

# IT update

Digitize the Depot

## What's Inside

### About IT

- Store Walks
- Project Server Available
- IT Idol Event

### Human Resources

- Situational Leadership
- New Manager On-Boarding

### Technology

- TechBridge
- Security Terms

### Recognition

- Pillars of Excellence
- Service Anniversary Celebration
- Leadership Profile - Dan Nicklen

## Enhanced Pillars of Excellence Program

The Pillars of Excellence program provides all IT associates with a means to recognize peers and co-workers for the outstanding work and/or deeds they have done that represent The Home Depot's core values. "We began the Pillars of Excellence program a little more than three years ago," said Dave Kardesh, vice president, IT Corporate Systems. "The POE committee wanted to make sure the program was meeting the expectations of the IT associates, so we did a survey to see what was working and what needed changed. Overall, most associates we surveyed really liked the program and felt it was positive, important and effective. The one thing that stood out the most was to improve the nomination process. I am pleased to let you know we've done just that and added a few enhancements."

All Pillars of Excellence monthly winners will be honored at an annual breakfast celebration where our top leaders will recognize their efforts. So, nominate the IT associates or teams you see going above & beyond. Your recognition of their hard work will be greatly appreciated.

Look for the details about the Pillars of Excellence recognition program on DEPOTech. Monthly winners will be highlighted in each issue of the *IT Update* newsletter.



Continued on page 2

## TechBridge Sponsors Reach Beyond



Source: TechLINKS, The Guide to Technology in Georgia, Q3-07

The seventh annual Digital Ball®, presented by Accenture, was a tremendous success. On Saturday, May 5, 2007, more than 1,170 business, technology and nonprofit leaders enjoyed a gala evening of dinner, dancing and visually stunning performances. The event, themed *Voltaire, Reach Beyond*, featured 97 corporate sponsors and generated more than \$1 million in cash and in-kind donations to continue the TechBridge mission - to put technology know-how in the hands of nonprofits throughout our community.

The 2007 Digital Ball was co-chaired by Kristin Kirkconnell, SVP and CIO, AGL Resources and John Seral, VP & CIO, GE Infrastructure. Speaking of his involvement in TechBridge, Seral says, "Community involvement is key to business success and TechBridge has become a focal point for community service activities for technology professionals. It is an honor to be heading up this effort, and I call upon all of Atlanta's technology leaders to join us in ensuring that the Digital Ball continues its track record of success."



L to R: Steve Linowes, CEO, Damballa, Inc. and TechBridge Co-Founder; Dave Kardesh, IT VP; Faith Bridges, IT Project Analyst; Doug Pisik, Sr. Project Manger; Jennifer Higgins, Director of Outreach, TechBridge

TechBridge, a nonprofit organization, delivers critical technology services and solutions to Georgia's nonprofit community. The Home Depot and IT contribute volunteer hours by participating in TechBridge's Corporate Partner Program. If you are interested in volunteering to this worthy cause, contact Faith Bridges, THD/TechBridge Volunteer Coordinator, at ext. 13053 or [faith\\_bridges@homedepot.com](mailto:faith_bridges@homedepot.com).

## Be "In the Know" with Common Security Terms:

**Biometrics** - the study of methods for uniquely recognizing humans based upon one or more intrinsic physical or behavioral traits.

**Botnet** - a group of compromised computers used without the owners' knowledge by Internet criminals to send spam, viruses, or launch DDoS attacks.

**DDoS (Distributed Denial of Service)** - online attackers use multiple compromised computers to send messages to a target system such as an e-commerce site, forcing it to shut down and preventing legitimate users from accessing the site.

**DMZ (Demilitarized Zone)** - a sub-network between a company's private network and the external public network, where organizations often place their Web servers.

**Exploit** - an attack on a computer system that takes advantage of vulnerability on the system.

**HIDS/NIDS (Host Intrusion Detection Systems/Network Intrusion Detection Systems)** - HIDS are installed on individual systems to detect changes or attacks. NIDS monitor network traffic for potential attacks.

**PCI (Payment Card Industry) Data Security Standard** - standard created by the Credit Card industry to use as guidelines for organizations accepting credit cards. There are 12 functional areas described in the standards.

**Penetration Test** - testing the security of a system or network by trying to break its controls and gain access.

**Port Scan** - an attacker sends a series of messages to a computer to figure out which network services it is running in order to probe these services for vulnerabilities. Each service is associated with a port number.

**Rootkit** - a collection of programs that provides administrator-level access to a computer. An attacker that breaks through the user-access controls of a computer can install a rootkit, which can hide the intrusion and provide privileged access.

**Script kiddie** - less skilled hacker; typically uses existing programs and scripts to launch attacks.

**Security token (sometimes referred to as a hardware token, authentication token or cryptographic token)** - may be a physical device

that an authorized user of computer services is given to aid in authentication.

**SOX (Sarbanes Oxley)** - a law that established new or enhanced standards for all U.S. public company boards, management and public accounting firms. The Act contains 11 titles, or sections, ranging from additional Corporate Board responsibilities to criminal penalties, and requires the Securities and Exchange Commission (SEC) to implement rulings on requirements to comply with the new law.

**Spear phishing** - fraudulent e-mail that targets a specific organization and aims to fool the recipient into divulging confidential data. Generally, the message will appear to come from someone within the recipient's company, such as an IT administrator.

**Trojan horse** - a computer program that appears harmless but contains malicious code.

**Zero-day exploit** - an exploit that takes advantages of a vulnerability that isn't generally known until the exploit surfaces; consequently no patch is available.

These and other Security Policies, Practices and Standards can be found in DEPOTech > Team Spaces > Information Risk Management.