."[30] The OECD guidelines also direct member countries to "provide for adequate sanctions and remedies in case of failures to comply."

Section VIII, article 17, of the European Union Data Protection Directive of 1995 governs the security of data processing: "Member States shall provide that the controller must implement appropriate technical and organizational measures to protect personal data against accidental or unlawful destruction or accidental loss, alteration, unauthorized disclosure or access, in particular where the processing involves the transmission of data over a network, and against all other unlawful forms of processing."[31] Per articles 22 and 23, member states must provide for a judicial process for any violation of these rights as well as compensation for any damages.

Even though the US does not have general data protection laws, it does have laws for data protection in several important sectors, including financial institutions, healthcare and the insurance industry.

Title V of the Gramm-Leach-Bliley Act of 1999 (GLBA) governs the security and confidentiality of customer information

by financial institutions. The Health Insurance Portability and Accountability Act of 1996 (HIPAA), in conjunction with 45 CFR part 164, Department of Health and Human Services Security and Electronic Signature Standards, established regulatory guidelines for the health and insurance industries.

GLBA "requires that federal regulators issue rules that call for financial institutions to establish standards to ensure the security and confidentiality of customer records."[32] These rules were established by the US Federal Trade Commission and are similar to the Banking Agency Guidelines, which focus more on the process of safeguarding customer information, not on the actual technology used.[33] Section 314.4 is relevant to PEDs and states that a financial institution must "identify reasonable internal and external risks to the security, confidentiality and integrity of customer information that could result in the unauthorized disclosure, misuse, alteration, destruction or other compromise of such information and assess the sufficiency of any safeguards in place to control these risks."[34] Penalties for noncompliance range from fines to criminal prosecution.

*Risks associated with inaction can have a significant, negative long-term impact.*

HIPAA and 45 CFR part 164 establish standards for the healthcare industry to take "reasonable and appropriate" steps to "ensure the confidentiality, integrity and availability of all electronic protected health care information the covered entity creates, receives, maintains and transmits."[35] They also state that protected health information must be protected from any "reasonably anticipated threats or hazards" and from any "reasonably anticipated uses or disclosures" that are unauthorized. Penalties range from US $100 per violation and US $25,000 for all violations of a single requirement up to US $250,000 and/or imprisonment of up to 10 years.[36]

Other areas of concern are institutional reputation and civil lawsuits for damages as a result of identity theft or release of sensitive information. While laws and regulations govern unintentional releases of information that may occur as a result of not taking appropriate security precautions, it is beneficial for corporations to apply preventions that go above the minimum required by law. All it takes is one incident for an institution to lose all confidence from consumers, and there are financial risks associated with loss of consumer confidence—not only a potential loss of revenue but also significant civil penalties awarded by sympathetic juries if lawsuits are brought against the organization. Security of PEDs that store consumer information and other sensitive data should not be sacrificed to satisfy the bottom line, as the risks associated with inaction can have a significant negative long-term impact on the institution.

## Conclusion

Many risks are associated with PEDs. The loss, theft or damage of these devices increases the possibility of unauthorized access to sensitive corporate and personal information, unauthorized access to unsecured devices by determined hackers with readily available tools, and unauthorized access by unscrupulous repair personnel. Taking simple precautions can reduce the likelihood of these risks occurring. These precautions include physical security of the device, encryption of the data and appropriate disposal at the device's end of life. If appropriate and reasonable measures are not taken, consequences relating to legal and regulatory noncompliance can have a negative impact on a company that goes beyond the cost of compliance. Negative impacts include fines and judgments, prison time, and loss of consumer confidence. Many businesses have tainted reputations caused by not taking appropriate security and data protection measures. While it is too early to determine the effects of security incidents, such as the loss of backup tapes from Bank of America or the release of sensitive consumer data to identity thieves by ChoicePoint, the loss of reputation will likely haunt both organizations for years to come. What institution wants to be the next associated with the loss of potentially damaging information in the case of, for example, an employee who leaves a laptop in an airport bar? Security is possible, it is not difficult, it pays off and it is everyone's personal responsibility.

## Endnotes


1 MediaLive International and Core Competence Inc., "Mobile User Security," *http://hhi.corecom.com/IPcomm2004-MobileUserSecurity.pdf*, 2004

2 *Ibid.*

3 LeBlanc, Linda; "Lost Handheld Puts Your Data in Danger," RIMROAD: Special Reports, 8 February 2005, *www.rimroad.com/articles/2005/2/2005-2-8-Lost-Handheld-Puts.html*

4 Leyden, John; "PDA Security Still Dismal," *The Register*, 1 September 2004, *www.theregister.co.uk/2004/09/01/pda_sec*

5 Granneman, Scott; "Owning a New Phone," *Security Focus*, 23 March 2005, *www.securityfocus.com/printable/columnists/310*

6 *Op. cit.*, Leyden

7 CACI, "HIPAA Penalties," *www.caci.com/cacihealth/penalties.htm*

8 Sinrod, Eric J.; "Serious Data Loss From Missing PDAs Poses Threats," *USA Today*, 21 August 2003, *www.usatoday.com/tech/columnist/ericjsinrod/2003-08-21-sinrod_x.htm*

9 University of Arizona's Information Security Office, "Palm Pilots/PDAs/Cell Phones/Wireless Security," *http://security.arizona.edu/WirelessSecurity.ppt*

10 *Op. cit.*, Sinrod

11 Ahlberg, Magnus; "Exposing Your Life—The Top Facts on PDA Usage," *Help Net Security*, 19 September 2003, *www.net-security.org/article.php?id=564*

12 Gartner, "Gartner Advises Businesses to Save Money by Tracking Low-cost Portable Assets," Press release, 24 April 2001, *www4.gartner.com/5_about/press_room/pr20010424a.html*

13 Gartner, "Gartner Says Worldwide PDA Shipments Grew 7 Percent While Revenue Increased 17 Percent in 2004," Press release, 14 February 2005, *www3.gartner.com/press_releases/asset_120374_11.html*

Press release, 14 February 2005, *www3.gartner.com/press_releases/asset_120374_11.html*

14 "Ricoh Laptop With Customer Info Stolen," *Japan Today*, accessed 12 April 2005, *www.japantoday.com/e/tools/print.asp?content=news&id=333056*

15 Roberts, Paul; "Stolen Laptops Contain Medical Info on 185,000 Patients," *Network World*, 8 April 2005, *www.nwfusion.com/news/2005/0408stolelapto.html*

16 Liedtke, Michael; "Stolen Laptop Exposes Data of 100,000," *Miami Herald*, 30 March 2005, *www.miami.com/mld/miamiherald/news/breaking_news/11265931.htm*

17 *Op. cit.*, MediaLive International and Core Competence Inc.

18 Shinder, Deb; "Securing Your Pocket PC," *Windows Security*, 6 July 2004, *www.windowsecurity.com/pages/article.asp?id=1344*

19 *Ibid.*

20 Karlinsky, Harry; "Is Your Personal Digital Assistant Secure?" *CPA Bulletin*, October 2003, *www.cpa-apc.org/Publications/Archives/Bulletin/2003/october/karlinsky.pdf*

21 *Ibid.*

22 *Ibid.*

23 Federal Register, "45 CFR Part 164 Security and Privacy," Library of Congress, 12 August 1998, *www.access.gpo.gov/nara/cfr/waisidx_02/45cfr164_02.html*

24 Taylor, Laura; "Security Basics for PDAs and Handheld PCs," *Small Business Computing*, 27 August 2004, *www.smallbusinesscomputing.com/webmaster/article.php/10732_3400641_2*

25 Simonds, Lauren; "Dial 'V' for Virus: Cell Phones and PDAs at Risk," *Small Business Computing*, 20 January 2005, *www.smallbusinesscomputing.com/news/article.php/3461671*

26 *Op. cit.*, Shinder

27 *Ibid.*

28 Privacy International, "PHR2004—Overview of Privacy," 13 November 2004, *www.privacyinternational.org/article.shtml?cmd[347]=x-347-82589*

29 Council of Europe, "Convention for the Protection of Individuals With Regard to Automatic Processing of Personal Data," 28 January 1981, *http://conventions.coe.int/Treaty/en/Treaties/Html/108.htm*

30 OECD, "OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data," 23 September 1980, *www.oecd.org/document/18/0,2340,en_2649_34255_1815186_1_1_1_1,00.html*

31 "Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data," 24 October 1995, *http://europa.eu.int/smartapi/cgi/sga_doc?smartapi!celexapi!prod!CELEXnumdoc&lg=EN&numdoc=31995L0046&model=guichett*

32 Murphy, M. Maureen; "Privacy Protection for Customer Financial Information RS20185," CRS Report for Congress, 28 February 2003, Library of Congress, *www.epic.org/privacy/glba/RS20185.pdf*

33 Office of the Comptroller of the Currency, Treasury; Board of Governors of the Federal Reserve System; Federal Deposit Insurance Corporation; Office of Thrift Supervision, Treasury; "Interagency Guidelines Establishing Standards for Safeguarding Customer Information and Rescission of Year 2000 Standards for Safety and Soundness," 9 June 2000, *www.federalreserve.gov/boarddocs/press/boardacts/2000/20000621/attachment.pdf#search='12%20CFR%20Part%2030'*

34 Federal Register, "16 CFR Part 314 Standards for Safeguarding Customer Information," Library of Congress, 23 May 2003, *www.access.gpo.gov/nara/cfr/waisidx_03/16cfr314_03.html*

35 *Op. cit.*, Federal Register, 1998

36 *Op. cit.*, CACI

***Richard A. Bassett, DPS***
is an assistant professor of management information systems at Western Connecticut State University (USA). He founded and was CEO of Bassett Computer Systems Inc. for 17 years where he was involved with the design and implementation of information systems for hundreds of small and midsized businesses. He has authored several articles and is actively involved with the technology endeavors of numerous organizations including The Children's Center, Bridges of Milford, North Haven Rotary Communicare and the Amber Alert System.

***Rita Mack***
is retired from IBM with more than 30 years in information and computer systems and is now employed by Deloitte & Touche as an information systems auditor. She can be reached at *ritamack1@juno.com*.

***Jason Foster***
is a project manager with nine years of experience in ERP implementations, business process analysis and design, and regulatory compliance. He can be reached at *jasonfosterct@yahoo.com*.

***Andrew Swiatlon***
is a recent graduate with a promising future in the field of information technology.