



# E-Telligence

## 2009 Calendar of Events

- January 19-21, 2009  
**e-Forensics 2009**  
Adelaide, Australia  
[Click here](#)
- January 24-Feb. 01, 2009  
**SANS Conference Security 2009 West**  
Las Vegas, USA  
[Click here](#)
- Feb. 01-03, 2009  
**SCADA Security Summit**  
Lake Buena Vista, FL, USA  
[Click here](#)
- Feb. 03, 2009  
**Government Security and Privacy Conference**  
Victoria, BC, Canada  
[Click here](#)
- Feb. 23-27, 2009  
**International Fraud Conference**  
Toronto, ON, Canada  
[Click here](#)
- March 30-April 2, 2009  
**USAIEEE Computational Intelligence Society Conference**  
Nashville, Tennessee, USA  
[Click here](#)
- April 13-16, 2009  
**Cyber Physical Systems Week**  
San Francisco, CA, USA  
[Click here](#)
- April 20-24, 2009  
**18th Annual International World Wide Web Conference**  
Madrid, Spain  
[Click here](#)
- May 12-14, 2009  
**APWG Spring Counter-eCrime Operations Summit** Barcelona, Spain  
[Click here](#)

## HEADLINE NEWS — January 13, 2008

### What's New on the Frontline!



## Team Cymru Offers Specialized Services

Team Cymru is a specialized Internet security research firm dedicated to making the Internet more secure. By researching the who and why of malicious Internet activity worldwide, Team Cymru helps organizations identify and eradicate problems in their networks.

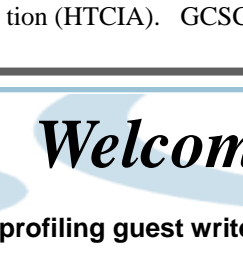
### For Banks

The BIN (Bank Identification Number) feed comprises a near-real-time list of bank accounts and credit cards that have been identified by Team Cymru as potentially compromised. This data comes from Team Cymru's unique insight into the underground economy. This service is provided to verified financial institutions at no cost to them.  
<http://www.team-cymru.org/Services/BINFeed/>

### For Law Enforcement

The Botnet Analysis and Tactical Tool for Law Enforcement (BATTLE) displays IRC and HTTP botnet data on an interactive world map in near real time. It is intended to provide enough information to enable law enforcement to identify botnets and attacks that are of interest to them. On the right-hand side of this page, you can see an example screen shot of the BATTLE interface.  
<http://www.team-cymru.org/Services/battle.html>

## Announcing the 2009 Tri-Lateral Security Conference



Mark June 18 and 19, 2009, in your calendar for the 2009 Tri-Lateral Security Conference in Calgary! Just a click away, visit [www.trilateralcalgary.ca](http://www.trilateralcalgary.ca) to learn more. This year's event is titled **Securing Our Sustainable Society: Critical Infrastructure and Public Safety in Today's Economic Climate** and will focus on the safety and security of our critical supply chain infrastructure.

The Tri-Lateral Conference is a joint initiative sponsored by three separate and distinct organizations: the Security Professionals Information Exchange (SPIE), ASIS International Chapter #162 and the Western Canada Chapter of the High Tech Crimes Investigation Association (HTCIA). GCSC will also be supporting this conference.

# Welcome to E-Telligence

Twice a month, we'll be profiling guest writers, cyber crime news and important events to keep you informed.

## Dispatches From the Frontlines of Cybercrime

By Tom Keenan

**Dr. Tom Keenan, FCIPS, I.S.P. is a professor at the University of Calgary as well as a national technology columnist for the Business Edge News Magazine (www.businessedge.ca). For the benefit of E-Telligence readers, he has provided this early version of a report that will appear in the January 23, 2008 issue of that newspaper, courtesy of Business Edge.**

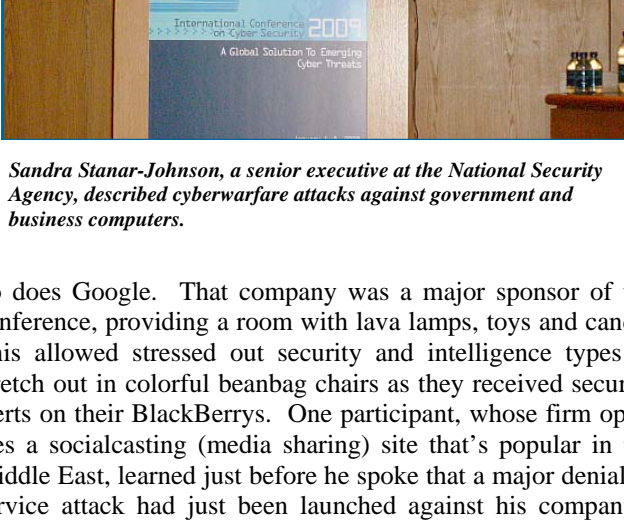
New York, NY

It's hard to imagine a safer place than the recent *International Conference on Cybersecurity*, held at Fordham University in New York City, January 6-8, 2008. An NYPD mobile command post bus was parked outside; uniformed officers searched every bag of every participant and serious looking FBI agents sporting earpieces guarded the doors to the sessions. A hilarious side effect was that almost nobody tried to break the "no food or drinks" rule in the auditorium. Sneaking in a shot of joe just didn't seem worth tangling with a beefy Fed. I got stopped just because my conference badge had flipped around the wrong way.

Anyway, nobody needed coffee to stay awake, as speaker after speaker revealed new and frightening facts about the global reach of cybercrime. This event marked the first such collaboration between the Federal Bureau of Investigation and a university, driven by a growing awareness of the serious threats to business, military and even personal computers in North America.

Shawn Henry, Assistant Director of the FBI's Cyber Division, said the US government now considers cybercrime the most critical threat "after a weapon of mass destruction in one of our cities." To emphasize this commitment, 22 federal departments and agencies have been told to work together in a comprehensive national cybersecurity initiative, some of whose details remain classified.

Sandra Stanar-Johnson, a senior executive at the spooky National Security Agency, described cyberwarfare attacks against government and business computers in Estonia and, more recently in Georgia, as well cyberfrauds such as a phishing scheme in Romania that just saw 40 people arrested. "Rather than employing foot soldiers and thugs to intimidate, they recruit young hackers," she said, adding, "we are in a world where technology moves much faster than the government typically moves." Appearing rather nervous, because "I almost never do unclassified briefings" she said the US government takes cybercrime and cyberwarfare so seriously that they're reaching out to anyone who can help. The 200 or so computer security experts, from 37 countries, seemed to agree that urgent action is required.



Sandra Stanar-Johnson, a senior executive at the National Security Agency, described cyberwarfare attacks against government and business computers.

So does Google. That company was a major sponsor of the conference, providing a room with lava lamps, toys and candy. This allowed stressed out security and intelligence types to stretch out in colorful beanbag chairs as they received security alerts on their BlackBerrys. One participant, whose firm operates a socialcasting (media sharing) site that's popular in the Middle East, learned just before he spoke that a major denial of service attack had just been launched against his company's computers.

Adam Swidler, a senior product marketing manager at Google, reported that his company is a major target for cyberattacks, because "we're more than just scrutinized more often than anyone else, we're attacked more often." In a private conversation he acknowledged that Google has suffered outages to Gmail and other services, but argued that their track record is better than competitors and that "when we go down everybody knows about it."

Swidler urged companies to consider "cloud computing" solutions, which, of course, Google's enterprise division is happy to sell you.

He cited Circuit City, Jenny Craig, and (his *alma mater*) Fordham University as companies that were taking this approach. Although farming your data out to remote computers might seem risky, he said it's actually safer, because Google hides it in very secure places. "Even I have never seen one of Google's storage facilities," he said, "and I don't ever expect to." In companies, he said, "60% of corporate data resides unprotected on PC desktops and laptops" and "1 out of 10 laptops will be stolen within 12 months of purchase."

Eastern Europe is apparently a cesspool of computer fraud, child pornography and hacking and merited its own session at the conference. Agent Darren J. Mott of the FBI computer intrusion unit reported that cyberevil is radiating out from Russia into neighboring countries. "We've seen malware sent from St. Petersburg to Estonia," where "you can get free a free wireless connection wherever you want." Expect arrests there soon, he predicted.

Mott says the highly publicized takedown of the Russian Business Network, which provided Internet hosting for many criminal sites, may have been something of a false victory. "The RBN gets all the news," he laughed, "but it was only one of about 20 bulletproof Internet service providers in Russia." He suggested the bad guys may have offered it up as a sacrifice to take the pressure off their other illegal operations. Making arrests in Russia is tricky, Mott says, because of police corruption. "When you go to the FSB (Russian police authorities) to report one of their computer criminals, the police officer may realize - hey, that's my nephew."

Several speakers referred to the catastrophic events of 9/11 and suggested that terrorists could cause even more havoc with computers than by flying planes into buildings. Targets could range from banking and business computers to the SCADA systems that run power grids and other utilities.

The US military academies have turned network security into a team sport with an annual cyber defense exercise. Lt. Col. William J. Adams of West Point said the main thing his cadets learn from it is how quickly an attack can occur and how overwhelming it can be.

Evan Kohlmann, senior investigator at Global Terror Alert in Washington, D.C., showed how Islamic terrorist groups are using the Internet to recruit, organize, and fund their operations. He displayed chilling chat posts of terrorists such as Abid Hussain Khan, now serving a 12-year prison term in the UK. Khan wrote that "attacks are permissible through out this world, so the world is a battlefield in my vision, everything, almost, is a target... so if you can find a big target and take it out, say like a military base in UK, then alhamdulillah." (which roughly translates as "All praises are for Allah only.")

One of the most unlikely speakers in this mainly male group of intelligence gurus was Hon. Shannen L. Rossmiller, a Montana mother of three and former judge, who is self-taught in Arabic. Motivated, she says, by patriotism, she creates fictitious terrorist identities and role-plays them in online discussion groups. To date, her radical Muslim male characters and online stings have resulted in 214 cases of actionable intelligence. These include the case of *United States Army v. Spec. Ryan Anderson* who received five life sentences for attempted espionage and providing material support to a terrorist group during a time of war.

The overwhelming impression left by this conference is that we are indeed locked in a nasty and continuous cyberwar, and that the bad guys only need to find one vulnerability while the cyberdefenders need to plug all the holes. Doing this is probably going to bring changes in how people use their workplace computers. The US government is already cracking down on recreation computer use on its premises and strongly suggesting that companies do the same. The days of taking a break to check the sports scores or book a vacation may be numbered. As for watching videos or downloading software at work, in the words of Tony Soprano, who would have been decidedly uncomfortable at this conference, "Forgedaboutit."

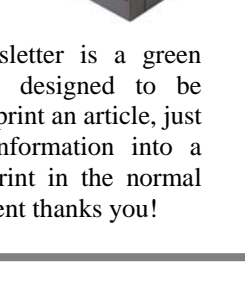


Google's lounge at the International Conference on Cybersecurity.

## Websites you should visit...

- Fourth Annual Tri-Lateral Security Conference in Calgary  
<http://www.trilateralcalgary.ca>
- Technology Crime Interpol  
<http://www.interpol.int/Public/TechnologyCrime/default.asp> Information
- Cool current affairs and searches on many topics  
<http://current.com/topics/75850792/tech/new/0.htm>

## If you need to print...



The E-Telligence newsletter is a green document and is not designed to be printed. If you wish to print an article, just copy and paste the information into a Word document and print in the normal manner. The environment thanks you!

## Exposing the Real Meaning of Hackerspace

By Wil Knoll

**Wil Knoll (GCIA Gold) is a security analyst for Axia NetMedia in Calgary, AB, and has presented for SPIE, Checkmate.org and SAIT. His exploits in the physical world can be followed on twitter at <http://twitter.com/winkn> where any news about the Calgary Hackerspace will be posted.**

It would be simple enough to say that there will be a Hackerspace meet up on Tuesday, January 15, 2009 in Calgary. Unfortunately, almost any article that contains the word "hacker" seems to contain an expository paragraph about the true history of the word and how it has been co-opted by the media. Because of this, the term, hackerspace may already be branded with connotations that are not earned or just. So, here is my expository paragraph about the term hacker.

The term hacker generally glosses over so much of its depth and history. Hacking is not isolated to computers and computer networks; it is beyond just pure technology. It is present in art, infrastructure and the interactions between people. Paul Brodeur of iStockphoto has one of my favourite definitions. "Anyone is a hacker if they possess the mindset of curiosity, abstract thought, and imagination." He is also the Calgaryian who delivered the call to action, sparking this attempt for a hackerspace in Calgary.

In my belief, Shakespeare and Keats were the most righteous word hackers, and Frank Lloyd Wright was a physical space hacker who shaped how architects would look at overhanging. To some degree, we could say that the Fonz pounding the jukebox is a hacker. We could say that it was a kludge of a hack (physical violence? lacks class), or we could say that it was an elegant hack (so simple and direct). It is the creative answer that did not exist before someone asked the right questions that embodies a hack. A hacker simply appreciates the process of questioning and, when their muse accompanies them, they create.

### Hackerspace – A Space Heater and a Worn Down Couch

I wasn't much of a member of the "frat house" I lived in during my university days. As the only computer/performing-arts geek in a group of fifty guys, there wasn't much of a common space for me to geek out in. I often found myself relegated to the basement, among cast away furniture and other detritus, to pursue my exploring of technology and art. It was in its own way a very endearing place. Two incandescent bulbs, cold concrete floor, a space heater and a worn down couch. It was almost everything I needed. But it lacked community. It lacked the like-minded individuals to tackle muses and prompt questions.

Hackerspaces range in quality of furniture and the amount of heat in the building, but the defining characteristic is community. Hackerspaces are community operated spaces akin to a clubhouse. They normally consist of a common space, a few break-out rooms, a kitchen and a bathroom. They are not meant to be a residence or halfway house for hackers. It is the community lab where one can socialise, work on projects, learn, teach, coo, play videogames, forget to water the plants and generally be in element with others of one's kind.

The physical space is part of it but each hackerspace is defined by its community and what the community does. Existing design patterns for hackerspaces comment on having goals for the space or direction for the community. The consensus seems to be just make sure the community can manage the space, take care of collecting memberships and paying the bills. If that is in place, then the members will come up with the projects that give each hackerspace its DNA, the work that will become its shared tradition and history.

Part of that DNA is creativeness that extends beyond computer and network technology. Popular topics of discussion and peering training at hackerspaces range from woodworking, knitting, cooking, acid etching metal, paper making, and introductions into other trades as each member shares what they know. A friend joked to me once that the reason that we need hackerspaces is that "when the revolutions comes, we'll be glad we learned how to get stuff done." And that can extend beyond the membership. Many hackerspaces do some form of education for the masses, open nights where non-members are invited in to learn about a particular topic. This can help pay the bills (with a small donation asked for at the door) but also exposes potential new members to the community and the space. Along those lines, the hackerspace can be used as a gathering place or rally point for other community groups.

### Hackerspace – A Model Railway Club

It's been said that the spiritual parents of the hackerspace are the Tech Model Railroad Club at MIT, and c-base in Berlin.

The Tech Model Railroad Club, formed in 1946, is exactly as it sounds; a model railway club formed by students of MIT. Students would gain a key to the room if they logged 40 hours worth of work on the tracks. A group of members was not too interested in the model trains themselves, but in the switching equipment and circuits created to run the model trains on. This group, the Signals and Power Subcommittee played with some of the most powerful computers of the era outside of the club while at MIT, and built an amazingly elaborate system of circuits controlled by 1,200 relays to run the railroad on. They coined terms that permeate hacker and IT culture, "foo", "hack", "mung" and others. Clubhouses have been part of computer culture since there was a word to describe it. The modern PC was born from members of the Homebrew Computer Club back in 1975.

The modern incarnation of the hackerspace grew out of c-base in Berlin, a non-profit organisation formed in 1995. The membership has spearheaded an initiative to create free public access wireless networks across Berlin among other projects. c-base also hosts a weekly 'open mic' for musicians of every kind to hold jam sessions or concerts. Events and parties are popular, whether they are art exhibitions, theatrical performances, or technical presentations. c-base has been a case study in how to deal with membership and the other nuances or running a hackerspace. In July of 2008 c-base came very close to bankruptcy and facing eviction from their gorgeous space. This was primarily due to rent debt and financing costs. c-base was rescued from bankruptcy by the larger international community and admit in their press release that "the issue went beyond the cash box." Their flirt with bankruptcy taught many lessons to the community.

There are roughly 150 hackerspaces around the world that are either planned, being built, or currently active. In Canada, there are a handful of them already. If you're interested in locating or starting an effort in your city, check [http://hackerspaces.org/wiki/Hacker\\_Spaces](http://hackerspaces.org/wiki/Hacker_Spaces) for more info.

### Hackerspace – Calgary

So, to start again from the beginning. There will be a Hackerspace meet up on Thursday, January 15, 2009, at the Oolong Tea House in Kensington. If you are interested in participating in the discussion or at least listening to the planning, then join us at 6:30 pm.

This meeting will be to discuss details pertaining to planning, location, organisation and others. More details can be found on Paul Brodeur's blog, along with background material and information for the Facebook group and mailing list. <http://ultramegam.com/blog/?p=50>

I'll be there. I'm hoping that this idea comes together. I'm wondering what it will look like. I would even take two incandescent bulbs, cold concrete floor, a space heater and a worn down couch, as long as there was someone else there to hack with.

## You'll be Interested in This

Data Breaches Up Almost 50 Percent, Affecting Records of 35.7 Million People  
Washington Post (01/06/09) P. D2 ; Krebs, Brian

The number of data breaches rose almost 50 percent in 2008 compared to the year before, compromising the personal records of at least 35.7 million Americans, says the Identity Theft Research Center (ITRC). ITRC says that 656 breaches were reported last year, versus 446 in 2007.

Approximately 37 percent of the breaches targeted businesses, while the segment of breaches attributed to data theft from current and former employees rose from 7 percent in 2007 to close to 16 percent in 2008.

"This may be reflective of the economy, or the fact that there are more organized crime rings going after company information using insiders," says ITRC's Linda Foley. She says that many businesses fail to disclose data breaches even though 45 states have rules that consumers must be alerted of any loss or theft of private records.

Nearly 42 percent of organizations that reported a data breach or loss last year did not reveal the number of consumer records that might have been compromised. About 14 percent of the data-breaches were blamed on computer hacking and data-stealing software.

Human error caused the most data breaches, ITRC says, such as lost or stolen computers and removable electronic devices or the accidental exposure of consumer data. ([go to web site](#))

Twitter Has Security Meltdown  
InformationWeek (01/05/09) ; Claburn, Thomas

A security breach at the microblogging site Twitter has resulted in a number of high-profile Twitter accounts including accounts belonging to President-elect Barack Obama, CNN's Rick Sanchez, and Britney Spears being compromised.

According to Twitter, these accounts and 30 others were breached by an individual who hacked into the support software the site's employees use to help users perform tasks such as changing the email address associated with their account. The individual then used the hijacked accounts to send fraudulent messages and spam.

Twitter has since taken the support tools offline, and has said that it will not put them back until they are safe to use. The site is urging its users to reset their passwords and verify that the email address stored in Twitter's account setting area is correct.

In addition, there has also been a phishing attack aimed at Twitter users. In this attack, which was first reported Jan. 3, victims received a direct message from one of their Twitter followers telling them to visit certain sites, which look like Twitter's logon page but are actually fraudulent sites that steal the victim's account information. ([go to web site](#))

## Cyber Tips: WIRELESS SECURITY

Many people rush through the set up process for a wireless home network but that can put you at risk.

- 1. Change Default Administrator Passwords**  
The logins provided by equipment manufacturers are simple and very well-known to hackers on the Internet. Change these settings immediately.
- 2. Turn on (Compatible) WPA/WPA2 Encryption**  
Normally, you will want to pick the strongest form of encryption that works with your wireless network.
- 3. Change the Default SSID**  
Change the default SSID immediately when configuring wireless security on your network.
- 4. Enable MAC Address Filtering**  
Many such products offer the owner an option to key in the MAC addresses of their home equipment that restricts the network to only allow connections from those devices.
- 5. Disable SSID Broadcast**  
In the home, this roaming feature is unnecessary and it increases the likelihood someone will try to log in to your home network. Disable it.
- 6. Do Not Auto-Connect to Open Wi-Fi Networks**  
This setting should not be enabled except in temporary situations.
- 7. Assign Static IP Addresses to Devices**  
Turn off DHCP on the router or access point, set a fixed IP address range instead, then configure each connected device to match.
- 8. Enable Firewalls on Computer and the Router**  
Ensure that your router's firewall is turned on and consider installing and running *personal firewall software* on each computer connected to the router.
- 9. Position the Router or Access Point Safely**  
Try to position these devices near the center of the home rather than near windows to minimize leakage.
- 10. Turn Off the Network For Periods of Non-Use**  
Consider doing this during travel or extended periods offline.