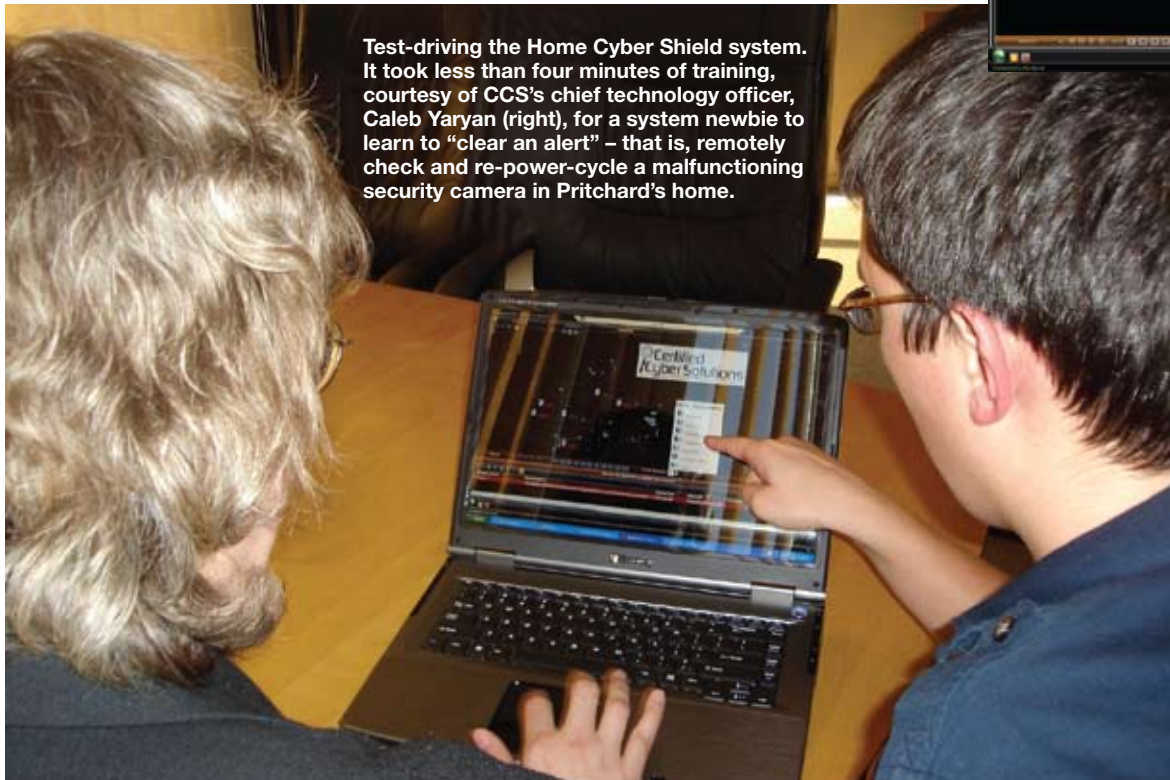


Worry-free



Test-driving the Home Cyber Shield system. It took less than four minutes of training, courtesy of CCS's chief technology officer, Caleb Yaryan (right), for a system newbie to learn to “clear an alert” – that is, remotely check and re-power-cycle a malfunctioning security camera in Pritchard’s home.

IP

Certified Cyber Solutions’ elegant residential network security fix

D

By Nancy Klosek

otting the ‘i’s and crossing the ‘t’s is de rigueur for the best integration companies in our business. After all, you employ checks and balances in every vulnerable phase of your company—background checks, vehicle insurance and your phone number on the sides of the van so your guys know they’ll get busted for driving like madmen. You may even use outside CPAs to double-check your in-house accounting staff.

But in today’s home, where IP-addressable products are ubiquitous, at the end of the day, there are no checks and balances

currently for CEDIA dealers to employ, and they are exposing their clients to the possibility of network intrusions and cyber crime that could easily morph into a negligent liability nightmare for the business and its employees.

That reality was illuminated by a series of events that, three years ago, confronted Russ Pritchard, a founding dealer member of CEDIA and proprietor

for more than 25 years of Charleston, S.C.’s award-winning Audio Warehouse.

“One Saturday night at around 10 p.m., I was called by a client who demanded a list of my employees and copies of their background searches we have on file. Some sensitive information had been leaked to the Internet and since my guys had access to his system, they were the first to be blamed. As it turned out, it ►

THE FOUR PILLARS OF HTSA

- IDEA & INFORMATION SHARING
- RELATIONSHIP BUILDING
- ECONOMY OF SCALE IN MARKETING
- PROGRAM ADVANTAGES

Find out more about
the HTSA team.

Visit HTSA.com today.



HOME THEATER SPECIALISTS OF AMERICA

www.HTSA.com

Cyber Security

was not our employees who were at fault; it was someone who worked for the client and had been fired,” says Pritchard.

Even so, this episode—one of a series touching upon residential network security—brought into sharp focus for him the need to shield his employees and his company from the potential for undeserved blame, should a client’s privacy ever be breached in any manner through IP-addressable access.

“It made me realize the exposure and liability both myself and my employees have, just because we have access,” he explains.

And that is how Certified Cyber Solutions, Inc. (CCS), a new company founded by Pritchard, its CEO, and Doug Weinstein, its president, came to be.

Fringe Benefits Beyond Security

CCS exists to provide CEDIA dealers with the ability, in-house, to monitor their clients’ networks and the devices that reside on them, to ensure against cyber security intrusions and grant permissible access to the network for normal remote servicing. But the benefits beyond that are manifold for integrators, says Pritchard.

“This is a product that was born from the field,” he says. “Then, the proactive problem-solving technology that was researched and fine-tuned for the system kept expanding. And we developed new benefits the dealer could exploit to gain an incredible competitive edge in the marketplace.”

“These extend well beyond cyber security, into areas like advanced performance monitoring and system troubleshooting,” Weinstein adds. “All of it is done in-house, instead of the commercial model of network monitoring where the CEDIA dealer is trusting a third-party vendor



The Home Cyber Shield H-100, a single-rack-space server, deployed at the Kiawah Island home

with the system. We project that an integrator’s top programming staff will save one or two hours a week, not to mention a ton of unnecessary truck rolls,” he points out.

“We all have these events that are commonly dealt with in the service space,” concurs Pritchard. “Having to yank a guy off a billable job to go over and unplug and then plug a modem back in—that’s not billable.”

“Ninety percent of problems that occur in these systems are no-brainers that drain a company’s resources and dramatically impact client satisfaction. If you can fix those without the client even knowing that a problem happened, everyone’s happy,” says Weinstein. “And you protect your company, knowing that your field technician cleared an alert, but never had direct configurable control of any product. It’s safe and secure.”

Another plus: any monitoring that results in a system fix is tracked and recorded, and a monthly statement can be generated and presented to the homeowner.

“Dealers are able to give clients network security and an enhanced, concierge-level service,” he adds. “Because the events and service in this recurring revenue model are documented, the client not only gets peace of mind from a security and performance-monitoring perspective, but it’s in a measurable and justifiable package, so the client understands the value of what they are paying

Continued on page 50 ▶

5 Questions Integrators Should Ask Themselves about Residential Cyber Security

- 1: How do you safeguard on-site and remote access to your clients’ networks by current and past employees?
- 2: How do you safeguard your client, your staff and your company from the risk of unauthorized access to client networks and their private content?
- 3: How do you safeguard system performance and user satisfaction from common service interruptions or system failures before they impact your client?
- 4: How do you safeguard your company from the growth in IP-addressable devices, network-related issues and the soaring costs of IT support?
- 5: Do you see the need for residential network security, and a single solution to address these issues?

(For the answers, check out www.CertifiedCyberSolutions.com/Learn)

Continued from page 42

for every month.”

The system, dubbed Home Cyber Shield, consists of two hardware models—the D-500 server, outfitted with dual 500GB hot-swappable drives for system redundancy, in place at the integrator’s establishment, and the H-100, a single-rack-space server with dual 250GB hot-swappable drives for system redundancy, which is installed at the client’s home. Its base network-monitoring software has been developed with a systems security and engineering company that works with the military.

“The basic technology has been in the field for eight years,” explains Pritchard, “but our proprietary technology makes it unique. With this system, we’re not beta-testing dealers. It’s very elegant, with robust, reliable software and battle-tested servers. My integration firm has had systems deployed for some time.”

The proprietary element of the software is a password management system (SAM, or Secure Access Manager) that authenticates the dealer’s technician with the IP devices. The technician never needs to know the IP address or individual device username and password; SAM takes care of that. Techs cannot access networks or devices on their own, so if they are not authenticated by SAM, they can’t gain access to the client’s systems or private information. Levels of access are set by the dealer for each assigned user and password, and should an employee leave the company, his or her permission can easily be switched off, maintaining the security of the client’s systems and



Russ Pritchard and Doug Weinstein

avoiding dealer liability. The system also keeps track of who accessed what, and when.

“By keeping track of user activity with a log, it gives people a level of accountability; it leaves a footprint,” says Weinstein. “At the administrator level, you give maximum access to the network and the devices residing on the network. At the field technician level, access is customizable to the tasks appropriate to the tech’s role within the company. It is configurable up, down, left to right in any number of configurations, depending on the dealer, the client, the residence—totally customizable.”

Ease of Use & Cost Savings

Best of all, says Pritchard: the system is a breeze to use. “Its software was designed to be point-and-click. It does all the heavy lifting and, in fact, is tailored to the non-IT person. Now that we can assign any or all technicians the ability to clear those 90 percent of routine IP lockup issues, we have dramatically improved our bench strength and our operating costs by freeing up the programmer, who generally deals with these interruptions. And it’s secure.”

The system monitors product performance as well as system-affecting elements such as bandwidth usage levels, and when it detects an anomaly of any sort, it sends out an email or text message “alert” to the integrator or his field technician that there is a problem needing to be investigated. The designated troubleshooter on staff—at the job site, at the dealer location, or from his backyard on a Saturday afternoon—can then log into the system using his or her unique password, with either a PC or a Mac, view only what is neces-

sary to address the issue on an uncomplicated “dashboard” screen, check the problem and on many occasions, do a simple power recycle, which effectively solves the problem and clears the alert.

Cyber Solutions’ first dealer, Audio Warehouse, is currently monitoring IP installations at multiple locations up and down the East Coast and in the Caribbean. One such location we visited, an exclusive residence on Kiawah Island, not far from CCS’s headquarters, has 46 IP-addressable devices which are being successfully monitored, including an AMX control system, Kaleidescape and Sirius XM servers, an Internet modem, wireless access points, a bank of satellite receivers and a Lutron lighting control system, to name a few.

Audio Warehouse offers its clients package pricing on the CCS system that includes secure monitoring and 10 hours of remote service per month on an unlimited number of IP devices, but Pritchard emphasizes that dealers could, as an example, bundle the hardware into their own unique service plan and build out pricing in the recurring-revenue model “to suit whatever is in the home, or to suit what is important to the client.”

Weinstein says that the monitoring model that CCS has established within the residential installation space is one that readily translates to other marketplaces and applications, and strengthens the dealer position for involvement in energy management and in the burgeoning aging-in-place market sector, where personal medical information fed over IP-addressable systems could pose serious breach-of-privacy issues—not to mention the value of monitoring medical device performance.

But for now, the focus is squarely on residential systems and will move to dealer training initiatives at the administrative and field technician levels. The company is in the process of developing on-line videos and webinars as part of its outreach education and training, says Weinstein.

“Our goal,” says Pritchard, “is to make it easy for dealers to bring it in and implement it. It’s about security and reliability—and that needs to be our culture. In fact, from a negligent liability issue, it is a CEDIA-wide fundamental responsibility for both the dealer and manufacturer to proactively ensure client privacy since we’re the ones putting in the networked systems and opening up the doors to possible cyber crime activity in the first place.” **CR**



The study in a Kiawah Island home equipped with the Home Cyber Shield monitors 46 IP-addressable devices, including an AMX control system.

Custom Retailer, November 2009; Volume 8, Number 11. Custom Retailer (US ISSN 1541-7735) (USPS 0023-295) is published monthly by North American Publishing Co., 1500 Spring Garden St., 12th floor, Philadelphia, PA 19130-4094 (215) 238-5300. Periodicals postage paid at Philadelphia, PA and at additional mailing offices. POSTMASTER: Send address changes to Custom Retailer Subscription Services Dept., P.O. Box 1090, Skokie, IL 60076-8090. SUBSCRIPTIONS: Free to qualified recipients. All others, U.S. 1 year \$65; 2 yrs. \$110; 3 years \$160; Canada, 1 year \$85; All other countries, one year air mail \$110. Back issues and single copies, when available, mailed by publisher, for \$10 each. Selected articles from North American Publishing Company (NAPCO) magazines are available for research and retrieval from electronic databases and search services exclusively through ProQuest. For information on availability, call (800) 521-0600 or visit the ProQuest Web site at proquest.com. Microform is available from National Archive Publishing. (800) 420-6272. Authorization to photocopy articles for internal corporate, personal or instructional use may be obtained from Copyright Clearance Center (CCC) at (978) 750-8400. Articles may not be reprinted without publisher’s permission. For reprint information, contact Kathy Kling at k.kling@napco.com Custom Retailer Reprint Services or call, (215) 238-5361. All rights are strictly reserved, and reproduction in whole or in part is expressly prohibited without prior written permission from the publisher. Copyright 2008. Printed in the U.S.A. Byline contributors’ views should not be construed as representing the opinion of the publisher.