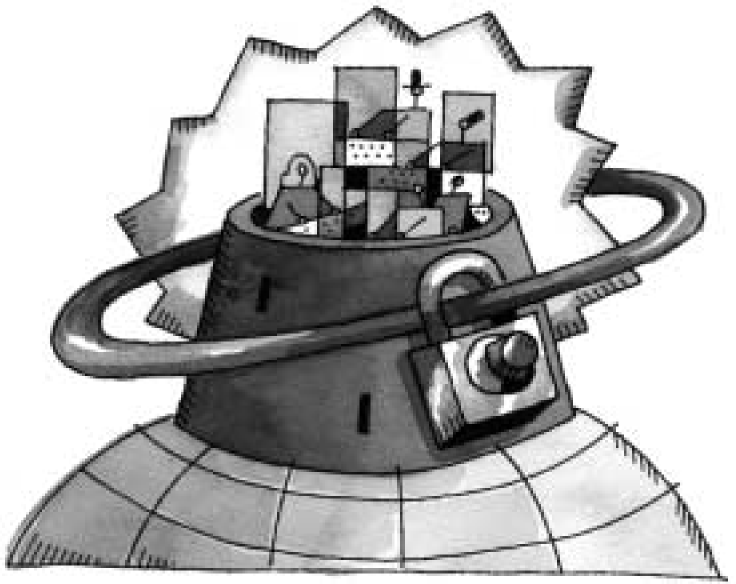
;login:

THE MAGAZINE OF USENIX & SAGE

December 2002 • volume 27 • number 6

Focus Issue: Security

Guest Editor: Rik Farrow



inside:

USENIX & SAGE

The Advanced Computing Systems Association &
The System Administrators Guild

the regional information watch

by Abe Singer

Abe Singer is a computer security manager at the San Diego Supercomputer Center, and occasional consultant and expert witness. His current work is in security measurement and security "for the life of the Republic."

Abe@SDSC.edu

Introduction

The San Diego Regional Information Watch (SDRIW)[1] is a sort of "network neighborhood block watch," a venue for bringing together area system/network security people and law enforcement, providing education about the technical and legal issues surrounding computer security, and providing an opportunity for "human networking." It has been very successful, and with the ever growing need for effective security and investigation of intrusions, we would like to share our experience and encourage others to form their own regional information watch.

Evolution

SDRIW began in part as a reaction to the incident of Steve Jackson Games and Operation Sundevil.[2] University system administrators (and others) were hesitant to report intrusions to law enforcement for fear that their systems would be seized for long periods of time. We were looking for a way to get these groups talking when an opportunity appeared: the mayor's "City of the Future" program[3] realized that there was a need for some type of high-tech law enforcement to be ready to protect the city's new high-tech sector.

SDRIW was originally thought of as a regional CERT;[4] however, we discovered that providing introductions and building trust between law enforcement, academics, and companies was more important and beneficial than being a CERT would have been.

SDRIW started as a three-way partnership between the San Diego Supercomputer Center (SDSC), Space and Naval Warfare Systems Command (SPAWAR),[5] and San Diego Data Processing Corporation (SDDPC).[6] SDDPC has faded from the scene, but we still have ties to SPAWAR, and our participation from law enforcement and local high-tech companies has grown. In the last couple of years, our meeting attendance has averaged around 40 people. We have over 200 addresses on our mailing list. Our "members" include system and network administrators, consultants, federal and local law enforcement, attorneys, students, researchers, local press, and even members of the local 2600 chapter.[7]

And we have realized our goal. Members are familiar with each other. If I have an incident at 3 a.m. and think it warrants attention from the FBI, I can get an agent to return my call. (We've actually had to do this.) Likewise, we've been called by some of our friends at other companies when they were in the thick of it. People are actually talking to and helping each other.

Mission

The Regional Information Watch is a combination of network neighborhood block watch, users group, and information-sharing organization.

We provide opportunity for:

- Information exchange/information sharing on technical and legal issues relevant to computer security.
- Face-time and familiarity between area professionals and law enforcement.
- "Networking" opportunities for people in the computer security arena.
- Early warning of regional incidents.
- Education on security tools, techniques, and standards.

The Regional Information Watch is open to anyone who wishes to participate.

[1] San Diego Regional Information Watch: *http://www.sdriw.org*.

[2] Bruce Sterling, *The Hacker Crackdown*: *http://www.mit.edu/hacker/part2.html*.

[3] "San Diego: City of the Future — The Role of Telecommunications," Report of the Mayor's Advisory Committee on the City of the Future, San Diego, March 11, 1994: *http://www.smartcommunities.org/city_of_the_future_report.pdf*.

[4] Computer Emergency Response Team: *http://www.cert.org*.

[5] Space and Naval Warfare Systems Command: *http://enterprise.spawar.navy.mil/spawarpublicsite/*.

[6] San Diego Data Processing Corporation: *http://www.sddpc.org/*.

[7] San Diego 2600: *http://www.sd2600.org/*.

Activities

Currently, the group's only activity is to hold monthly meetings, and we maintain a Web site with some local information, such as contacts in the area.

At our meetings we have had presentations on software security tools, the USA PATRIOT Act, forensics, California computer crime laws, data recovery, and handling email and phone threats, just to name a few. Some of our presentations are quite technical, others are for beginners.

But we don't just do presentations; in fact, we usually have 20 to 30 minutes of discussion before the "feature presentation." Our meeting agenda looks something like this:

- Introductions
- Announcements
- Current events
- Incidents, vulnerabilities, exploits
- New security tools
- Upcoming conferences and other events
- Featured speaker – varying topics, varying levels
- Call for speakers
- "Social hour"(sometimes with food)

The meeting is all in an open, round-the-room format, which gives people the opportunity to ask, "Has anyone ever seen probes like X?" or "Where can I find a tool to do Y?" or "We have a job opening for Z."

Our law enforcement members actively participate, letting us know about things happening on the legal side, and sometimes telling us about interesting cases that have been closed.

While our presentations are always useful, the social hour is often especially so, providing an opportunity for people to chat and get to know each other (some like to call this "networking").

And we occasionally act as a point of contact for related issues; we will get a call from law enforcement or a local company asking, "Do you know whom to contact at company X?"

Members/Structure

Officially, SDRIW doesn't exist. We're just a "public meeting," a group of people peaceably assembling to chat about interesting stuff. There is no board, no corporate entity – just some people putting stuff on a Web site and mailing out information about who might be somewhere at a certain time. We chose that path on purpose; there's no one to point a finger at, no membership requirements, restrictions, or dues (for that matter, no official membership).

Our "membership" consists in part of:

- Academics: sysadmins, researchers, and students from UC San Diego and San Diego State University.
- Large companies in the area: Qualcomm, SAIC, Cox Communications, TRW, SPAWAR, Exodus.
- Small companies: Anonymizer.com, local ISPs, independent consultants, forensics companies.

- Hardware vendors: Sun and others.
- Law enforcement and government: FBI, Secret Service, Postal Service, US Attorney's Office, City Police, County Sheriff, University Police, County D.A.
- Community: local members of 2600.

Future Goals

While we feel we have accomplished our primary objective, we do have some goals for expanding our activities. We are looking for sources of funding to allow us to pay expenses for out-of-town speakers and eventually host some workshops or a conference.

We would also like to provide job listings for security-related positions in the area.

And, of course, we always want to expand our "membership." We'd like to get more participation from ISPs and other companies in the area. In an ideal world, we'd have a security contact for every ISP in town, and for the security or sysadmins for (at least) the larger networks in the area.

Competition

When telling people about SDRIW, I am sometimes asked, "Isn't that what HTCIA (High-Technology Crime Investigation Association)[8] does?" Well, yes and no.

San Diego does have an HTCIA chapter. There is also a San Diego chapter of Infragard,[9] and a chapter of ISSA (Information Systems Security Association).[10] Many of the SDRIW participants are members of these groups too. In other cities, HTCIA or Infragard chapters might provide some of the services that SDRIW provides. But in San Diego, SDRIW was already so successful that the local Infragard chapter decided that it would not try and reproduce the effort in the same area; instead, it suggests that Infragard members interested in computer security participate in SDRIW.

HTCIA is roughly 80% law enforcement and 20% technical people. HTCIA is a formal organization with annual membership dues. New members have to be endorsed by existing members and consent to a background check. HTCIA's scope is wider than just computer security and is focused on criminal/legal aspects.

Infragard is also wider in scope than just computer security – its members are involved with "critical infrastructure" organizations. The San Diego chapter does not require dues but, like HTCIA, does background checks and has confidentiality requirements.

ISSA requires dues ($100 in San Diego).

SDRIW is about 80% technical people, 20% law enforcement, is focused on computer security, and is free.

How to Form Your Own

Okay, so you're sold, and you'd like to form your own group. Here's how to do it:

Find a space for a meeting. Maybe your employer has an auditorium or a large meeting room; someplace with a video projector for laptops is best; Internet access is helpful.

Pick a time for your first meeting. You'll eventually want to schedule a regular time, but start with a single meeting. We schedule our meetings from 2 to 4 p.m., which gives some people the opportunity to avoid having to go back to the office afterwards.

[8] High Technology Crime Investigation Association: *http://www.htcia.org*.

[9] Infragard: *http://www.infragard.net/*.

[10] Information Systems Security Association: *http://www.issa.org*.

If you can, find someone to give a presentation on something interesting. Do one yourself if you can't find anyone else. Or come up with a discussion topic for the group.

Put up a Web site (it can be simple to begin with) and mailing list for announcing meetings. Our mailing list is moderated and is used almost exclusively for the meeting announcements, so volume is quite low. We have found that some people rely on the mailing list to know when the next meeting is, and some look at the Web site. So it's useful to have both. Put information about the meeting on your Web site, including presentation topic and directions to the meeting. Also include information on subscribing to the mailing list.

Invite people to attend. For people you know, you might be able to get away with an email. But for people you don't know, you might want to pick up the phone and talk to them. They'll take you more seriously. Especially law enforcement people.

Who should you invite? Well, start with local companies. Call all the ISPs in town and ask to talk to their security person. Find security consulting firms and invite them. If you've got any colleges or universities in town, find a contact there, and ask them to forward it on to others. Identify companies with large networks and contact their security or network administrators, and/or CIOs.

Go visit local user groups, like the Linux users group, and give a five-minute spiel about the Regional Info Watch. If you can, make and give out a little flyer that describes the group, has the meeting time, Web site URL, and mailing list information.

Don't forget government agencies, such as county or city – they've got sysadmins too, y'know.

Get some law-enforcement participation. If you don't know any, call your nearest FBI office and ask to speak to an agent who handles computer and/or high-tech crime. Some offices have a squad specializing in that, while others just have one or two agents who handle those areas. Call the local police and sheriff's departments, too. Some places have people dealing with high-tech crime (we've got an entire task force here).[11] Oh, and there's also the prosecutors – district attorneys, state attorneys, and US attorneys. And it never hurts to ask each of them if they know people at other agencies who might be interested.

The Meeting

So you've got a meeting scheduled and people invited. What now?

About two weeks in advance, verify with your speaker that they're coming. Don't rely on the speaker to remember to contact you if they have to cancel, especially if they have something like a family emergency.

Send out a meeting announcement to the mailing list at least a week in advance. Include the time and date, location, directions, and a description of the talk. If you want, send out a (short) reminder the day before, too.

Before the meeting, make sure that whatever you need for the meeting is in place and working (chairs, video projector, whatever). Also, make a list of things to talk about: news, new vulnerabilities and exploits, tools, etc. Don't rely on your audience to supply information – anything that they do is a bonus.

[11] Computer and Technology Crime High Tech Response Team: *http://www.catchteam.org*.

If necessary, put up signs showing people where the meeting is. Also have someone to greet and escort the speaker to the meeting.

Plan to show up for the meeting a half-hour early so that you can be prepared and greet people as they show up. You may have to assist the speaker in getting set up. Put the meeting agenda (see above) on a whiteboard. Also put up the URL for the Web site, subscription information, and when the next meeting is (once it is determined).

One agenda item for your first meeting is to set a regular time for future meetings. We have found that a consistent meeting time is helpful (ours are currently the 2nd Monday of the month). People tend to set aside the time when they know when the meetings are, and they remember a regular time better. Get some consensus on the time – more people show up that way.

Also, see if you can get volunteers to give presentations at upcoming meetings, at least for the second meeting. We pitch our meetings as a “friendly audience,” a way to try out a presentation before giving it elsewhere.

Finally, use the social hour as an opportunity to thank people for showing up and get feedback from people on what they liked or didn’t like. You may find that people volunteer to help or volunteer to speak.

Lather, rinse, repeat the following month.

Getting Speakers

The hardest part about doing this is rounding up speakers. Sometimes you get volunteers quickly, but often you have to do a little convincing. Sometimes when somebody tells us about something they’re working on, we ask them if they wouldn’t mind talking to the group about it. Occasionally, we pick a topic and find somebody to speak on it. Other times, we see a presentation elsewhere and invite the speaker to give the same presentation to our group.

We emphasize that the talks can be on a wide range of topics, 20 to 40 minutes, and can be low-level or high-level. In this way we have a forum that attracts both beginner and expert-level people.

And we try to have a balance between technical and non-technical presentations. As it turns out, the legal/law enforcement people are often very interested in the technical presentations, and the geeks are interested in the legal presentations.

But we strongly *discourage* presentations by vendors who just want to do a sales pitch. We allow product vendors who wish to do a technical presentation on their product – how it works and what problem(s) it solves. But in our case, some members of the audience are quite savvy and quick to tear apart a product that is smoke and mirrors – and we point this out to the vendor. Since our mission is to be educational, there’s no value in our “members” learning about a tool that is not effective.

Some Tips and Gotchas

Some random tips, in no particular order:

- Be sure to coordinate with your speaker on what technical requirements they have for their presentation (e.g., video projection, Internet connection, audio, microphone) and/or what you are able to provide. And make sure that someone is present who knows how to work the equipment.

- If applicable, on the day of the meeting inform your receptionist(s) about the meeting so they can direct people to it.
- If you have to change a meeting from its regularly scheduled date or time, send out extra announcements making it clear that it's not at the usual date/time.
- Remember to provide directions and parking information. No use having a meeting if people can't find it.
- The meeting date/time has a big effect on who shows up. Some people do better with mornings (law enforcement), some do better with afternoons (geeks). Some people prefer after-hours, but others want to be home with their families (or don't want to miss the latest episode of "Buffy the Vampire Slayer").[12] Friday afternoons are probably the worst day for a meeting, as many people take off early Friday to do weekend stuff or are caught up with end-of-the-week tasks that they need to finish.
- Consistency and continuity is important. Keep the meeting cycle going. If once a month is too much, try once every two months, but keep it steady. If your meetings become too irregular or infrequent, attendance will taper off drastically.

Finally...

If you do form a Regional Info Watch, let us know, and we'll put a link to your site on our Web page. And we'd love to know how it's going. Just send an email to *sdriw@sdriw.org*.

Oh, and if you'd like to give a presentation at SDRIW, send an email to *speakers@sdriw.org*. We're always looking for speakers.

[12] *Buffy the Vampire Slayer: http://www.buffy.com/*.