IT SECURITY REBOOT 2007

The end of yet another year sees in this final 2007 edition of SC Magazine our annual roundup of top thinkers, interesting happenings, business developments and criminal acts. With a little help from our Editorial Advisory Board members, we look to include in this issue a review of the past 12 months, highlighting who we think have been the most inspiring — yet perhaps somewhat overlooked — IT security luminaries, the business changes that impacted the industry landscape the most, the vulnerabilities and attacks that hit the corporate world the hardest, and today's more notorious cybercriminals. Finally, we've asked some experts to gaze into their crystal balls to tell us how they see next year playing out in the IT security industry.

TOP 5 INFLUENTIAL IT SECURITY THINKERS

Photo by Forrest MacCormack

KAREN EVANS

Age: 47

Occupation: Administrator for e-government and IT at the federal Office of Management and Budget

Personal: Married, two children

Recent accomplishments: Oversaw a memo mandating federal agencies establish a breach-notification policy and evaluate their use of Social Security numbers.

Awards: Distinguished Service Award from the Harvard Policy Group on Network-Enabled Services and Government; Security Leadership Award from the SANS Institute

If 2006 marked the year of the high-profile federal agency data breach, one could have predicted 2007 would be the year the feds tried to straighten out what seemed like a regular occurrence of lost personal information.

So naturally, the woman responsible for IT across the 26 cabinet-level federal agencies, Karen Evans, has been keeping busy this year. Evans, who carries the title of administrator for electronic government and information technology inside the White House's Office of Management and Budget (OMB), serves the CIO for the federal government.

The 47-year-old, now in her fifth year in the role, is optimistic about information protection, but she knows a lot of improvements need to be made.

"We have a lot out there," she says, matter-of-factly. "If you don't know your inventory, it's really hard to assess."

Evans has not been shy about assigning homework. Earlier this year, OMB issued a 22-page memo that directed federal agencies to review their use of Social Security numbers, implement user-awareness training requirements, and create a breach notification plan.

Known as M-07-16, the policy orders agencies to store the minimum number of personal records and to devise a plan to end the unnecessary use of Social Security numbers.

"SSNs should not be used as personal identifiers," Evans says. Still, she noted the numbers have value at some agencies and therefore must be stored and protected there. "In the case of government, we can't just shut down who you are."

Before M-07-16, OMB issued other directives, mandating such measures as two-factor authentication and encryption on all mobile devices.

Another milestone IT security accomplishment this year came when OMB announced that all agencies must transition to a common Microsoft operating system configuration, and all software vendors must configure their products to work with the new standard. Agencies have until February to comply.

"It raises the level of security," Evans says. "We have one configuration. It allows us to gain efficiencies from patch and configuration management. When you analyze these breaches, you realize what it comes down to is that a lot of these could be avoided if you have good configuration management and patch on time."

Alan Paller, director of research for the SANS Institute, says this undertaking is a perfect example of why Evans is the right person to lead federal information initiatives. The idea drew resistance from IT departments across government who claimed the standard configuration would break systems or not receive vendor support, he says.

"I know how many people fought her in doing it," he says. "She's the right character with the right experience to do that job. I despair that we'll never find another one like her. She's really the only person really high up in the administration of IT technology that's lived through a computer hacking," Paller says. "That was the real thing. They got in and we don't know who they are. That's a life-changing event."

As much as OMB is preparing to prevent breaches, they also want agencies to be able to strongly react when the inevitable happens.

The breach notification plan mandate is one example. Another example is two federal contracts — one for credit monitoring services, the other for risk analysis services — signed with vendors this year that will allow compromised agencies to immediately respond to data-loss incidents.

"They are tools that are ready to assist agencies ain responding to the incident," Evans says.

Evans also is immersed with driving agencies toward compliance with the *Federal Information Security Management Act of 2002 (FISMA)*. How well agencies meet the mandate determines their annual *FISMA* grades - a controversial report card that has cast a dark shadow on the federal government's security posture in recent years.

In June, Evans told the U.S. House Committee on Government Reform that progress is underway, but agencies continue to fall short in several key areas.

TOP 5 cyberattacks

1. The Storm Worm

What began as an email-spawned trojan attack using fake news stories to lure victims became the most widespread cyber-assault in recent memory. Still replicating, and exploiting a number of patched vulnerabilities, the botnet-fueled, socially engineered attack may make next year's list as well.

2. Estonia attacked via DDoS

Russian hackers were blamed for a politically motivated cyberattack on Estonian infrastructure. Comprised of nearly 130 unique DDoS attacks on Estonian websites, the attacks are believed to have been launched by Russians angry that Estonia's prime minister wanted to relocate a war memorial.

3. A Monster(.com) of an attack

Tens of thousands of users of Monster.com had their info stolen by a multi-layered attack on the website. Cyberattackers used credentials to access the site, then spread a trojan to capture data that was used to deliver spear phishing emails to job seekers, requesting financial details.

4. The Italian Job

Cyberattackers thought locally, using the MPACK web exploit toolkit, when creating a large-scale trojan attack that affected nearly 10,000 web pages. Called the Italian Job, because most of the pages were hosted in Italy, the trojan downloaded a keylogger designed to steal banking data.

5. Disabled firewall allows attack

Attackers infiltrated a server at the University of Colorado, Boulder, and exposed the personal information of 45,000 students. IT officials said the attackers were looking to use targeted PCs as part of a botnet, not purge sensitive information. The attack may have been stopped if a network firewall was enabled.

Photo courtesy of Monster.com

WINN SCHWARTAU

Age: 55

Occupation: Author; founder, SCIPP International; also founder of InfowarCon, NiceKids.Net and Interpact, Inc.

Personal: Married, two children

Recent accomplishments: Completing three separate books; still skiing

Awards: "Have a whole bunch in boxes. I don't hang them on the walls because I prefer pictures of the mountains to looking at awards."

Ask Winn Schwartau what first made him interested in end-user education and he'll immediately list two reasons — his children.

"It started back in the early 1990s, I guess Windows 3.1 more than anything, and then my kids were on it," he says. "My daughter was six years older than my son, and [they were using] the dial-up [connection]. And I wrote a book back then that morphed into *Internet and Computer Ethics for Kids*."

About 15 years — and numerous operating systems — later, the concept of user education, championed by author and consultant Schwartau, has given birth to a nonprofit organization providing cybersecurity certification to ordinary PC users.

SCIPP International (the acronym's meaning is unavailable) was formed by Schwartau with the help of an all-star roster of prominent IT security minds and uses the organization's SCIPP General Accepted Practices and an annual certification program to bring end-users up to date on threats and best practices.

The program is another instance of Schwartau, who gained acclaim in the 1990s for his books on cyber-warfare and future threats, playing a lead role in public advocacy of security issues, says Howard Schmidt, former White House cybersecurity adviser and (ISC)^2 security strategist.

"[End-user education] is one of the three legs of the stool. You have the hardware and software vendors building better products, the enterprise operators, and that third leg is the user and consumer space," Schmidt says. "He's looking for ways to solve the problems. A lot of people talk about the problems and complain, but he's been proactive in coming up with ways to solve the problems."

SCIPP International's genesis occurred at a trade show, Schwartau recalls.

"My career has been about awareness and getting people to think about things that they don't have to think about. And I was at a trade show in Washington, D.C. and I remember talking to a bunch of folks at (ISC)^2 about how security awareness is getting to be important, and what we really need to do is to get a certification going," he says. "Everybody said it was a great idea, but the question was, 'Who is going to take the lead?"

TOP 3 most important M&As

1. Cisco acquires IronPort, $830 MILLION

The networking giant picks up a leading spam and spyware defense provider. The acquisition represents a paradigm shift that would resonate throughout the year. Securing the data has become the top-of-mind priority.

2. IBM buys Watchfire, UNDISCLOSED

Big Blue strikes another key security deal. The purchase of Watchfire not only extends IBM's governance and risk management strategy to include quality and compliance testing, but it also validates the application security sector.

The organization faces daunting challenges. Schwartau, who fondly recalls arguing web addiction with Bill Gates and internet militarization and social dangers with Al Gore in the 1990s, says education also needs to reach hardware and software vendors, which are giving home and office end-users more technology than they need.

"Vendors provide them with an environment that will launch a space shuttle, so hopefully education will be two-fold over time," he says.

SCIPP has assembled an impressive list of officials and advisers from both the private and public sectors to create smarter, more security-savvy end-users. Sitting on the group's advisory board are Schmidt; Rob Pate, deputy director of outreach and awareness at the Department of Homeland Security's National Cyber Security Division; Stephen Carrick-Davies, CEO of Childnet International; and Stephen Katz, founder and president of Security Risk Solutions.

And that diversity of experience will come in handy. The group plans to issue distinct certifications for corporate and government employees and customers, as well as the self-employed and educators.

Schwartau, who compares IT security awareness in some schools to *Lord of the Flies*, envisions a world where training will make companies safer and help their bottom lines.

"I'll tell you what my hope is, and maybe it's fairly unrealistic considering how long things take in the real world. It's where employees can get certifications that would be able to reduce risk cost, insurance costs and, from a real dollars and cents perspective, the losses are much less internal than external," he says.

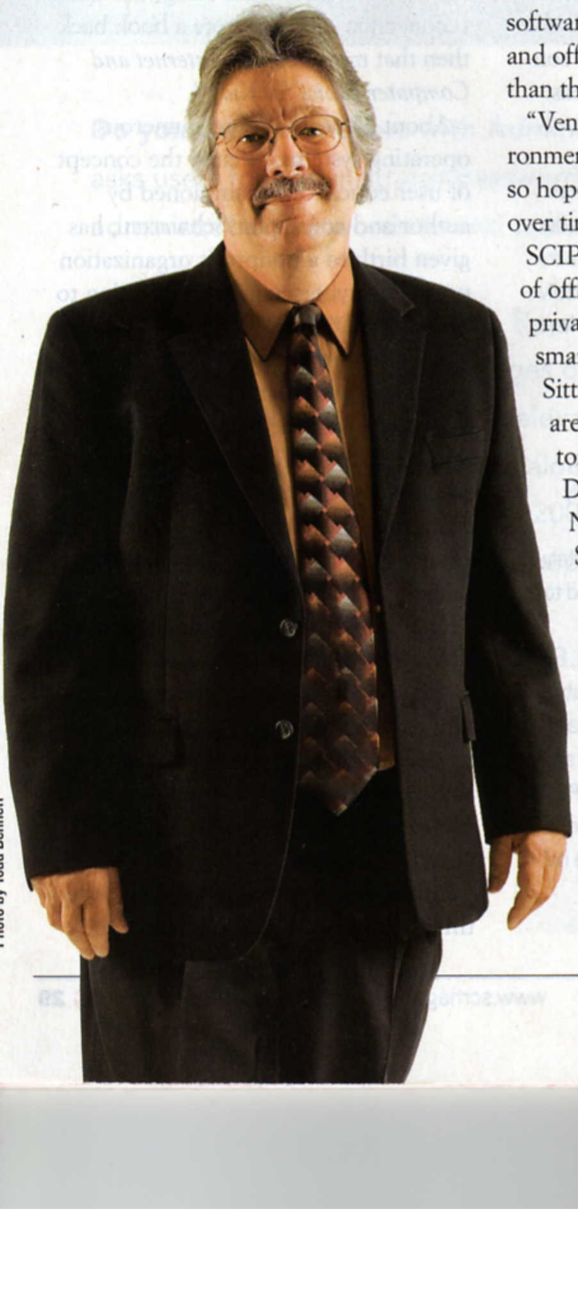


Photo by Todd Bennett

RANDY HILLMAN

Age: 43

Occupation: executive director, Alabama District Attorney's Association and the State Office of Prosecution Services

Personal: Married, three children

Recent accomplishments: Member of the Alabama Bar Association, the Shelby County Bar Association, and the Board of Directors for Owens House (Children's Advocacy Center)

When we last spoke with Randy Hillman (for the July cover story), the National Computer Forensic Institute (NCFI) was still in its formation stages. Construction on the center in Hoover, Ala., began last month and Hillman, who was instrumental in getting things going, projects completion in six months. By mid-May 2008, the 32,000 square foot center will be fully operational in its training of law enforce-

3. Symantec buys Vontu, $350 MILLION

symantec. A number of data-leak prevention (DLP) providers fell into the hands of general security players. DLP solutions have become one of the hottest new technologies as businesses place greater focus on defending against the insider threat.

ment personnel, judges, prosecutors and private sector employees in computer forensics. Hillman expects there to be between 280 to 300 people in the institute's first group. Approximately 1,000 people are envisioned to attend the NCFI each year.

Hillman, the executive director of the Alabama District Attorney's Association, says the NCFI was formed because police and law enforcement are poorly trained in IT security and computer crime.

"If you don't train prosecutors, then you're backing up [the dockets]," he says. "When you go to trial, if the judges don't understand the evidence, they could make their ruling based on a faulty understanding."

The NCFI, which will be annexed to the Hoover Public Safety Center, came into being after Hillman arranged for interested parties — including the U.S. Department of Homeland Security, the U.S. Secret Service, as well as Alabama state and local officials — to talk with each other about the need for a national cybercrimes training facility. The goal is to equip law enforcement with the sophisticated skills necessary to combat criminal computer activity.

Eric Zahren, a spokesman for the U.S. Secret Service, says it is very important to stay ahead of threats emerging in the arena of cybercrime, adding that the NCFI brings great value to local and state law enforcement personnel.

He credits Hillman with not only coming up with the idea of a national center to train law enforcement in computer forensics, but also in bringing substantial resources to the table to make it a reality.

The facility will include six classrooms, a computer forensic lab (with an advanced research and development area and an evidence vault), storage and server rooms, public education exhibition space and a conference room.

The NCFI is being funded though a cooperative effort by the U.S. Department of Homeland Security, the U.S. Secret Service, and Alabama state, county and local governments.

Zahren says 18 U.S. Secret Service personnel certified to the highest level of the agency's Electronic Crimes Special Agent Program (ECSAP) will act as instructors. The Alabama District Attorney's Association also will provide training.

Rep. Spencer Bachus, R-Ala., who helped procure $4 million to fund the start-up of the NCFI, acknowledged the need for such a facility in a statement: "Juries today demand scientific and forensic evidence. The number of phones, computers, blackberries, GPS units, and other devices from which information can be extracted is mushrooming. This information can be used to put identity thieves, child molesters, murderers, and even terrorists behind bars. But there is a bottleneck getting this valuable data into the courtroom. What we don't have is trained, qualified professionals to find, extract, analyze and preserve the data."

"Putting all the pieces in place was a chore, I promise you," says Hillman. But, he adds, it wasn't rocket science. "It was a matter of all the planets lining up. We put the people together and things started rolling quickly."

In addition to law enforcement and legal personnel, the private sector will benefit from the NCFI as well by attending classes, though at a cost.

"There are many times where the private sector needs a working relationship with law enforcement. They need to know who it is they should talk to before there is an emergency. They need to know how to handle evidence before we can get there."

Now that the hammers are pounding and the funding secured, Hillman will be relinquishing some of his duties at the NCFI, while still maintaing a supervisory role. He will also serve on the board of a 501(c)(3) foundation set up in parallel to keep things focused at the institute.

The foundation has big plans. It will host two national symposiums a year, form a think tank, produce publications, and establish a network to keep all who pass through the Institute connected.

Photo by Owen Stayner

ARI SCHWARTZ

Age: 36

Occupation: Deputy director, the Center for Democracy & Technology

Personal: Married, two children

Recent accomplishments: Formed the Anti-Spyware Coalition.

Awards: Won the Excellence in Public Policy Award at the 2006 RSA Conference.

No one understands better than Ari Schwartz the tenuous nature of online privacy.

"Individuals who want to protect themselves online today have a hard time doing it," says Schwartz, the deputy director of the Center for Democracy & Technology (CDT), a nonprofit organization fighting to ensure, among other things, that personal privacy rights aren't stomped on, especially in dealings online. And it's all that work now conducted via the internet that he believes makes people feel very vulnerable.

Schwartz, one of the leading experts on the issue of privacy on government websites, has worked to defend and enhance electronic privacy protections by promoting increased individual control over personal information. A former chair of the World Wide Web Consortium's Platform for Privacy Practices (P3P) Policy and Outreach Working Group (the standards-setting body for web technologies), Schwartz has testified before Congress and the White House on privacy issues.

He became involved in privacy issues in the early 1990s, when he saw that the web was a true democratic medium, and policy-makers in Washington needed to be made more aware of it.

Privacy and security are a major stumbling block in the potential of the web, he believes. "Because we don't know what's happening behind the scenes, there's a feeling of a lack of control that makes people feel that nothing they do online has protection."

Overcoming those kinds of issues is one of the key objectives of the CDT, he says.

"We try to work with companies that provide services, with policy-makers who make decisions about privacy policies, and with public interest groups to come up with consensus decisions in technology, in law and in public policy that gives consumers more control over the information they share online," he explains.

Right now, he says there's a dichotomy to our online existence: "We have different controls than we used to have. It's interesting, because in some ways, we have more control, in some ways less, and there's a feeling of a lack of control that comes from that."

Still, he thinks the internet community has a long way to go before consumers can feel truly safe online. For instance, there hasn't been a great deal of success in consumers feeling that their information is being treated with the respect they expect, and that they themselves have control of their own information.

"There are still companies out there with privacy policies that allow them to do whatever they want with personally identifying information, and we can't do anything about it," he says.

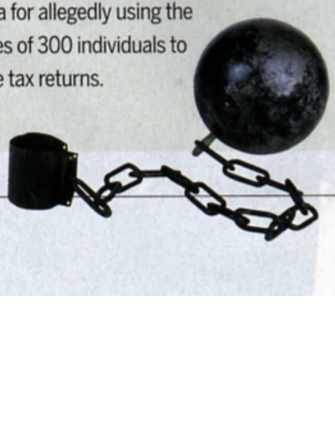
The bright spot, on the other hand, is in the fight against spyware, which Schwartz championed as the organizer of the Anti-Spyware Coalition.

Schwartz and the CDT have also worked to repeal the *Real ID Act of 2005*, which would create a backend database of personally identifiable information,

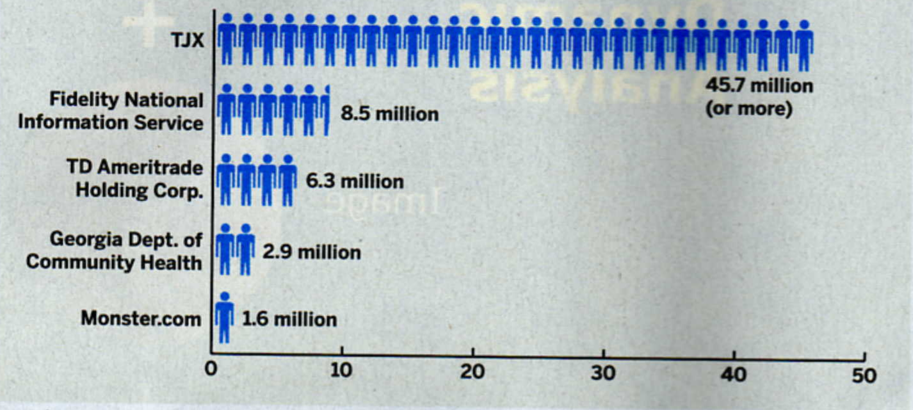
Photo by Forrest MacCormack

TOP 5
savvy criminals

1. **"Spam King" Robert Soloway** faces 35 charges, including email fraud, identity theft and money laundering.
2. **Leo Kuvayev, aka BadCow**, a Russian/American spammer believed to be behind numerous phishing and mule-recruiting sites hosted on botnets.
3. **James Brewer** is accused of infecting over 10,000 computers with viruses.
4. **Li Jun** and three other 20-somethings stand accused of writing the notorious virus "Xiongmao Shaoxiang," causing damage to millions of computer users.
5. **Ervin Patrick Somba** was arrested in Kenya for allegedly using the identities of 300 individuals to file false tax returns.



TOP 5 data breaches



Source: SC Magazine

and he's involved in other legislation regarding consumer rights in the ID theft area, says Timothy D. Sparapani, senior legislative counsel with the American Civil Liberties Union (ACLU) in Washington, D.C.

"He's widely respected for his balanced and very careful analysis of new technologies and of the questions they raise," Sparapani says. What drives Schwartz, according to Sparapani, is his natural curiosity about new technologies and to think not just about how they may facilitate our work and business, but how they change our culture.

Leslie Harris, the CDT's president and chief executive officer, offers another look into what motivates Schwartz.

"What drives Ari is a passion for the issues we work on — the solid belief that there are practical solutions, and that people will come together and find them," she says. "Ari is not an idealist, he's not a lone ranger, he's not a person who thinks that he knows all the answers to complex problems. He's looking for real privacy and security solutions in the real world. Ari understands that the best answers are found when people are consulted, when there's dialog between everyone involved in an issue."

SUZANNE HALL

Age: 40

Occupation: Former director of IT operations and security, AARP; she just recently became CIO of Major League Baseball's Washington Nationals, as well as its parent company, Lerner Enterprises, a real estate firm

Personal: Married, two children

Recent accomplishments: Implementation of an ID and access management platform

Awards: Named "One to Watch" by the 2006 Executive Women's Forum; Information Security Executives Mid-Atlantic People's Choice Winner in 2006

Let the AARP's Suzanne Hall ruminate a little bit about her job, and inevitably the conversation will turn to the fiduciary bottom line — lending long-term fiscal value to this, applying business objectives to that.

Such talk is common for the calls with analysts and the pages of *The Wall Street Journal*, but certainly not expected to be regular rhetoric for the director of IT operations and security at a nonprofit.

Folks like Hall are supposed to be concerned only with bits and bytes, trojans and botnets, uninformed employees and unpatched PCs. And they are supposed to be resigned to the fact that nonprofits are not wealthy, heavily regulated Wall Street investment firms — meaning financial priorities rest in places other than IT, such as keeping the doors open for business. Times have changed.

Consider Hall the poster child of the new-age CISO. The 40-year-old, who began her career at AARP in the internal audit department a decade ago, feels right at home in the board room. She has long recognized that business acumen and strong communication skills are what will separate a healthy IT budget from a bare-bones spending plan.

"It's important when you run security to understand the technology," she says. "You can't get fully away from that. You need to understand your infrastructure, your applications, your data. But at the end of the day, it's a business issue, and if you can't articulate what it is that you're doing as far as value to the enterprise, you're going to be left behind."

That mentality was clearly evident this year when she began jockeying for funding for the organization's first true identity and access management platform to support the new Web 2.0 framework.

When Hall initially was selling the idea to AARP's board of directors, she didn't talk a lot about the privacy ramifications. Instead, she gushed about the customer service benefits. She mentioned how the framework will allow the organization to create a unique identifier for each member as they interact online, helping AARP better understand their clients' interests.

At AARP, a 35 million member organization, Hall had to really be on her game. The 50-year-old foundation has always taken great pride in maintaining its members' trust. But as a nonprofit, AARP has few guidelines to follow when it comes to documenting IT security controls. Hall doesn't have the luxury of using that comply-or-go-to-jail tactic. She has to be a saleswoman and talk in terms that board members can understand: dollars and cents.

TOP 5 responses to Live Free or Die Hard

1. Apple vs. the security community
The "Mac guy" from Apple's hysterical Mac vs. PC commercials was the guy chosen to play the ace security researcher? Hackers might have chosen someone else.

2. Hopefully it's not that easy

The villain is said to have taken over NORAD's system using only a laptop. At least we know that screenwriters are paying attention to FISMA grades.

3. Critical infrastructure
Power stations, traffic systems and a fighter jet are all hacked during the plot. Who says SCADA issues don't get enough attention?

4. It's not really like that, is it?
Talk about stereotyping. Clerks director Kevin Smith cameos as a hacker working out of his mother's basement.

5. Security researcher/superhero
Actor Justin Long's character goes from making illegal downloads to stopping a cyberattack, saving the country's infrastructure and maybe getting the girl. This just in: security researchers are the new James Bond.

Unimedia/Fox Films

"In my mind, if you want to continue to get to the board, you've got to bring value to the table," she says.

When she emerged from the internal audit department at AARP, Hall achieved immediate success. She led the creation of a vetting process for third-party contractors, while building the organization's first security program. In both cases, she sold the ideas by explaining how they will benefit the organization's financial health.

Her audit background may be shunned by IT purists, but it immediately came in handy for Hall.

"I knew what the board calendar was, so I knew when the board met," she recalls. "I knew what topics were going to be top-of-mind for the board. I tied my proposals with what else they were dealing with during that session."

Matt Mitchell, AARP's chief information officer, says Hall's managerial and leadership traits caught the eye of execs. For example, when AARP Financial, the organization's financial arm, was being created, Hall did not just lead the security technology end but also was tapped to assist with the business planning.

"The most successful IT folks are people that really understand business operations," Mitchell says. "Her skill set is seen as being equal among the business operators."

Nowadays, AARP is extending an internal identity program to its 2,300 employees across the United States and countless other partners. The nonprofit plans to transition to a single sign-on platform for employee end-users and, eventually, a federated framework for its partners, which includes health insurance providers, financial organizations and technology companies.

For Hall's (now former) IT staff, the project will mean a significant reduction in help desk calls and, with fewer passwords floating around, enhanced security.

But the board's blessing came when she promised how the project will ultimately lead to the delivery of better services and save the organization money.

"If I can reduce the number of password resets, I'm going to save AARP and my own department the budget money," she says. "I can start spending money on a lot of things that lend long-term value to AARP, other than password resets. I don't think there's any employee at AARP that wouldn't want fewer IDs and passwords."

To succeed, Hall does not solely rely on impressing the board, but also building a rapport with other departments within AARP, namely the membership, audit, general counsel, accounting, financial management and human resources teams, she says. If Hall has learned anything, it is that collaboration and trust are key.

"To build a program that's going to last, you need buy-in from a large group of business partners across the enterprise," Hall says. ■

Click on www.scmagazineus.com for longer versions of these profiles, other industry players we feel deserve honorable mentions, as well as more Top 5 lists.

Photo by Forrest MacCormack