CPCU SOCIETY INSURING YOUR SUCCESS

Cutting Edge IT

Volume 15 Number 2 September 2008

Meet Our New Information Technology Interest Group Chairman

by Celeste Allen, CPCU, CLU, ChFC, FLMI

■ **Celeste Allen, CPCU, CLU, ChFC, FLMI**
State Farm Group
Bloomington, Ill.

Congratulations to **David L. Mowrer, CPCU, CLU, ChFC, AIT, ARM, AIM,** the new chairman of the Information Technology Interest Group. We look forward to his vision and leadership.

Mowrer has worked in auto claims with State Farm Insurance for 35 years. He joined State Farm after graduating from Washburn University in Topeka, Kan., with a bachelor's degree in business.

Mowrer received the CPCU designation in 1990. He served the Central Oklahoma CPCU Society Chapter as treasurer in 1991, vice president in 1992, and president in 1993. Mowrer became a volunteer in the CPCU Society in 1994 and worked on the Intra-Industry Committee until October 1999. He served on the Sections Web site Task Force from October 2000 until it completed its mission in August 2001. Mowrer joined the Information Technology Section Committee (now the Information Technology Interest Group Committee) in October 2001.

Mowrer is a strong supporter of CPCU Society involvement on local and international levels. He believes that receiving the designation is not the end of the journey but rather the opening of the door to many opportunities.

"One has the opportunity to continue learning and growing through speakers, seminars and workshops from the local chapter, the CPCU Society Annual Meeting and Seminars, and the CPCU Society Center for Leadership. There is also the opportunity to work with, and learn from, people in other areas of the insurance industry by serving in a chapter or the CPCU Society. Joining an interest group gives one access to resources and the opportunity to network with others in a specialty or particular area of interest. The strength of the Society lies in its volunteers."

Mowrer encourages all CPCUs, from new designees to those who have had their designation for years, to spread the word about CPCU and take the step toward getting involved, either at the chapter level or in the international CPCU Society, as it is a win-win for the volunteer and the Society. ■

What's in This Issue

My Desk Is Wherever I Lay My Mobile Device

by Celeste Allen, CPCU, CLU, ChFC, FLMI

The next time you are on a plane, a train, or in any waiting area, you will see a large number of people with some type of handheld device — be it a cell phone, laptop or BlackBerry. The ideal device would be all encompassing (e-mail, telephone, Internet access, etc.) and lightweight, thus reducing the need to carry multiple devices and alleviate the need for a laptop (and avoid the laptop screening at airports) . . . oh happy day! Handheld devices provide connectivity. While you are traveling or waiting for a home or car repair or installation, you can easily remain in touch with office colleagues and clients. Mobile devices also enhance productivity, because you can attend to e-mail and other tasks during absences from the office.

Trends and Issues

Personnel Today cites reports by the Business Performance Management (BPM) Forum that uncovered key issues of companies participating in BPM Forum's mobile workforce studies:

- Seventy-one percent of respondents said the percentage of remote workers is increasing at their organizations.
- Eighty-six percent said their IT departments felt increased pressure to support mobile and remote workers.
- Forty-one percent said their firms suffered business disruptions because of ineffective support.

Protecting against threats, intrusions and viruses is the number one IT priority associated with remote and mobile workers, followed by improvements in technical support.

Increased numbers of mobile workers and an increased importance of getting important communiqués to these workers serve as an impetus for organizations to beef up infrastructure support of mobile workforces. Lack of speed and innovation in this arena will lead to missed and failed communiqués, which in turn can impact customer service and worker productivity.

While there is an increased tendency and flexibility to allow employees to work from home, which can often enhance productivity, there is a corresponding need to ensure that information transmitted to and from workers' homes remains secure. There are various options available to connect remote workers, but whatever option is chosen, workers must have consistent and reliable connectivity.

Options include:

- Using 3.5 G networks, which provide access to the Web at up to 2Mb per second broadband speeds through the use of mobile phones, laptops, personal digital assistants or smartphones.
- Wi-Fi (wireless networks) hotspots.
- The Internet.

Increased mobilization of our workforce leads to increased security concerns, such as the theft of data and breach of confidential information, because of the use of handheld devices and laptops.The Computing Technology Industry Association reported that 55 percent of its organizations reported significant increases in security issues over the last 12 months. Eighty percent of organizations permitted data access by remote or mobile workers, with 32 percent having implemented security awareness training. As such, IT shops are looking to their mobile operator partners to help them manage, control and secure mobile devices. CIOs reported significant productivity gains through the use of mobile technology, and are in search of comprehensive mobile device management (MDM) solutions. Sixty percent of U.S. companies indicated they would switch mobile operator partners to one which could provide MDM as a managed service.

IT shops are presented with the challenge of doing more at remote locations, and thus have a need for the right set of tools to provide reliable performance for applications. They need to be able to assess network performance and diagnose problems for remote workers, especially during network outages. Challenges lie in the fact that most in-band network management systems were designed to work with LAN systems versus WANs. Out-of-band technologies pertain to devices such as keyboards, mouses and console servers that provide an alternate means to access remote devices. A key requirement of a remote management solution is constant connectivity and access to devices being managed. Direct access to devices by IT staff is another requirement which would allow them to stay on top of security management policies not available through network dependent tools. Also important would be a local suite of management functions, such as automated routine system monitoring, maintenance, configuration and recovery tasks.

The Latest and Greatest Tools

Given the increased mobility of workforces, Benjamin Gray of Forrester, an independent business and IT research organization, indicates from a technological perspective that the sky is the limit in terms of where businesses can venture relative to speed

of decision making through the use of very small devices. Challenges lie in the pace at which hardware technological innovations far outpace those of software innovations.

Examples of fast-paced hardware technological innovations include new wireless standards, such as 802.11, WiMAX and component technology. Companies must ensure that they have both the public and private wireless infrastructure to support client devices used for its mobile workforce. Client management suites, from companies such as HP, Symantec and CA, were previously used for desktops and laptops, but they either lacked sufficient client management or companies chose to look at different suites, such as iAnywhere Solutions, Motorola and Nokia, for management of handheld devices.

Gray forecasts that we are three to four years away from a unified solution. The above becomes even more important given the following:

- Entry of the Millennials (with real-time needs) into the workplace.
- Increased dependence on mobile-like applications beyond e-mail.
- Steady reductions in the prices of PCs and handheld devices.
- Increasing speed of networks.
- Increased number of hotspots.
- Increased usage of mobile devices in the workplace.
- Threats that mobile devices present to the security of personal and corporate information because of viruses, worms, theft and opening up devices to networks.

IT shops would love to have a handle on the future outlook of new mobile technologies, yet this is not always possible. As such, companies need to develop a mobile enterprise technology road map and revamp it each year. The growth of laptops and smartphones

has outpaced the growth of desktops and mobile phones. This is significant, especially given that many workers are extending work hours and opting for flexibility in work arrangements.

The newest trend in devices is ultra-mobile PCs (UMPCs). Although providing the experience of a full-size PC, these devices can be as small as a paperback book. The hold-back for enterprise-wide adoption of this type of device is lack of user experience and cost. Convertible tablets are lightweight PCs (2.5 to 5 pounds) with 12- to 14-inch displays that are rotatable, can fold down, and also can be used as slates for writing. Touch screen capabilities are available. Convertible tablets are considered niche solution devices, not yet ready for prime time until a significant drop in the price differential between convertible and standard laptops. IT shops will need to increase the rate at which they mobilize applications.

Consumers are provided with a wealth of mobile devices. There is positive growth in worldwide sales of handheld cellular devices, especially given decreasing prices for services and equipment. Some devices are fully loaded and include MP3 players, FM radios, built-in cameras, games, wallpaper downloads and a plethora of ringtones. Business users, on the other hand, may be encumbered by trying to use enterprise applications and services.

Phones deemed suitable for business include:

- The Palm Treo 700W, provided by Verizon, which operates on a Windows Mobile platform (versus Palm OS platform), provides support of Exchange-based e-mail, has ease of integration with desktops, and operates on Verizon's very fast network.
- The Motorola Q, which features a thin design, a micro keyboard, a sleek design (as evidenced by RAZR phones), and supports a range of audio and video file types.
- The BlackBerry 8700c, offering very good push e-mail for enterprise users and has a robust catalog of third-party software.
- The HTC Apache, which has a keyboard that slides out from behind the unit and operates in a landscape orientation.
- The LGVX9800, a clamshell hinged along the long side of the phone, with two speakers aside the screen and a full keyboard at the bottom.
- The Sony Ericsson P910i, with a flip-down micro keyboard, an on-screen keyboard and a suite of productivity applications.
- The Nokia E61, optimized for e-mail and with great standards support for adoption of wireless Web-based services.

Continued on page 4

My Desk Is Wherever I Lay My Mobile Device

Continued from page 3

There are also two phones that utilize Bluetooth in linking multiple mobile devices. One is the Nokia 770, which runs on Linux and a browser, and has an 802.11g Wi-Fi radio. It uses a WPAN (wireless personal area network) approach to mobile computing. The other is the OQO 01+, which is a full-blown PC with a 30 GB hard drive and includes 802.11b and Bluetooth.

Keith Shaw, programming director and columnist for *NetworkWorld*, came upon several "cool tools" for enterprise and business users at the CTIA Wireless 2007 show. These tools included:

- The LE1700 by Motion Computing, which is a slate-tablet PC with Intel Core 2 Duo processors; embedded wireless WAN; Window's Vista; WriteTouch display that switches between writing with a finger and a stylus; fingerprint-reader technology; built-in Wi-Fi and Bluetooth with a battery with a life of up to three hours (optional extended battery support available); and a hard-drive accelerometer that stops the hard drive when a shock or drop is encountered.
- Motorola's MC35 Enterprise Data Assistant, a handheld mobile computer primarily designed for a mobile field sales workforce, with built-in GPS, Wi-Fi and Bluetooth connectivity, digital camera, e-mail, Internet browsing, bar code reader, and wireless Edge support.
- High Tech Computer's (HTC) shift portable computer with windows Vista, advanced wireless connectivity, Windows Mobile 6 operating system, and a magnetic connection system that adds a keyboard. And, to boot, the device folds up to fit into a coat pocket!

The Future

Paul Jackson, a principal analyst with Forrester, is a proponent of collaboration between PC and wireless industries for the delivery of the most viable path for mobile Internet devices (MIDs). He cites

the following February 2007 statistics: 73 percent of adults in the U.S. were owners of mobile phones; 21 percent of adults visited mobile Internet sites; and 32 percent of U.S. households own laptops, with 24 percent of this number having accessed the Internet outside of their homes via hotels, coffee shops, airports, train stations and other public access points. With three-quarters of U.S. adults online, there has been an increasing demand for Internet–residential services. This shows that Internet access is pretty much an integral part of our lives. A good example of this phenomenon is the iPhone, which represents a device that merges connectivity, storage and local processing power. Consumers are now not only downloading digital photographs and music, but also sharing them among peers.

Jackson asserts there is a disparity between advances in technology for mobile devices and the mobile Internet experience, triggering issues such as: folks who feel encumbered by phones that do not take crisp photos; laptops that are too unwieldy; and design of the Web, currently geared toward viewing on standard monitors rather than on a very small mobile phone. When PC, Web, and wireless industries collaborate effectively, we expect that the collaboration will yield a new category of devices — MIDs that will give consumers more bang for the buck. Such devices will be capable of not only fitting in a purse or pocket but also providing Web, location-based services, e-mail, video and music photos tailored to all applications. In addition, in all likelihood they will take on the form of media tablets, clamshell (pretty much a power-packed flip phone), and e-Reader. The e-Reader is a device made by Nintendo for its Game Boy Advance portable video game system. It has an LED scanner that reads "e-Reader Cards" and paper cards with specially encoded data printed on them.

Collaboration between industries with a focused vision (this would entail standard components, standard operating systems and a large application developer network) is needed. As of now, both PC and wireless industries have different visions for MIDs. The OC industry shapes best approaches for open application architecture, and the wireless industry has a lock on the right economic model to offer ubiquitous access.

Successful MIDs will feature the ability to run any application, an all-day battery life, the ability to provide a quality mobile Internet experience, media playback, and be cheap, ubiquitous, and provide a high-speed network and more!

Craig Mathias, the founder of the wireless advisory firm Farpoint Group, predicts that next-generation handsets will include cellular and Wi-Fi functionality and provide increased integration between enterprise voice and data networks, a minimized need to carry a second personal handset, the ability to provide still photos and video, and timely access to information. He also predicts a trend away from Palm OS and to Windows Mobile.

Per Benjamin Gray, laptop growth is projected to rise between 30 to 50 percent by 2010. Smartphone growth is also predicted to be significant over the next 10 years, and ultra-light laptops are poised to grow significantly within the next three to four years. PDA and mobile phone growth is on the decline.

Denise Pappalardo, a senior editor covering service providers at Network World Inc., predicts that worldwide shipments of mobile devices will experience a compound growth rate of 54 percent between 2007 and 2011, with 82 million devices in use. Devices include smartphones, PDAs, and BlackBerrys with, according to the global market research intelligence firm IDC, about 9.6 million already in use as of May 2007. Growth markets for corporate mobile devices include parts of the Asia-Pacific region, Latin America and Eastern Europe. Global adoption will be enhanced, given more flexible connectivity options and reduced spending on telecommunications.

Conclusion

While there is a plethora of mobile devices available to mobile workforces, enterprises need to select software and hardware that is an appropriate fit for their organization's infrastructure. Products chosen must ensure that security is not breached, workers are not frustrated accessing enterprise applications, and the suite of management software selected enables easy support of such devices from remote locations.

Future considerations entail increased capacity for speed of broadband connectivity; a blurring of the lines between media such as TV sets, radios, Internet and telephones; and improved technology in mobile networking

Take the time to investigate where your employer stands with regard to the support for enterprise mobile devices and how such devices can enhance your productivity. ■

References

Anonymous."Mobility Management Causing Concern." *Communications News* Dec. 2007: 6.

Gray, B. Forrester."Tech Radar: Enterprise-Class Mobile Devices and Management Solutions." Forrester Research Inc. Accessed Jan. 29, 2008: www. Forrester.com.

Jackson, P, Schadler, T., Golvin, C.S., and Menke, L."Defining Mobile Internet Devices." Forrester Research Inc. Accessed Jan. 29, 2008: www. Forrester.com.

Mathias, C.J.,"New Tools for Enterprise Mobility." *Business Communications Review* Mar. 2006: 44-47.

Pappalardo, D."Mobile Device Use Surges." May 2007 Study. Network World Inc. Accessed Jan. 29, 2008 www.networkworld.com

Shaw, K."Cool Tools." Network World Inc. Accessed Jan. 29, 2008 www.networkworld.com.

Simmons, R."How to Manage a Mobile Workforce Through Skill and Technology." Reed Business Information Ltd. Accessed Jan. 29, 2008: www.PersonnelToday.com.

Talbot, B."Are You in Control?". *Communications News* Nov. 2007: 24.

Beware of Phishing Expeditions

by Celeste Allen, CPCU, CLU, ChFC, FLMI

Phishers are Internet pirates and scam artists who use e-mail, spyware, search engines, cyber sources and programs that trawl the Internet. Using these methods, phishers can develop profiled lists of targets. Phishing occurs when a sender poses as a company to induce users to share personal or account information for fraudulent purposes. Users can click on a link that will allow someone else to control their machine. Unfortunately, prosecution of this form of cyber crime is hampered by legislatures which struggle to define and prosecute cyber crimes, the expense of tracking phishers who reside and operate in foreign countries, and the lack of a software solution that can completely filter data transmission.

Ira Winkler, the author of *Spies Among Us*, reports that U.S. Corporations lose approximately $300 billion a year due to cracking, hacking, physical security breaches and more. Access to corporate networks sometimes can be obtained simply by requesting a new username and password by posing as a remote worker. The SANS Institute, an information security research and education organization, coined the term "spear-phishing" for instances where individual employees are sent e-mail messages that appear to come from individuals in authority within the company requesting specific information. These attempts can be thwarted by providing employees with information on social engineering and how to detect and report same. The SANS Institute is in favor of running mock phishing attempts as a means to enhance awareness.

In one of his *NetworkWorld* columns, **Andreas Antonopoulos** shares a tale of a phishing attack where CEOs, on the pretext of responding to a federal grand jury subpoena, were lured to a site with malicious software. He suggests that corporations attempt to take a proactive stance but cautions them against developing generic security-prepared programs, as most conventional strategies view attacks from a two-dimensional perspective. This is problematic because attacks that fall within technology-hacking or social-engineering veins have an attack space that "stretches out to infinity."

I'm sure most of you have received an e-mail from PayPal regarding the updating of account information. Chances are that e-mail was part of a scam. Writing for *InformationWeek*, **Tim Wilson** notes that fake messages from PayPal and eBay make up more than half of spam and refers to it as "phishmail." PayPal "signs" its e-mail by using DomainKeys and Sender Policy Framework (SPF) to drop all e-mails that are not verified as officially coming from the company. DomainKeys has been tested on Yahoo since October of 2007 and has resulted in 50 million messages having been blocked, thus lessening use of Yahoo Mail by phishers. PayPal will expand efforts to block phishing sites using SPF and Extended Validation Secure Socket Layer (EVSSL).

DomainKeys is a system used to authenticate e-mail by verifying the DSN domain of an e-mail sender, and its specifications have been used to develop an enhanced protocol called DomainKeys Identified Mail (DKIM). An evaluation takes place as to whether or not a message should be trusted for delivery. Spammers and phishers forge sender addresses. SPF permits an organization to determine which machines are authorized to transmit e-mail for that domain. EVSSL allows users to see information about the owner of the Web site and trust that they're connecting to the right one. EVSSL certificates are issued to businesses that complete a documentation process. Microsoft's Internet Explorer 7 recognizes EV certificates for businesses that have completed the process — the address bar is colored green upon recognition. Microsoft has developed software specifically for law enforcement to help track down phishers and to enable people from different organizations to work together to solve crimes.

I recently accessed my bank account online and received a useform, purportedly from my bank. When the link within the request was launched, I noticed UK in the URL. I uttered a loud "hmmmm" and went to the bank's Web site to learn how to report the incident. I forwarded the questionable e-mail to the bank. Alertness, education, caution, and reporting the incident were simple tools I used to fight a tiny wave of cyber crime!

We should take the time to investigate and report attempts to access our bank and credit card information. Protection can lie in the simple act of deleting e-mail when you are not sure of the sender. We should have the same regard for protection of personal information as we do for protection of personal property and valuable assets. ■

References

Antonopoulos, A. "Attackers Are Thinking Outside The Box." *Network World* Apr. 2008: 17.

Brandel, M. "How to Spot a Spy." *Computerworld* Apr. 2008: 36, 38.

Gohring, N., McMillian, R. "Microsoft's Efforts to Police the 'Net." *Network World* May 2008: 12.

Liebesfeld, J., Liebesfeld, T.M. "Phishing Isn't Fishing." *Security* May 2008: 78-79: www.Microsoft.com/Windows/products.

Wilson, T. "Phishing For Answers." *InformationWeek* Apr. 2008: 20.

Wikipedia. Wikimedia Foundation Inc. Various: www.wikipedia.org.

Just When You Thought Your Data Was Secure

by Celeste Allen, CPCU, CLU, ChFC, FLMI

I'm sure the vast majority of you subscribe to some sort of security service and have gone to great lengths to encrypt access to, and key data on, your machines. *The New York Times*, in a February 2008 article, reported that a research group at Princeton University, consisting of five graduate students and three independent security consultants, discovered a means to capture encrypted information stored on computer hard disks. After reviewing a technical paper by a Stanford group addressing the persistence of data in memory, the Princeton group decided to assess the vulnerability of encrypted data.

There is a longstanding assumption that when the electrical power of a computer is shut off, data temporarily held on dynamic random-access memory (DRAM) chips, which includes data-scrambling algorithms, disappears. The Princeton group chilled the chips using an inexpensive can of air and discovered that information is retained and easily read. Retention of this information for several hours was achieved using liquid nitrogen (–196 degrees C). Special pattern-recognition software, developed by the group, and special utilities within Windows, Macintosh and Linux operating systems were used.

Per John Markoff, the article's author, both Microsoft and Apple ship their operating systems with encryption files turned off and leave it to the customer to turn on this feature. OK, get thee to thy computer to turn this on! Dismay not, as the retention techniques could not be carried out remotely and additional hardware security can be obtained by purchasing secure cards or a special USB hardware key. The research group could not access encrypted data when advanced modes of security were in place.

The research findings reveal vulnerability in "trusted computing" hardware, which is an industry standard approach and assumed to be a means to increase the security on modern personal computers. This newfound vulnerability, although

frightening, poses an opportunity to assess how to further strengthen security on our hard drives. Keep current on threats to your computer hardware and invest in appropriate measures to keep your data secure. ■

References

Markoff, J. "Researchers Find Way to Steal Encrypted Data." *The New York Times* 22 Feb. 2008. Accessed Feb. 22, 2008, at www.nytimes.com/2008/02/22/technology/22chip.html. by Bob Siems.

Plan to Attend

April 21–25, 2009 • Phoenix, Ariz.

CPCU Society's 2009 Leadership Summit

Witness Leadership in Action!

Plan to be a part of this distinguished gathering of CPCU Society leaders and insurance industry professionals. Open to all volunteer leaders.

This unique event will feature:

- Society business meetings.
- A leadership development schedule with greater flexibility and convenience.
- Specialized chapter leader workshops.
- CPCU Society Center for Leadership courses, including courses designed for chapters and interest group leaders. Open to all Society members.

Visit www.cpcusociety.org in early 2009 for the latest information.

Cutting Edge
is published four times a year by and for the members of the Information Technology Interest Group of the CPCU Society.
http://infotech.cpcusociety.org

Information Technology Interest Group Chairman
David L. Mowrer, CPCU, CLU, ChFC, AIT, ARM, AIM
State Farm Insurance
E-mail: david.mowrer.apxd@statefarm.com

***Cutting Edge* Editor**
Celeste Allen, CPCU, CLU, ChFC, FLMI
State Farm Group
E-mail: celeste.allen.aaiy@statefarm.com

Director of Program Content and Interest Groups
John Kelly, CPCU, AIT
CPCU Society

Managing Editor
Mary Friedberg
CPCU Society

Associate Editor
Carole Roinestad
CPCU Society

Design/Production Manager
Joan Satchell
CPCU Society

CPCU Society
720 Providence Road
Malvern, PA 19355
(800) 932-CPCU
www.cpcusociety.org

Cutting Edge
Volume 15 Number 2 September 2008