Uplink

January • February 2002
Volume 14, Number 1

Published bimonthly by the National Institute for Computer-Assisted Reporting

www.nicar.org

Bits & Bytes

New Uplink

This edition of *Uplink* is the result of rethinking and redesigning, with the goal of delivering the most useful information we can. The design changes were well under way when the events of Sept. 11 occurred, so in addition to a new look, *Uplink* devotes most of this edition to the coverage of security and terrorism.

As always, we seek your input, so please drop us a line and let us know if the design meets with your approval, if you have suggestions, which articles appeal to you the most, and, of course, if you have suggestions for future articles. We welcome stories from our subscribers. E-mail your thoughts to Managing Editor Jeff Porter at jeff@nicar.org, or mail him at 138 Neff Annex, Missouri School of Journalism, Columbia, MO 65211.

Data updates:

The IRE and NICAR Database Library has recently updated the following databases:

Trucks

The U.S. Department of Transportation's Truck Census File, which contains records on each company that has com-

continued on page 2

TEACHER QUALITY

Flunking tests

By Becky Beaupre, *Chicago Sun-Times*

Teachers who had flunked at least one test of teacher competence taught more than 180,000 Illinois schoolchildren last year. Some of these teachers failed exams–including a Basic Skills test written at an eighth- or ninth-grade level – five or 10 times before passing. Some never passed.

But before the Chicago Sun-Times started poring over teacher test score data earlier this year, nobody but the individual test takers knew it – not even the state agency that kept the data.

Our quest to investigate teacher quality in Illinois began with a Freedom of

continued on page 26

SPOTLIGHT: TERRORISM

Poor airport security

By Matt Carroll, *Boston Globe*

How were the Sept. 11 hijackers able to skip through security at Logan International Airport to commandeer not one, but two airplanes?

That was one of the key questions *Boston Globe* reporters sought to answer following the horrific events that ended with the four planes crashed, the World Trade Center in ruins, and thousands dead. This much was known about Logan already: The Massachusetts Port Authority, the public agency that runs the airport, was a patronage haven, filled with former state officials, relatives and cronies. Articles in the days following the crashes hammered that point home.

The suspicion was that security at Logan was weak. There was anecdotal proof — passengers who walked onto planes while accidentally carrying along knives, scissors and corkscrews — but no hard numbers.

continued on page 24

SPOTLIGHT:

FOR MORE ON TERRORISM SEE:

- CNN's 'Flight Risk,' p. 2
- In-depth online, p. 3
- Access after attacks, p. 5
- Putting together the data puzzle, p. 7
- Security problems, p. 9
- Comparing foot traffic, p. 10
- Tracking a suspect, p. 11
- Detailing identities, p. 13
- War windfall p. 14
- Meeting the data challenge, p. 16
- Lessons from disaster, p. 20
- Fighting the airport, p. 22

Bits & Bytes

continued from page 1

mercial interstate vehicles weighing more than 10,000 pounds. This group includes buses, semis and shippers of hazardous materials. Current as of July 2001.

Dams
The National Inventory of Dams includes U.S. dams. The fields cover the construction date, the last inspection date and whether an emergency action plan is in place in case the dam fails. Current as of mid-October

OSHA
The OSHA workplace safety data contains detailed information about workplace inspections, injuries, hazardous-substance accidents and violations for companies in the U.S. and its territories. Current as of March 2001.

SBA
The Small Business Administration disaster loan database includes loans that have been approved – although not necessarily fully distributed – for businesses and individuals in the wake of emergencies. The update includes more than 700 loans related to the Sept. 11 terrorist attacks. Current as of Oct. 31, 2001.

For more information about the database library's collection, including purchase prices, go to *www.ire.org/datalibrary/databases/*. To order data, contact NICAR at 573-884-7711 or download an order form at *www.ire.org/datalibrary/orderform/orderform.pdf*

SPOTLIGHT: TERRORISM

CNN's 'Flight Risk'

By Denise Prodigo-Herrmann, *Database consultant*

In the weeks following 9-11, journalists around the country were scrambling to make sense of the Federal Aviation Administration Enforcement Information System (EIS) database.

Under the guise of "national security and safety" the Federal Aviation Administration refused to comment about any information relating to the enforcement database, making it difficult to decipher the meanings of some codes within the database. The NICAR listserv was flooded with information, ideas, concerns and strategies relating to the data and was a helpful resource during the entire analysis process.

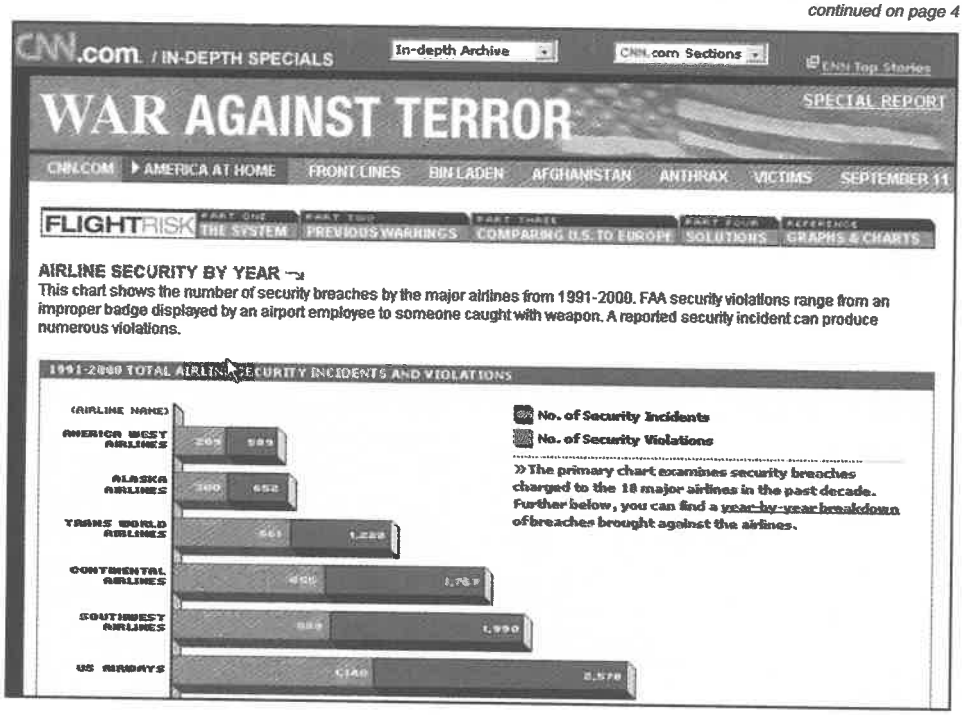
Because CNN was interested in security issues relating to the top 25 airports and the top 10 airlines in the country, I obtained a list of the top 25 airports based on passenger load from Airports Council International and a list of the top 10 airlines from the U.S. Department of Transportation. My analysis focused mainly on the FAA EIS database, but reports about airport security and safety from the General Accounting Office also were used. While the enforcement data was said to date back to 1962, the earlier years of data did not seem complete. The final CNN analysis covered a 10-year period from 1991-2000.

Within the FAA database, the main table included all incidents relating to enforcement, such as flight operations, training, drug testing, hazardous materials and security. Using Microsoft Access, security incidents were isolated using cat_code = 20 in the main table. The security table detailed the type of security violations.

When linked with the main table, the database started to tell a story. For example: On April 19, 1991, at Anchorage International Airport, concourse B, a male passenger, whose identity is expunged in this database, had a firearm in his possession. The firearm was detected in the X-ray machine, and the firearm was unloaded.

For the CNN analysis, it would be im-

continued on page 4



SPOTLIGHT: TERRORISM

In-depth online

By Mike Fish, *CNN.com*

Before the events of Sept. 11, air travelers might have thought security personnel at airport checkpoints worked for the government. The airlines, maybe. Or they may have guessed the local airport authority.

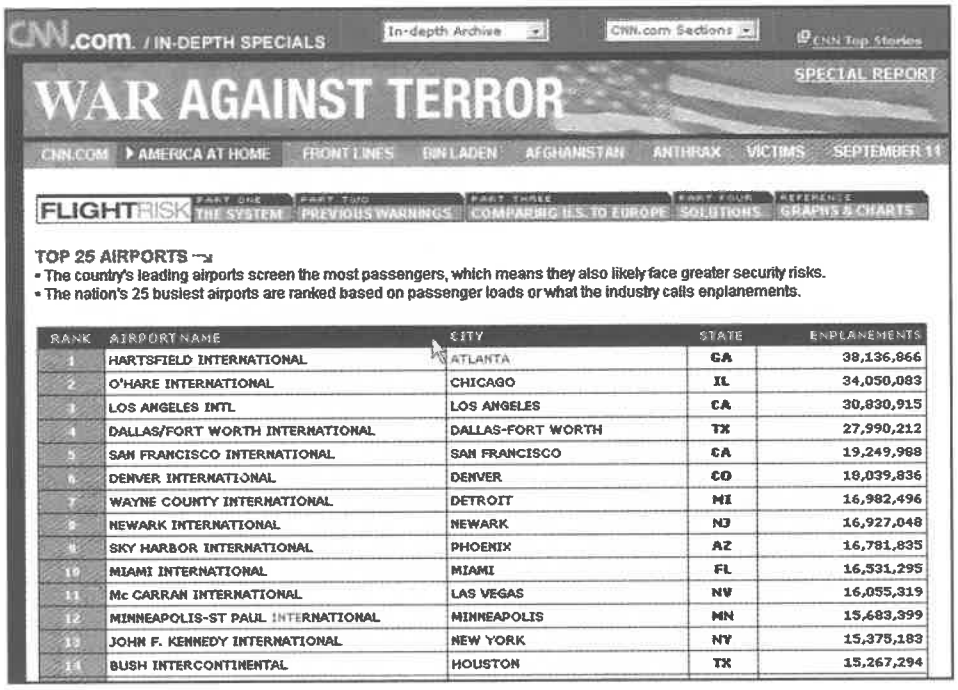
The truth is, under Federal Aviation Administration guidelines, the airlines are responsible for airport security – but they bid the job out to private security firms. So, how does the system grade out and should travelers feel secure? And, if not, what are the holes in the system and why have they gone uncorrected?

Armed with a laundry list of questions, CNN.com embarked on a computer-assisted reporting project that produced the four-part series "Flight Risk" (*www.cnn.com/SPECIALS/2001/trade.center/flight.risk/index.html*). The Web site contracted with Denise Prodigo-Herrmann, former Atlanta Journal-Constitution database editor, to clean up the data and oversee its analysis. We also performed extensive searches of government and aviation Web sites, which proved helpful in providing context and leading us to earlier critical reports submitted to Congress.

A 2000 report from the General Accounting Office was of particular interest, revealing that the starting salary for security screeners at 14 of the nation's 18 largest airports was $6 or less an hour (*www.gao.gov* click on Airport Security under GAO Reports). The federal minimum wage is $5.15 an hour.

Saddled with low wages, entire airport security teams – considered one of the most crucial jobs in assuring passenger safety – routinely turn over at least once a year.

Watchdogs had identified this extraordinary turnover as a dangerous shortcoming, though offering little or no statistical support. In a bid to do so, we took the GAO turnover rates for the individual airports and compared them with security breaches reported by the FAA during the same 12-month period ending April 1999.



RANK	AIRPORT NAME	CITY	STATE	ENPLANEMENTS
1	HARTSFIELD INTERNATIONAL	ATLANTA	GA	38,136,866
2	O'HARE INTERNATIONAL	CHICAGO	IL	34,050,083
3	LOS ANGELES INTL	LOS ANGELES	CA	30,830,915
4	DALLAS/FORT WORTH INTERNATIONAL	DALLAS-FORT WORTH	TX	27,990,212
5	SAN FRANCISCO INTERNATIONAL	SAN FRANCISCO	CA	19,249,988
6	DENVER INTERNATIONAL	DENVER	CO	18,039,836
7	WAYNE COUNTY INTERNATIONAL	DETROIT	MI	16,982,496
8	NEWARK INTERNATIONAL	NEWARK	NJ	16,927,048
9	SKY HARBOR INTERNATIONAL	PHOENIX	AZ	16,781,835
10	MIAMI INTERNATIONAL	MIAMI	FL	16,531,295
11	Mc CARRAN INTERNATIONAL	LAS VEGAS	NV	16,055,319
12	MINNEAPOLIS-ST PAUL INTERNATIONAL	MINNEAPOLIS	MN	15,683,399
13	JOHN F. KENNEDY INTERNATIONAL	NEW YORK	NY	15,375,183
14	BUSH INTERCONTINENTAL	HOUSTON	TX	15,267,294

readme.txt

Links

The CNN.com original project "Flight Risk" was reported by Mike Fish. Denise Prodigo-Herrmann conducted the database analysis. Kevin Drew was the editor. Emily Chen was the designer and worked with Ann Hoevel to develop graphics, charts and images. Meriah Doty also developed images. Robert Felker was the illustrator. Charles Rawls was the web editor.
www.cnn.com/SPECIALS/2001/trade.center/flight.risk/

General Accounting Office reports on airport and aviation security
www.gao.gov/airptsec.html

Breaking security

Our analysis revealed that at major airports experiencing a more than 200 percent annual turnover rate – like Lambert in St. Louis, Hartsfield in Atlanta and O'Hare in Chicago – screeners detected a smaller percentage of security breaches. And at airports with lower turnover, screeners uncovered more security violations.

The CNN.com computer-assisted analysis of FAA enforcement data from 1991 to 2000 also found:

• The top 10 carriers incurred $13.13 million in FAA fines since 1998, fines which critics say have done little to fix security shortcomings.

• Logan International Airport in Boston, Dulles in Virginia and Newark International – the originating points for the Sept. 11 terrorist hijackings – have some of the lowest number of weapons caught by the airline screeners as a percentage of all reported security violations at each airport.

• American Airlines, one of the carriers whose planes were hijacked

continued on page 4

CNN

continued from page 2

possible to provide that level of detail on deadline for 25 airports and 10 airlines over a decade.

As with all information collected from databases, the data must be confirmed by other sources, such as police records, to accurately report the story. So, I decided to summarize the database by counting specific weapons detected at airports over a 10-year period. My theory was, if airports like Newark and Logan could have terrorists board planes with weapons, they likely would have a low number of weapons detected at their airports as compared to equally large U.S. airports. If few weapons are detected as compared to other airports, then screeners aren't doing their jobs.

Focus on weapons

With more than 300 security codes and no FAA confirmation, it was difficult to ascertain the meanings of some of these codes. After much debate and research, I decided to focus on all security breaches related specifically to weapons. Weapons were defined using the following security descriptions: bludgeon, explosive, firearm, firearm – hand gun, firearm – long gun, incendiary, knife, other weapon, stun gun and tear gas/chemical.

Grouping these descriptions into one category showed the number of weapons detected at each airport by year with further breakdowns of the number of weapons.

Security descriptions allegedly relating to tests conducted by the FAA, where FAA employees dress in plain clothes and try to get items through security check points, were not used as the meanings of the code descriptions were unclear. Some reports, for example, stated that the code "Fail Detect HG" meant failure to detect a handgun while others reported that it meant failure to detect a hand grenade. Without FAA confirmation of the meanings, I decided to take a more cautious approach to my analysis.

Stories and graphics

The six-week project produced nine stories written by CNN.com reporter Mike Fish and a number of detailed graphics designed by the CNN.com staff. The graphics showed:

- The number of incidents and violations at the top 25 airports and the top 10 airlines over a decade. For each incident, there could be numerous violations. The numbers were broken down year by year for each airport and airline in separate charts.
- The number of weapons found at the top 25 airports over a 10-year period. These numbers also were broken down year by year for each airport in separate charts.
- The dollar amount paid in fines by the top 10 airlines from 1998 – 2000, according to the FAA quarterly enforcement reports.
- The annual turnover rate of security screeners at 18 airports as reported by a GAO aviation security report from June 2000. The percentages of security violations for the same period also were reported from the enforcement database.

Denise Prodigo-Herrmann can be reached by e-mail at dmph@bellsouth.net

online

continued from page 3

Sept. 11, was cited for the most security incidents in the decade. Delta Air Lines was second, and United Airlines, the other carrier whose planes were hijacked, had the third-highest number of incidents. Combined, American and United airlines have paid more than $5 million in FAA fines during the past three years.

Our six-week project produced nine stories under the sub-heads: The System, Previous Warnings, Comparing U.S. to Europe and Solutions. Kevin Drew edited the project, while designer Emily Chen worked with Ann Hoevel developing graphics, charts and images.

Because CNN.com isn't hamstrung by space limitations of a daily newspaper, we were able to effectively support our stories with extensive graphics and charts. We were able to take the top 10 airlines and break down their security breaches on a year-by-year basis over the last decade. The same was done with the nation's top 25 airports, where we further detailed the weapons violations at each of the airports.

Critics of the security system had accused the FAA of perpetuating a system of levying fines when breaches are found rather than seeking harsher corrective measures for the airlines. We chose to profile one of the leading security providers, Atlanta-based Argenbright, while also examining the fines assessed by the FAA against the airlines over the past three years (*www.faa.gov/agc/enforcement).*

Different approach

Several media organizations also were analyzing FAA data in the wake of Sept. 11, but Prodigo-Herrmann followed a slightly different approach for CNN.com.

While the data came with detailed record layouts, some data within specific fields were hard to decipher, specifically security descriptions. Despite numerous requests from NICAR, the FAA refused to unveil details about the data. The NICAR listserv was flooded with commentary from journalists around the country on the complexity of the security code definitions. Prodigo-Herrmann focused her analysis on weapons or violations actually detected by screeners as opposed to an analysis of weapons that screeners missed in FAA tests of the system.

Mike Fish can be reached by e-mail at Mike.Fish@turner.com

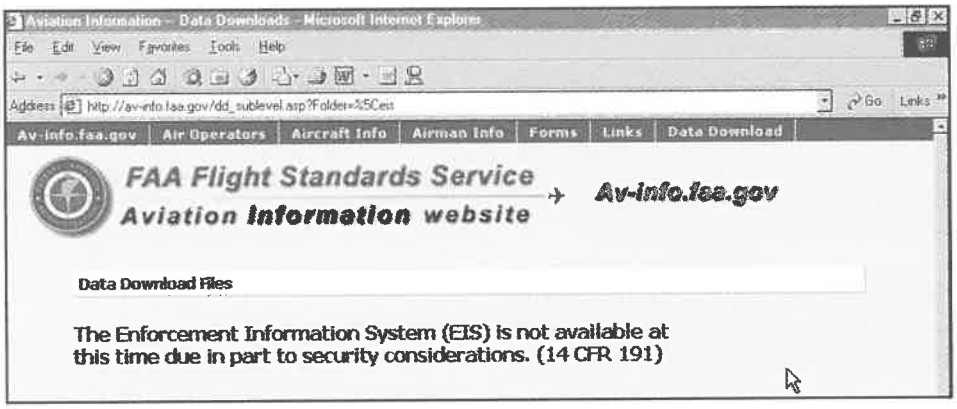
SPOTLIGHT: TERRORISM

Access after attacks

By Jennifer LaFleur, *St. Louis Post-Dispatch*

Just as federal agencies were beginning to develop useful Web sites, where more and more data was being made available, many agencies are now swiftly pulling databases from their sites.

Since the Sept. 11 attacks, several federal agencies have removed public records and documents from their Web sites because of security concerns. In addition, some states have proposed rules that may limit access to public records.



Much of the information federal agencies handle is covered by the federal Freedom of Information Act, a law enacted in 1966 that requires government agencies to disclose records. Since then, Congress has amended the law to encourage, but not require, agencies to make commonly requested information available on their Web sites. Many responded to that call, but some are now beginning to rethink what they put online. Among them:

- The Bureau of Transportation Statistics has discontinued public access to the National Transportation Atlas Databases and the North American Transportation Atlas. Environmental groups have used information from those sites to assess the impact of transportation proposals.
- The U.S. Geological Survey has removed several reports relating to water quality.
- The Office of Pipeline Safety has removed access to the pipeline mapping system, making the information available only to pipeline operators and government officials.
- The Federal Aviation Administration has removed a link to enforcement data that includes security violations at the nation's airports. Several news organizations used the information for stories before the agency removed it from its site.
- The Environmental Protection Agency has removed risk-management-plan records for chemical plants and other facilities that store and use chemicals.
- The state of New Jersey has removed chemical information from its Web site.

Chilling message

In each case, the agencies cited the need to take precautions in the face of the terrorist threat. But it appears they are acting on their own. A White House spokesman said that it has issued no request for agencies to remove materials from their sites. But they have done it with the backing of U.S. Attorney General John Ashcroft. On Oct. 12, Ashcroft issued a memorandum to the heads of all departments and agencies in which he told agencies to carefully consider "disclosure determinations" under the FOIA.

The memo also states: "When you carefully consider FOIA requests and decide to withhold records in whole or in part, you can be assured that the Department of Justice will defend your decisions unless they lack a sound legal basis or present an unwarranted risk of adverse impact on the ability of other agencies to protect other important records."

The memo "sends a chilling message to the entire federal bureaucracy that they better think long and hard before they fulfill an FOIA request or they will be in trouble," said Charles Davis, executive director of the Freedom of Information Center, based at the Missouri School of Journalism in Columbia. "If they want to deny it, the Justice Department is right behind them. In addition, it gives very little credit to the positive values of freedom of information."

Security also was a concern for the FAA when the agency removed a file of enforcement records on Sept. 14 at the request of the agency's general counsel, according to FAA spokesman Paul Turk. But Turk noted that limited access to enforcement information is still available on the Web site; it lacks some of the details that were in the database.

Those details are what *Cleveland Plain Dealer* reporter Beth Marchak says are so important. She used FAA enforcement data to examine the 1996 ValuJet crash in the Florida Everglades.

"You can't make intelligent decisions about safety unless you can look at these records," Marchak said. "In the past, I've used the data to look at how FAA handles enforcement cases. They were settling cases for pennies on the dollar and a lot of cases were just being resolved with paper. People need to know that."

New security restriction

Another database routinely used by reporters to tell their readers and viewers that might be at risk from old, rarely inspected dams was the Army Corps of Engineers National Inventory of Dams. Now, when you go to *crunch.tec.army.mil/nid/webpages/nid.cfm* and click on MAP DISPLAY, you get a screen that says:

Public access to the National Inventory

continued on page 6

access

continued from page 5

of Dams is currently restricted. Please contact the NID Pagemaster if you have any questions. Thank you.

The most recent data on dams is still available online at a Stanford University data query site and from NICAR's data library.

Those with concerns about access to government information don't discount the terrorist threat. But it requires balance with the public's right to know, says Gary Bass, executive director of OMB Watch, a nonprofit organization concerned with freedom of information issues.

"We live in an open society. Everything we put out carries a risk. Are we not going to announce where the next football game is?" Bass said. "The flip of that is we end up living in a closed system."

OMB Watch has come under criticism itself recently for continuing to make risk-management-plan data available. Bass said such information is necessary for citizens and communities to know their risks.

"They could identify the names of these chemical companies, but if you go to the yellow pages you can do the same thing," he said.

The records also provide information about what effects an accident would have. "It will say something like the plume would go 4.3 miles affecting x number of people, two child-care centers and a school," Bass said.

"If I were the parent of a kid in one of those child-care centers, I would want to know that. Doesn't OMB Watch have a responsibility to provide that information to the parents. If we don't do that, aren't we guilty of not doing everything we can to protect them?"

For almost 14 years, Paul Orum, director of the Working Group on Community Right-to-Know, has used public records to try to make chemical plants safer for citizens and to make communities aware of their risks.

"We have pushed for many years for improved site security and hazard reduction at chemical plants," Orum said.

"There has been a great deal of complacency that has accompanied traditional secrecy in the industry. Environment groups and public interest groups have relied on the right to know to push government and industry to make changes as far as hazards."

Haphazard actions

Bass also argues that much of the information was removed randomly without a clear directive. When he's asked agencies for the reasons behind their actions, he's gotten vague responses.

An e-mail response to Bass from the Department of Transportation's information services department said: "Due to the attacks on September 11th, BTS and all other government agencies have had to re-evaluate the content available through our Web pages."

Bass was particularly concerned about the phrase "all other government agencies." He argues that much of these actions have been done without a clear plan.

"We need to have a reasoned debate about this," Bass said. "We shouldn't be acting precipitously to take things down.

"If there is a reasonable argument with reasonable benchmarks. I think we want to hear that and act accordingly. But until then I think in an open society public right to know has to prevail."

"Bin Laden doesn't need a click of a mouse to get this information," Bass said.

Press for information

In the current atmosphere, reporters may have to be more diligent in their requests for public information.

Agencies can't just deny a record without citing a specific exemption to FOIA or a state public records law, said Rebecca Daugherty, director of the Freedom of Information Service Center of the Reporters Committee for Freedom of the Press.

And agencies can't simply invoke national security, Daugherty notes. "If you're going to invoke national security, the records have to be classified. If it has been public before, they can't now reclassify it."

Daugherty also said that reporters should appeal any denials they get and that organizations such as the Reporters Committee can help reporters write appeal letters. She also suggested that reporters ask for expedited review for their requests dealing with Sept. 11 and terrorism. Doing so puts those requests at the front of the line.

"They are probably going to be successful when they do because of the widespread interest," Daugherty said.

Daugherty also emphasized the importance of covering public records issues at this time.

"I don't think the public has any idea how much information is being withheld from them," she said. "Journalists need to challenge closures and write about them."

Jennifer LaFleur can be reached by e-mail at jlafleur@post-dispatch.com

readme.txt

Links

OMB Watch list of information removed from government Web sites: ***www.ombwatch.org/info/2001/access.html***

Reporters Committee for Freedom of the Press: ***www.rcfp.org***

Investigative Reporters and Editors FOI site: ***www.ire.org/foi/***

To follow FOI issues, subscribe to FOI-L or just browse the archives at: ***listserv.syr.edu/archives/foi-l.html***

SPOTLIGHT: TERRORISM

Putting together the data puzzle

By John Perry, *The Oklahoman*

The Federal Aviation Administration probably deserves an award for creativity in thwarting public access to information. The agency's Enforcement Information System database, which includes information about airport security violations, is publicly available. But the FAA releases only sketchy documentation.

Query

lid	Sec_code	Sec_desc
1974SO760024	M140	DETECT X-RAY
1974SO760024	M180	WEAPON UNLOADED
1980AL710001	M100	FIREARM
1980AL710001	M170	WEAPON LOADED
1980AL710002	M100	FIREARM
1980AL710002	M170	WEAPON LOADED
1980AL710003	M100	FIREARM
1980AL710003	M180	WEAPON UNLOADED
1980AL720015	M100	FIREARM
1980AL720015	M140	DETECT X-RAY
1980AL720015	M180	WEAPON UNLOADED
1980AL720020	M170	WEAPON LOADED
1980AL720021	M180	WEAPON UNLOADED
1980AL720022	M170	WEAPON LOADED
1980AL720023	M170	WEAPON LOADED
1980AL720024	M180	WEAPON UNLOADED
1980AL720025	M110	EXPLOSIVE
1980AL720026	M100	FIREARM
1980AL720026	M180	WEAPON UNLOADED

Among the information you can't get: an explanation of the security violation codes. Explaining what those codes mean could endanger airport security, the FAA argues.

After the Sept. 11 terrorist attack, that left newspaper data-crunchers scratching their heads, trying to make sense enough from the enforcement data to evaluate security at their local airports. What exactly is the difference, for example, between security violation code C130, cryptically described in the documentation as "FAIL DETECT – GENERAL" and violation code M140, described as "DETECT – X-RAY." And more importantly, which records represent security failures.

Data revelation

The enforcement data is split into four interconnected tables. For those of us looking at security violations, two tables are of primary interest: the main table that contains one record with general information for each case and a secondary table that usually includes several records with security violation codes for each case number.

Another table connects cases to the specific regulation violated, and another gives the action taken by the FAA in response to the violation.

The first thing I did with the files was to run a series of cross tabulations to see which codes in the violator name, violation source, operation type, certification type and employer fields matched with each other and with the security violation codes.

The first revelation, at least for me, was that the data included not just security lapses by airlines and airports, but also violations by members of the general public — the data recorded not only security lapses, but also security successes.

With only a few exceptions, when the operator type was either passenger or non-passenger, the certification type was "NONE," the violator name was expunged, the violation source was "LOCAL/ST GOVT" and there was an entry in the sex field.

Security codes that matched with the passenger and non-passenger operator type records tended to come from one group of codes, all beginning with an M, that seemed to include things people would get in trouble for: "FIREARM," "EXPLOSIVE," "DETECT – X-RAY," "WEAPON LOADED," "FAILURE TO SUBMIT TO SCREENING."

Crosstabs looking at records where

continued on page 8

readme.txt

Tipsheets

More information on covering aviation disasters is available from the following tipsheets in the IRE Resource Center:

Tipsheet #1210. Includes a list of agency Web sites such as the National Transportation Safety Board and the FAA. It also explains what each site can offer reporters investigating aviation safety.

Tipsheet #613. This package contains a tipsheet for using computer-assisted reporting when covering the aviation community, a sample story from *The Seattle Times*, sources for covering aviation and sample documents from the FAA.

Tipsheet #1211. This tipsheet gives a list of data useful for covering aviation safety and explains how each can be helpful for journalists. The tipsheet also includes a check list of what to do when a plane crashes to help the reporter find the information he or she is looking for more easily.

Tipsheet #1286. This 11-point tip sheet offers helpful advice on how and when to use data in the event of an airline crash, how to prepare the newsroom, which agencies are helpful sources of information.

To order, call the Resource Center at **573-882-3364** or go to ***www.ire.org/resourcecenter***.

Have you found a technical solution that saves you time? Share it as an *Uplink* Tech Tip, a story of 500-1,000 words showing a technique that you'd be willing to share. Please contact Managing Editor Jeff Porter at **jeff@nicar.org** or by telephone at **573-882-2127**.

readme.txt

Stories

Other aviation safety stories available from the IRE Resource Center:

Story #12191. In 1995, *U.S. News & World Report* published an article saying that "When passengers board an airplane, they expect the highest level of safety. In the United States, it is the Federal Aviation Administration's job to make sure they get it.... In a total of five crashes last year, the National Transportation Safety Board (NTSB) indicated that the FAA had fallen short, either failing to enforce its own rules or siding with airlines to oppose what many pilots and passengers considered sensible reform. Commercial air travel in the United States today is safer than in most places. But a three-month U.S. News examination of the FAA's enforcement record reveals significant lapses..."

Story #16047. In 1999, the *Arizona Republic* reported: "The Federal Aviation Administration in Washington waived a $2.5 million fine against America West Airlines in July despite objections from the agency's Phoenix inspectors. America West, slapped with a $5 million fine last year over safety and maintenance violations, had not fully complied with an agreement to fix the problems, according to FAA inspectors in Phoenix who oversee the airline."

To order, call the Resource Center at **573-882-3364** or go to ***www.ire.org/resourcecenter***.

Here's a list of stories, often including Web addresses, written after the Sept. 11 attacks using federal databases, from the IRE Resource Center: ***www.ire.org/store/books/aviation/story.html***.

puzzle

continued from page 7

the operation type was "AIR CARRIER" and the violation source was "SURVEILLANCE" or "SPECIAL SURVEILLANCE/INSPECTION" tended to match with security violation codes such as "FAIL DETECT – HAND GRENADE." These were apparently the incidents where FAA inspectors succeeded in sneaking things past screening stations.

But just to confuse things, in almost every case where the operator type was passenger or non-passenger, there was also the name of an airline in the employer field. So were these airline employees?

The FAA wasn't explaining. But the description of the field in the documentation said it included "violator employer *if applicable, or responsible air operator.*" Since airlines are responsible for passenger screening, the employer field entries made sense.

Filling in blanks

To confirm which records recorded security lapses and which were security successes, I took a clue from the violation source code "LOCAL/ST GOVT" and tried to match the records where the operation type was passenger or non-passenger with our database of local crime incidents.

Our crime incident database goes back to 1992 and is updated monthly by e-mail. The airport is a separate police reporting district to itself, so I pulled all the incident records from that reporting district and matched it with the FAA violation data by date.

In every case, the FAA violations matched with a crime incident record that seemed to match the security violation descriptions.

Our cop reporter pulled the full narrative police reports for the matching incidents, and when we compare the incident narratives with the FAA security violation codes, the data started to make more sense.

For example, a March 26, 2000, security violation in the main FAA table connected with four records in the security code table with the following codes: "DETECT – X-RAY," "FIREARM – HANDGUN," "WEAPON – LOADED" and "WEAPON – CONFISCATED."

The police narrative report said that the X-ray operator detected a handgun in a purse and called airport police. The purse was owned by a Fletcher, Okla., reserve police officer who had forgotten her handgun was in her purse when she came to meet her son-in-law. After a discussion with the FBI, she was released, but the police kept her gun.

The airport is a separate police reporting district to itself, so I pulled all the incident records from that reporting district and matched it with the FAA violation data by date.

The most entertaining incident, however, was coded only as "MISC OTHER" in the FAA data. When asked at the ticket counter if anyone had given him anything to carry on the plane, one man replied, "Just the bomb."

That quip got him a visit with the police and the FBI. He was released to catch a later flight.

John Perry can be reached by e-mail at jperry@oklahoman.com

SPOTLIGHT: TERRORISM

Security problems

By Paul D'Ambrosio, *Asbury Park Press*

As news organizations scrambled to produce special editions Sept. 11, CAR writers and editors were faced with reporting under some of the most difficult circumstances possible.

While the unfolding news changed from minute to minute, communication overloads at the *Asbury Park* (N.J) *Press* and perhaps other news outlets around New York City put a crimp in our usual tools of the trade. Telephone connections were sporadic and, worse, our Internet service was down more than it was up. Our on-site, online servers were overwhelmed with perhaps 10 times as many page views as normal.

Even the day after, it took more than three hours to download the latest FAA security data from NICAR – a 25-meg database that would normally slide through our pipeline within minutes.

The delay pushed the first story about weak security at Newark International Airport right up to our 8 p.m. deadline. I had never used the security data before, but was familiar with FAA terminology and mindset, having written several stories on the administration in the late1990s.

There were two key tasks: use the database to elicit reaction from airline officials, and find real people to tell their tales of security lapses.

Zeroing in with data

In the database, I focused on the SECURITY table, one of four in the FAA data. Pressed for time, I focused exclusively on Newark airport, the departure airport for United flight 93 – the flight that crashed in a Pennsylvania field.

After quickly scanning the security code violations at Newark (coded by its common call letters, EWR) I zeroed in only on two security issues: mock weapons making their way through checkpoints, and unauthorized personnel entering air operation areas, or AOAs. The latter are supposedly secure sites to prevent those bent on destruction from tampering with the aircraft itself.

Both areas were a critical concern since at that point, no one knew how the hijackers got their box cutters or knives on board.

I used security codes C111, and C130 to C139, which focused on security officers failing to detect weapons during undercover tests. A131 and A132 also gave me counts on unauthorized access to AOAs. The FAA cited United Airlines four times in 1999 for screening violations, but only issued warning letters.

Blackout limitations

United and the FAA had imposed a media blackout, so no more information about the lapses could be learned that night. The Port Authority of New York and New Jersey, which owns Newark Airport, provided some background on how security in the terminals worked.

The data had limitations. There was no way to know how many times airport security was tested, so no rate could be developed to compare one facility with another. But, recent Inspector General and General Accounting Office reports confirmed security was a major problem at airports around the county, which added depth to the story.

We also found a local resident who told of walking onto two empty planes just a month before the hijackings. She contacted me after reading our first story. She said she was appalled at the lack of security, which was so lax that an airline worker even helped her get onto one aircraft.

Her experience led to a second story the next day about people entering the sterile air operations areas. The data was again helpful in that area since AOA violations were well noted.

Paul D'Ambrosio can be reached by e-mail at pmd@app.com

readme.txt

Tipsheets

More information on airline security is available from the following tipsheets in the IRE Resource Center:

Tipsheet #1210. Includes a list of agency Web sites, such as the National Transportation Safety Board and the Federal Aviation Administration. It also explains what each site can offer reporters investigating aviation safety.

Tipsheet #729. Covers how to use aviation safety documents when an aircraft crashes in your hometown, including information on what documents are obtainable and how to get them. documents. Audio tape is available through Gaylor MultiMedia, Inc., 888-310-3100, for $6, ask for tape #63.

Tipsheet #613. Explains how to use CAR to cover the aviation community. It includes a sample story from *The Seattle Times,* sources for covering aviation and sample documents from the Federal Aviation Administration. Audio tape available through Gaylor MultiMedia, Inc. 615-361-3611, for $6, ask for tape #14.

To order, call the Resource Center at **573-882-3364** or go to ***www.ire.org/resourcecenter/***

SPOTLIGHT: TERRORISM

Comparing foot traffic

By James E. Wilkerson, *The Morning Call*

Like other CAR reporters across the country, I turned to the FAA enforcement data in the wake of the Sept. 11 terrorist attacks to see what I could find about our local airport.

Going back five years, I found that the Lehigh Valley International Airport had seen relatively little action. That smelled right, considering that it's a relatively small airport in a quiet corner of Pennsylvania.

However, two incidents stood out. In two separate tests conducted within three months of each other in 1999, FAA inspectors sneaked contraband through a passenger-security checkpoint. The entries for the smuggled objects were obscure, but others on the NICAR list had already decoded them as a fake bomb and a fake hand grenade.

Those incidents alone made for an interesting story, but before I started writing I had to put them into context by looking at similar lapses at other airports.

Those incidents alone made for an interesting story, but before I started writing I had to put them into context by looking at similar lapses at other airports. Because the Lehigh Valley International Airport is pretty small, I didn't think it fair to compare it to larger nearby airports in Philadelphia, New York and New Jersey. But I didn't have a clue about how to choose similar airports.

We all know how helpful the FAA has been in working with reporters lately, so needless to say, my call to flaks there for guidance went unanswered.

Enplanement data

I turned again to the NICAR mailing list, where some discussion of airport enplanement data caught my interest. I sent out a message asking for help and I soon had 1999 Department of Transportation enplanement data for all airports in the United States showing the number of passengers boarding planes and passing through.

I used Excel to sort the airports by the enplanement numbers. I eyeballed where our airport fell as compared to others and decided that a spread of 20,000 enplanements below and above our airport would be fair for a rough comparison. Others used different approaches.

Jeff Thomas of *The Gazette* (Colorado Springs, Colo.) chose airports with enplanements from 50 to 150 percent of his local airport, giving him a range of 37 airports, plenty for a fair comparison. Ken Ward Jr. of the *Charleston* (W.Va.) *Gazette*, chose a 25 percent range above and below his airport. He ran the results by an airport administrator, who confirmed that he had a good set of airports comparable to his. David Washburn, of *The San Diego Union-Tribune*, grabbed the largest 30 airports, of which his ranked 28th.

Comparing airports

My method left me with 20 airports. I used the Internet to look at information on each and eliminated a handful that obviously served a very different purpose than our airport, such as one in Nevada that appeared to be used exclusively by tourists into the Grand Canyon area.

Finally, I did the shoe-leather reporting necessary to fill in the gaps. I went out to the local airport to talk to personnel and get a better feel for exactly where the incidents occurred. I also called on security experts to give me some perspective about how the FAA conducts the tests.

On Sept. 21, we ran a front-page story that came as a shock to many readers, not to mention other reporters and editors, who were stunned that FAA inspectors were able to smuggle contraband into airports on such a regular basis.

James Wilkerson can be reached by e-mail at james.wilkerson@mcall.com

readme.txt

Stories

Other stories on investigating security available from the IRE Resource Center:

Story #15930. "Military's lax security putting weapons on the streets," *The* (Sacramento, Calif.) *Bee*. This story documents the General Accounting Office's probes of security at military bases, which lead to theft and sales of the military's weapons, including missiles and explosives, on the street.

Story #17462. "Open Door Policy," NBC News Dateline. This investigation uncovers "dangerous lapses in security at various motel chains across the country."

Story #15346. "High school security," WSOC-TV (Charlotte). This story looks at the reliability of security measures, including hand-held metal detectors, being used by the county school system at high school football games.

To order, call the Resource Center at **573-882-3364** or go to ***www.ire.org/resourcecenter***.

SPOTLIGHT: TERRORISM

Tracking a suspect

By Phil Williams, *WTVF-TV*

It was a phone call that brought an amusing reminder of the value of computer-assisted reporting.

For days, my photographer and I had been chasing down leads and reporting on a possible terrorist suspect who had operated in and out of the Nashville area. So, when the cell phone rang, we thought it might be someone with new information.

Instead, it was an investigator with a top law enforcement agency who had a question for us: Where were we getting our information?

In fact, in the days following the Sept. 11th terrorist attack, I would be repeatedly reminded of how many doors – or, should I say, Windows – have been opened by these CAR techniques.

From computer-assisted reporting to plain gumshoe work, we discovered that the Saudi pilot had come to Tennessee in August to buy two Tampico aircraft that would be used to train pilots.

Right after the attack, our first quick-turn investigation focused on the company in charge of security at Nashville International Airport. Argenbright Security also held contracts at the airports in Boston, Washington and Newark used by the terrorists.

A quick Google search pulled up years of news stories documenting the company's long history of security lapses. Combined with information that Tennessee regulators had caught the company using a security guard with a criminal history, we had our first story on the company's lackluster reputation.

Questions about Argenbright's background aside, that story still didn't answer the question about how well or poorly the company had actually performed at our airport.

Slicing the data

To get at that question, I downloaded the Federal Aviation Administration's enforcement database from NICAR and immediately sliced out only the data dealing with security violations at Nashville International Airport.

In analyzing the results and comparing notes with other NICARians, it became clear that there was lots of information that could easily be misinterpreted. That was especially true, given the FAA's refusal to help interpret the data.

For example, I pulled out the raw number of "security violations" at the airport. But many were cases where individuals were *caught* with weapons and other contraband. In fact, those violations might be an indicator of good security.

So, I decided to focus on a narrow snapshot – violations where security personnel had failed to detect weapons. The result was a story that the security forces had repeatedly flunked tests involving handguns, hand grenades and dynamite bombs.

Finding people

Over the coming days, we would use AutoTrack to background individuals whose names emerged as possible suspects.

readme.txt

Tipsheet

More information on terrorists is available from the following tipsheet in the IRE Resource Center:

Tipsheet #1168. From a 2000 New York conference panel, this tipsheet consists of a list of contact names and organizations to help reporters investigate terrorists and fringe groups.

Story

Another story on terrorists is available from the IRE Resource Center:

Story #16709. "Will Terrorists Go Nuclear?" *American Spectator.* After the 1993 World Trade Center bombing, the National Security Council began investigating terrorist use of nuclear weapons. This story looks at the threat radioactive waste materials pose to the public.

To order, call the Resource Center at **573-882-3364** or go to ***www.ire.org/resourcecenter***.

Links

Anywho, a Web site to find telephone numbers, addresses, maps and directions for business and people in the U.S. ***www.anywho.com***

A Web site locate information about aircraft, pilots and accidents. ***www.landings.com***

But the most interesting development came from a post to the IRE-L listserv by an international colleague. The post was a list of 370 individuals with possible terrorist ties that Finnish banking authorities had inadvertently released.

One of those names, Khaled Alzeedi,

continued on page 12

Q&A From the Lists

Listserv messages you may have missed between members of NICAR-L, Census-L and IREplus-L. To learn about joining these mailing lists, visit www.ire.org/membership/listserv.html.

Flipping a table

Q: How do I flip an Excel table so that the information in rows goes in columns and columns rows?

A: Select the cells you want to flip and hit copy. Open a new workbook or sheet. Then go to PASTE SPECIAL and down near the bottom click on transpose. Then hit OK.

Ranking with Excel

Q: I'm working with election results. We had 27 people contending for nine council positions; choose nine. I'm using the RANK function in Excel to tell me how each candidate ranked within each ward/precinct. Is there a way to write an expression that would boldface any rank/number 9 or below?

A: Simply highlight the entire column and select FORMAT > CONDITIONAL FORMATTING. Select CELL VALUE IS and LESS THAN OR EQUAL TO and type in the number 9 ... now select FORMAT and BOLD and RED and voila ... everything that is less than or equal to 9 should be red and bold.

continued on page 14

suspect

continued from page 11

had a Tennessee address and phone number, as well as an e-mail address for a company at *zidiaviation.com.*

A quick search of *anywho.com* linked the address to an aircraft sales company in nearby Clarksville, Tenn. The phone number belonged to a Hilton Suites in downtown Nashville.

From computer-assisted reporting to plain gumshoe work, we discovered that the Saudi pilot had come to Tennessee in August to buy two Tampico aircraft that would be used to train pilots. Hotel workers recalled that he had claimed to be an Iranian diplomat, and restaurant employees insisted he had been back since the Sept. 11 attacks.

Keep searching

With each new development, I returned to the computer to conduct new searches to see where those threads might lead.

For example, a search of aircraft registrations at *landings.com* confirmed that two Tampicos had been registered to Zidi Aviation in mid-August. Then, with those tail numbers, I went to the Web site for the aircraft sales company and discovered the sale information for the two aircraft – and photos of the actual planes!

Another Google search for Zidi Aviation led to the discovery that the company had been an authorized distributor for flight simulation software manufactured by Jeppesen, a Boeing subsidiary. A Jeppesen attorney refused to comment on the relationship with Zidi, saying she couldn't discuss "anything related to terrorism."

I also came across a reference for another Zidi Aviation e-mail address at *zidinet.com*. But the Web page for *zidinet.com* was nothing more than white type on a black screen, with no links. Our Webmaster suggested that I try a bit of simple hacking and add a "/images" to the URL. Then – *Voila!* – that led to a prototype Web page that showed pilots training to fly jumbo jetliners.

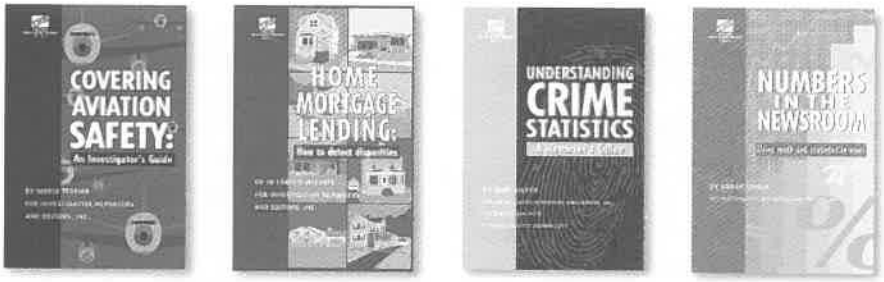
Local police followed our stories, but they reported back to me that they had checked with the local FBI office, and agents insisted they were not looking for Alzeedi. That had other media virtually ignoring our reporting.

So, it came as a relief when The Associated Press, following up on our stories, got confirmation from an assistant FBI director that the agency was indeed searching for Alzeedi.

Phil Williams can be reached by e-mail at pwilliams@newschannel5.com

REQUIRED READING For Your Newsroom

The IRE Beat Book Series



ORDER NOW!

BY PHONE: Call 573-882-3364 with your VISA or MasterCard
BY MAIL: Send your check to IRE, 138 Neff Annex Missouri School of Journalism, Columbia, Mo. 65211
BY WEB: Visit our Web site at *www.ire.org* for online ordering or order form downloads

IRE MEMBERS: $15 each • NON-MEMBERS: $25 each
Plus Postage: First Class-$4 for the first book, $2 for each additional book

SPOTLIGHT: TERRORISM

Detailing identities

By Richard J. Dalton Jr., *Newsday*

Just hours after two planes crashed into the World Trade Center, while all of us were still absorbing the immensity of the tragedy, *Newsday* reporters began writing profiles of the victims for the next day's paper. It has become the newspaper's forte, after winning a Pulitzer Prize for its coverage of the 1996 crash of TWA Flight 800.

Over the next several weeks, reporters gathered names of victims from many different sources: Web sites of companies who lost employees, press releases, relatives, airlines, the medical examiner's office, wire services, death notices, the police and New York State Supreme Court, which, at the request of relatives, issues death certificates for victims.

Reporters then turned to Nexis and AutoTrack to track down the victims' hometowns, ages and phone numbers.

A month after the disaster, we had collected the full names and hometowns of nearly 2,650 victims. The database, now even larger, is available online at *www.newsday.com*.

Profiling victims

The database proved useful for editors to keep track of which profiles had been written. But it also enabled three of *Newsday's* computer-assisted reporting specialists – Robert Fresco, Jo Craven McGinty and myself – to write a story showing just how far-reaching the acts of terrorism were.

Analyzing the database in Microsoft Access, *Newsday's* enterprise team wrote a story revealing that victims came from at least 41 states and the District of Columbia. Using ArcView, we created a map of the United States, highlighting how many victims came from each state. Another map showed the metropolitan area, with various sized dots indicating how many victims perished from each community.

The maps were powerful images, with all but nine states highlighted on the U.S. map and with dots small and large all over the place on the metropolitan area map. The map clearly showed a cluster of victims within easy commuting distance of Manhattan. Most of Long Island's victims, for instance, came from Nassau and Western Suffolk counties, each within an hour or less commute by train. (That's considered an easy commute in New York.)

We showed that the terrorists took the lives of people from more than 770 cities and towns – from Portland, Maine, to Honolulu, Hawaii.

We also produced a chart showing the number of victims in each age group, by decade. More than a third of the victims were in their 30s, and nearly half hadn't yet celebrated their 40th birthday.

Figuring percentages

We then determined the gender, based on the first name of the victim. The Census Bureau provides a database of male first names and female first names at *www.census.gov/ftp/pub/genealogy/names/*, including how frequently each name occurs for men and women. It's a little quirky. For instance, both the male and female databases list "James." But, only one-hundredth of 1 percent of women were listed as having the name "James," compared with 3.3 percent of men.

Of course, some names are both male and female, such as "Jamie" — 0.07 percent of men and 0.15 percent of women. When a name was listed in both the male and female databases, we used the frequencies to determine whether it was male, female or both. So, as expected, "James" turned out to be a male name while "Jamie" could be either. When calculating the percentage of male and female victims, we used only the names that were either male or female, excluding those that could be either.

We then supplemented the Census database with another database of names we found at *www.incompetech.com/named/*. The database is searchable online, and the Webmaster e-mailed us a link to download it.

Using these lookup tables, *Newsday* estimated that three-quarters of the victims were men. (OK, that's a lot of work for something that seemed obvious given the profiles we had been doing. But it gave us an approximate percentage.)

We, of course, revealed the shortcomings of the analysis. Our database was skewed toward mostly male victims of the New York City police and fire departments, which released the names of virtually all their victims. Many of the companies that lost employees have not released lists.

Richard J. Dalton Jr. can be reached by e-mail at rdalton@newsday.com

readme.txt

Story/Tipsheet

Available from the IRE Resource Center:

Story #16854. Michael Paterniti of *Esquire* tells the story of the crash of Swissair Flight 111. He tries to capture the feeling of the crash site and the emotions of the family members and rescue workers.

Tipsheet #538. On Aug. 7, 1994, Bruce Shapiro was among seven people stabbed and seriously wounded in a coffee bar a few blocks from his house. In "One Violent Crime," Shapiro shares the experience of being a victim.

To order, call the Resource Center at **573-882-3364** or go to ***www.ire.org/resourcecenter/***

Q&A From the Lists

continued from page 12

Updating with Access

Q: Is there a way to trim leading and trailing spaces from an Access field by doing an update query or some other function? I tried updating NewField with the expression: =trim([OldField]) and all it does is remove the equal sign and insert the text "trim([OldField])" in the field I'm updating.

A: I just used this one and it worked fine, trimming excess spaces at the beginning or end but not in the middle:

```
UPDATE [Text] SET
[Text].newtext = Trim([oldtext]);
```

Text is the table.
Oldtext and Newtext are the two fields.

To subscribe the NICAR-L discussion list, follow the instructions at *www.ire.org/membership/subscribe/nicar-l.html*. IRE members can read the archives of past NICAR-L messages at *notes.ire.org/nicarl.nsf*.

SPOTLIGHT: TERRORISM

War windfall

By David Wethe & Michael Whiteley, *Dallas Business Journal*

Within hours of the Sept. 11 terrorist attacks, many started to wonder what – if anything – the nation would do to respond.

Texans wondered if their loved ones would get the call to go to war. And the tech companies, machine shops and aviation subcontractors of the Dallas-Fort Worth area – businesses that had accounted for a dime of every dollar spent on Desert Storm – wondered if they could balance the losses to the airline industry with some profit from a new war.

We decided to use NICAR's database of federal contractors to identify and interview some of the companies on the early call lists for the Department of Defense or the Defense Logistics Agency.

We slated the story for a quick turnaround – to appear in next week's issue while the idea was still fresh on our readers' minds.

On Sept. 14, we ordered the Texas share of the database, which covered companies and their federal contract obligations for 2000. It arrived the following Monday morning, giving us time to write a story for the Sept. 21 paper.

Defense contracts

Using Visual FoxPro 6.0, we ran a series of relatively simple queries that split out the defense contracts, finding contractors based in the Dallas-Fort Worth area, summing their contract obligations and sorting in descending order.

We queried NICAR's data into successive tables, culminating with "metrodef.dbf." The values "DD" and "DT" in the field "prtagncy" identified contracts issued by defense agencies, including the DOD, the DLA, the Air Force and the Army.

We queried the table "Fedprc.dbf" with:

```
SELECT *;
FROM fedprc;
WHERE Fedprc.prtagncy = "DD";
OR (Fedprc.prtagncy = "DT");
ORDER BY Fedprc.contractor;
INTO TABLE d:\defense\defquery.dbf
```

We renamed defquery.dbf to "Texdef.dbf" and queried it to isolate contractors' home cities using the query:

```
SELECT DISTINCT Texdef.contcity;
FROM texdef;
ORDER BY Texdef.contcity;
INTO TABLE city.dbf
```

We edited the results to include only cities in Dallas County, Tarrant County and the surrounding counties in the Dallas-Fort Worth area.

We then ran the new table, "city.dbf" against our "Texdef" table using:

```
SELECT *;
FROM texdef  INNER JOIN city ;
ON Texdef.contcity = City.contcity;
INTO TABLE metrodef.dbf
```

Big dollar amounts

The query yielded a table of Dallas-Fort Worth area defense contractors – or at least contractors who did defense work in the Dallas-Fort Worth area last year — with a total of 6,507 contracts worth $7.7 billion. By comparison, our crunch of Texdef produced 19,614 contracts worth $12.8 billion for 2000. That meant the Dallas-Fort Worth area companies handled contracts accounting for 60 cents of every dollar spent in Texas.

The next step was to identify the major players, such as Lockheed Martin Corp., and to sort out the smaller shops that might depend on a DOD call for survival and might add a human element to our story.

We isolated the names of the contrac-

readme.txt

Data

The IRE Campaign Finance Information Center now offers a search page to locate federal contracts. Using the lookup, enter the name of a company, and the database will return any matching contract actions between fiscal year 1992 and 2000. The database includes details such as amount awarded to that business, the work involved and what type of solicitation process was involved. By looking at the "place of performance" field, you can see what jobs are taking place with federal money in your community. You will also eventually be able to connect the company to campaign contributions it made to federal candidates and in some states for which data was available. Because of space limitations, only a portion of the entire database is online. The entire dataset is available for purchase through the NICAR database library.
http://www.campaignfinance.org/fpds/index.html

To view the list of databases available at the IRE and NICAR Data Library, view the Web site ***www.ire.org/datalibrary***. From this page, you can also download an order form. The library's telephone number is **573-884-7711**.

tors and the dollar amount of each of their contracts using:

```
SELECT Metrodef.contnmcifl,
Metrodef.dollaramt;
FROM metrodef;
ORDER BY Metrodef.dollaramt;
INTO TABLE companytot.dbf
```

And we tallied their combined contract values, in descending order, with:

```
SELECT companytot.contnmcifl,
SUM (dollaramt);
FROM companytot;
GROUP BY companytot.contnmcifl;
ORDER BY 2 desc;
INTO TABLE Metrosum.dbf
```

With the help of staff writers Hala Habal and Margaret Allen, we divided the companies and called a healthy mix of those who'd done a brisk business with DOD and DLA in 2000 and those who'd handled smaller contracts.

Early on, we found some irony. Luminator Holding L.L.C. of Plano was expecting heavy losses from a division that makes instrument lights for jet airliners. But those losses were somewhat offset by an emergency order for search lights phoned in from a military base overseas within days of the attack.

In Garland, we found beefed-up security at a company identified as the sole manufacturer of U.S.-certified bombs. In Fort Worth, a company that makes bomb fuses and parts for the Bradley fighting vehicles had received the call to speed up orders.

Also in Garland, a startup quickly received word from the Pentagon to be ready for delivery of its new Thermal Angel, a device that can be used for warming IV fluids in the battlefield.

Quick, easy story

This story was done in a hurry. It was a quick and easy CAR story that can be done in just about any newsroom that has a database manager.

Although no one really knew what kind of war we were talking about, we felt confident many companies in our database would get the call. And one of them offered some news – the possibility that the nation might not be ready for another war.

"I don't think their inventory was that great," said Kyle Blake, vice president of AGH in Fort Worth. "After Desert Storm, the Department of Defense pretty much turned the spigot off. It got behind and never caught up again."

Michael Whiteley can be reached by e-mail at mwhiteley@bizjournals.com

David Wethe can be reached by e-mail at dwethe@bizjournals.com

CALL FOR ENTRIES

2001 IRE AWARDS

The annual contest of Investigative Reporters and Editors, Inc.

CATEGORIES

Newspaper

Television

Online

Other Media:
Magazine/Speciality Publication
Book
Radio

Special Categories:
Renner (crime reporting)
FOI
Student

DEADLINE
January 14, 2002

The contest recognizes the best investigative reporting in print, broadcast and online media, and helps identify techniques and resources used by entrants

For entry forms and additional information, visit our Web site at
www.ire.org/contest

SPOTLIGHT: TERRORISM

Meeting the data challenge

By Justin Mayo and David Heath, *The Seattle Times*

In just a couple of hours, 19 hijackers shattered public confidence in airport security. Even officials at the Federal Aviation Administration, who make the rules and monitor airport security, were so unsure of the system's ability to prevent further hijackings that they kept airlines grounded for three days.

So it was natural for newspapers to ask how safe airports are.

Sea-Tac's rank for gun violations

FAA firearm violations at the top 20 U.S. airports, ranked by violations per passenger

Airport (Numbers from 1999)	Passengers	Firearms	Firearms per 1 million
Los Angeles International	24,006,821	207	8.6
Seattle-Tacoma International	13,062,255	42	3.2
Phoenix Sky Harbor International	16,082,622	46	2.9
McCarran International, Las Vegas	15,310,851	38	2.5
Denver International	17,434,800	43	2.5
Philadelphia International	10,340,097	25	2.4
Orlando International	12,528,500	30	2.4
Dallas/Ft. Worth International	27,580,967	62	2.2
Hartsfield International, Atlanta	37,221,698	77	2.1
Miami International	12,721,257	19	1.5
Lambert-St. Louis Municipal	14,923,259	17	1.1
Wayne County, Detroit	16,562,956	18	1.1
Logan International, Boston	11,066,148	12	1.1
John F. Kennedy Intl., New York	10,136,654	10	1.0
Houston Intercontinental	14,734,821	13	0.9
San Francisco International	16,431,082	13	0.8
Minneapolis-St. Paul International	15,284,009	9	0.6
LaGuardia, New York	10,785,027	3	0.3
Newark, New Jersey	14,903,626	3	0.2
O'Hare International, Chicago	31,482,975	3	0.1

Failures at Sea-Tac checkpoints, 1999

Employees of the Federal Aviation Administration routinely perform unannounced tests of airport screeners at their screening stations, using carry-on bags containing fake guns, knives, grenades and suspiciously shaped, nonmetal or "opaque" objects that resemble explosives

All dates in 1999	Airline	Object	Sanction
March 15	Alaska Airlines	Hand grenade	Warning notice
March 27	Alaska Airlines	Hand grenade	Warning notice
April 23	Alaska Airlines	Toy pistol	$3,000
April 6	Alaska Airlines	Weapon, other	$4,000
June 9	Alaska Airlines	Toy pistol	$3,000
July 21	Alaska Airlines	Opaque bag	Warning notice
July 27	Alaska Airlines	Dynamite bomb	Warning notice
Sept. 15	Alaska Airlines	Toy pistol	$4,000
March 23	Delta Air Lines	Weapon, other	Warning notice
June 24	Delta Air Lines	Toy pistol	$8,725
July 2	Delta Air Lines	Opaque rectangle	Warning notice
July 25	Delta Air Lines	Hand grenade	Warning notice
Dec. 16	Delta Air Lines	Toy pistol	$15,000
July 28	Northwest Airlines	Dynamite bomb	Warning notice
Aug. 1	Northwest Airlines	Weapon, other	Not available
Sept. 14	Northwest Airlines	Hand grenade	$2,800
Feb. 3	United Airlines	Hand grenade	Warning notice
June 28	United Airlines	Weapon, other	Warning notice
Aug. 22	United Airlines	Dynamite bomb	Warning notice
Aug. 24	United Airlines	Weapon, other	$6,250
Oct. 23	United Airlines	Weapon, other	$4,000
Jan. 29	US Airways	Opaque rectangle	Warning notice
April 7	US Airways	Toy pistol	$2,500
May 9	US Airways	Hand grenade	Warning notice
July 21	US Airways	Toy pistol	$9,000

Source: Seattle Times research

THE SEATTLE TIMES

The Seattle Times began looking for information on Seattle-Tacoma International Airport security immediately. The data available through the FAA's Enforcement Information System had serious limitations. What's more, the agency was of little help and in some cases even hostile in our efforts to understand the data.

To supplement this data, we also requested all security incident reports at the airport for two years. We also interviewed employees and managers at airport screening companies, experts at the General Accounting Office and Transportation Department's Inspector General's office and former FAA security officials.

Finding context

The database lists each individual violation of FAA security rules, including the name of the offender, the name of the airport, the date, a description of the violation and what actions were taken for the past 20 years. FAA hires inspectors to test screeners and those violations were listed as "failure to detect" various types of weapons.

We first used the database for a Sept. 12 story, culling general statistics on the number of security violations and proposed penalties for airlines from the database.

But it was apparent that there was much more local detail, especially in the descriptions of security violations committed by airports and airlines. The problem was how to interpret it and put it in context without the benefit of knowledgeable sources willing to talk.

Finding a focus

The mechanics of analyzing the FAA enforcement data are straightforward.

To find security violations, you link the Main table, which contains basic data on the violator and when and where the violation occurred, to the Security table, which has distinct violations for each incident. Then, link to the Actions table to find the FAA's response, including civil penalties, warning letters, certificate revocation, etc.

Early on you have to decide how you're going to define a "security violation." One incident from the Main table could contain several security violations or actions. We decided to focus on incidents, not violations. That meant that if a loaded gun were found in a checked bag, which is against FAA rules, it was counted only once even though the agency may have issued several citations for failing to declare the weapon, illegally storing ammunition and improperly packing a gun.

The main challenge, however, was deciding which security violations to focus on. There are about 250 distinct security codes that airports, airlines, passengers or mechanics could be cited for violating. Most were cryptic, such as failure to detect "encap weapon." We were unable to decipher that description before our deadline.

To narrow our scope we looked at weapons violations.

The enforcement data can be divided into two broad categories of weapons violations: those where the security system failed and those where it worked. In the Security table the "failure to detect" codes show where airline screeners let FAA inspectors slip test weapons through undetected. These failures are detailed by date, airline, type of test weapon and in many cases even the specific concourse where the violation occurred. We used these failures to document problems

continued on page 21

readme.txt

The stories mentioned in this edition of *Uplink* will soon be available from the IRE Resource Center. Search the story database at ***www.ire.org/resourcecenter*** for order numbers. Call **573-882-3364** to order these and other investigative stories.

Tech tips...

Doing cross tabs can create quick comparisons

By Jeff Porter, *IRE/NICAR*

Call it an art form – rearranging data in a useful way, comparing fields across columns instead of down long rows. The spreadsheet program Excel calls it a pivot table. Database managers often call it a cross tab. For Visual FoxPro users, it's a fast, quick step to compare hundreds of thousands of records instantly.

Take, for example, Small Business Administration disaster loan data. The loans themselves are the primary form of federal assistance for nonfarm, private-sector disaster losses. The loans help homeowners, renters, businesses of all sizes and nonprofit organizations finance their rebuilding. The loans, which are repaid to the Treasury, are provided at low-interest rates and have tailored repayment schedules befitting each borrower's financial capability.

To create a cross-tab comparison, the rules are simple.

You want three fields. Ideally, the first has the most potential variables. Using the SBA disaster loan data, we'll compare states and a few other geographic areas, such as territories.

In the second field, you want to limit the number of variables, technically, to 255. In practical terms, you want just a few variables. In the SBA disaster loan database, there's a field called CHGOFF, noting whether a business disaster loan is deemed uncollectible. It's either a YES or NO – just two possible variables and perfect for a cross-tab.

The third field is the data field, a total count or sum, for example, categorized by the two other fields. For this example, the count will be categorized as the status of each loan in each state.

For Visual FoxPro 5.0, here's the SQL to first list the borrowers' states, whether the loan was charged off, and the total number for each category by state. The query limits the type of loan to just businesses – coded as a capital B in the data — not individuals, because the SBA won't tell the status of an individual's loan. In this example, the number of loans is limited to those since the beginning of 1990 to businesses:

```
select borstate, chgoff, count(*)
from disaster;
where apprdate > {12/31/89} and
type = 'B';
group by 1, 2
```

The results would look like this:

Query

Borstate	Chgoff	Cnt
	NO	1
AE	NO	1
AK	NO	68
AL	NO	97
AL	YES	2
AR	NO	216
AZ	NO	10
CA	NO	150
CO	NO	25
CT	NO	20
DC	NO	37
DE	NO	4
FL	NO	829
FL	YES	4
GA	NO	161

Helpful, but only slightly. Now, one could export results to Excel and create a pivot table to show the CHGOFF variables across the top of the spreadsheet and the states down the side, but Visual FoxPro can do it quicker. Just use one line of SQL in the software's command window:

```
do(_genxtab)
```

With this short command, you've created a new table called Xtab, created in the software's default directory. It should, though, be already open, so simply type

```
browse
```

And you should see this:

Xtab

Borstate	No	Yes
	28	4
AA	2	
AE	8	
AK	695	29
AL	1416	117
AP	4	
AR	642	25
AS	179	41
AZ	340	38
CA	36787	4752

Better – at least one can read across and see in a glance how a particular state is doing. Note here, for example, that in California, 36,787 loans aren't in trouble, while 4,752 are categorized as uncollectible.

What's that as percentage? Again, one could export over to Excel; instead, though, one could run one last, quick query to show the result. For this example, the number of total loans is limited to 101 or more by state or territory, to leave out areas with a tiny number of loans that might skew a comparison:

```
select borstate, no, yes, yes/
(no+yes) pct from xtab;
where no+yes > 100;
order by 4 desc
```

The query creates a new field – the number of loans charged off, divided by the total number – and names it PCT, short for percentage. Also added: The last line tells FoxPro to sort the records by highest percentage to lowest, finding the states with the highest percentage of loan default.

The answer:

continued on page 27

HOUSING

A problem company

By R.G. Dunlop and Mark Schaver, *The Courier-Journal*

Code enforcement seems like a ripe subject for computer-assisted reporting, and that is where reporters and editors at *The Courier-Journal* (Louisville, Ky.) turned when they first considered a housing project in mid-2001.

What they found, however, was a government database that contained potentially key information but needed lots of legwork before it could be unlocked.

What followed was an example of how traditional reporting and database analysis supported and strengthened each other.

Based on preliminary, anecdotal evidence, the newspaper decided to focus on a controversial apartment-management company, River City Properties, Inc., whose sprawling, low-rent complexes were located mostly in Jefferson County, outside the city limits of Louisville.

The county was of particular interest because it contained nearly as many rental-housing units as did the city, but had less than one third as many housing code-enforcement inspectors. And the Jefferson County Health Department, which is responsible for code enforcement in the county, was reportedly strapped for resources.

Rental units in the county were spread across 323 square miles, an area more than five times larger than the city itself and a logistical challenge for a mere handful of inspectors to navigate. And housing stock in the county, while generally much newer than that in the city, was aging to the point that decline was beginning to surface in some neighborhoods. Without inspectors' vigilance, we thought, landlords could take liberties.

The first hurdle was obtaining the database, which was maintained not by the local health department, but by the state Cabinet for Health Services, of which local health departments are a part.

Sketchy database

After a series of telephone calls, and written requests under Kentucky's Open-Records law, we got the database in Access format, making it easy to work with. Unfortunately, however, it provided only sketchy information for four years' worth of code-enforcement inspections – about 7,000 total – that were available.

Each complaint had a unique control number and was logged by date and by address. But, landlords' names and corporate affiliations, if any, were listed only occasionally.

Because of the missing ownership information, the health department couldn't assemble an overall inspection history for a particular property owner or manager, or even for a specific address. So how could we? And unless we knew the history of enforcement and the results attained, how could we judge the effectiveness of the health department's code-enforcement program?

If there was a solution, we decided, it lay in the street addresses contained in the database. By assembling the addresses of every property managed by River City Properties, we could begin to unlock its code-violation history as shown in the database.

To determine River City's apartment holdings, a reporter searched tax records and reviewed about 60 personal-injury and other lawsuits filed over a 20-year period against the company, its president, Garey Higdon, or the individual apartment complexes managed by River City Properties and owned at least partially by Higdon. Interviews with code-enforcement officials, attorneys, realtors and representatives of various advocacy groups revealed still more about River City's real-estate empire.

Missing information

But neither the lawsuits, the local tax records, nor the sources disclosed the crucial piece of information necessary to link the properties to the health department's database. That missing link was a comprehensive, up-to-date list of addresses for all the apartments in a particular complex.

Without those, complaints in the database couldn't be tied to a common

readme.txt

Stories

Other stories on housing problems available from the IRE Resource Center:

Story#17226 *New Times Los Angeles* reported that "slum properties can be shuffled among a small cadre of co-conspirators, keeping law enforcement and housing activists at bay," revealing "how a slumlord managed to defy the best efforts of housing enforcement officials and his own tenants to bring a substandard building up to code, even when he was slapped with a $455,000 judgment."

Story#15948 *The St. Paul Pioneer Press* published a three-part report on "chronic problem properties" and the effect they have on the Twin Cities. "At the heart of the issue," the newspaper reported, "is a badly broken system, rife with legal loopholes, spotty enforcement and too few penalties for lawbreakers." The newspaper found that "more than 6,400 properties in St. Paul and another 22,000 in Minneapolis have failed to comply with housing codes for two years or longer," inspectors are unwilling to crack down on the offenders and "a small group of landlords account for a disproportionate number of complaints."

source – in this case, a single property manager. We would not be able to determine River City's violation history or the health department's handling of it.

Finding the addresses was time consuming. River City wouldn't help – Higdon refused to be interviewed and his attorney declined to provide the names or locations of properties managed by River City. The telephone book and the city directory provided only the address of an apartment complex's main address as determined by local planning and zoning officials, and did not account for addresses among the various buildings in a complex.

Some of the company's complexes were crisscrossed by as many as eight or 10 streets. To determine conclusively how many complaints each complex generated would require knowing the street names and numbers for each building in each complex. To get this, a reporter went to each apartment complex associated with River City Properties – more than 40 in all.

Some streets, and some buildings, were unmarked or incompletely identified with names or numerals. The sketchy and often outdated public records that were available sometimes conflicted with visual observations. But eventually, by checking and rechecking, the newspaper was able to compile an address list with which reporters and editors felt comfortable.

Cleaning the data

Ultimately, the decision was made to focus on 17 complexes managed by River City Properties, Inc., and owned at least in part by Higdon. Other properties owned by Higdon but sold long ago were eliminated, as was another set of apartments currently or formerly owned by one of his brothers.

The newspaper constructed its own Access database of River City-managed properties, including tables for owners, street addresses, lawsuits and tax assessments. The addresses in that database were then matched against the county health department's database to determine how many housing-code complaints River City Properties' complexes had generated.

This couldn't be done with a simple query, however.

The county health department's database was dirty, with many streets misspelled or misnamed. So we created a new column in the database to put corrected street names, while preserving the uncorrected ones in case there were questions later. This made it easier to pull out the right properties and enabled us to calculate counts on complaints for each complex.

By assembling the addresses of every property managed by River City Properties, we could begin to unlock its code-violation history as shown in the database.

Because there were so many addresses, we decided that the simplest and surest approach for finding River City's properties would be to go through the database record by record, looking for the ones that matched the addresses the reporter had compiled.

We created a separate table of just River City complaints by deleting non-River City complaints from a database copy. That gave us two tables: one for all complaints, and one for just River City's.

Although this was a crude way to do it, it was the surest and most straightforward. Having a separate table of just River City properties made it easier to work with. We were confident these were the right properties, because we had examined each record individually, leaving out any that didn't clearly belong to River City.

The results were still striking: more than 1,200 complaints filed with the health department during the four-year period were tied to River City's complexes. And, the vast majority of complaints were anything but frivolous. Nearly 70 percent resulted in either a violation or an inspector taking some other sort of action, including a follow-up visit to the site of the problem.

Herculean task

The newspaper also devoted many hours to pursuing a database maintained by the City of Louisville, which has a separate housing inspection office. Although only a few River City properties were in the city, we also wanted to look at the company's violation history within the city. Obtaining city's records was complicated by the fact that the city's database was on a mainframe using decades-old CA Datacom/DB software that no one still employed by the city fully understood.

The city's computer staff ran previously created programs to generate reports from the database, but no one understood how the dozens of tables that made up the database were linked together and nobody was skilled at programming it. When the city had questions it couldn't answer, it called on a former city employee who now worked as a contractor.

Under Kentucky's Open Records law, agencies are required to provide electronic records only in their native format or as ASCII text. The city initially told us that the database would cost us $100,000 to obtain, because we would have to have purchase the original software to use it.

We knew this was nonsense, but we were afraid that even if we pursued a long records battle and obtained the database for a minimal cost, there was the chance we wouldn't be able to

continued on page 27

SPOTLIGHT: TERRORISM

Lessons from disaster

By Jeff Porter, *IRE/NICAR*

Be prepared, say the Boy Scouts. In the last few months, more and more journalists are saying it, too.

Indeed, one of the consistent lessons from almost any disaster is to keep a warehouse of data, preparing it for instant use for the next catastrophe. The advantages are twofold: There's no wait for the data, and reporters, without the pressure of disaster, can begin understanding the best uses and pitfalls of the data.

Case in point: FAA enforcement data, which many newsrooms used to focus on security breaches in airports after terrorist attacks killed thousands on U.S. soil.

The Web searches can be excellent starting points, especially on deadline, but only in a limited way.

"It was obvious on Sept. 11 that airport security had failed dreadfully," says Ron Campbell with the *Orange County Register*. "The FAA database showed that the failure was systemic. It showed many, many failures at every major airport nationwide for several years. It showed that the system worked on Sept. 11 exactly the way it was designed to work — badly."

The database, though, has its own limitations. It's often cryptic and open to interpretation (see numerous accounts of the use of the data in this edition of *Uplink*). While the data included the cases in which FAA inspectors penetrated airport security during surveillance, it didn't include those times when airport screeners caught them. The database, after all, is about enforcement actions. If the airport screeners did their job, no enforcement action is required.

"As valuable as the FAA database was, it has huge gaps," Campbell says. "We don't know how many times security caught the FAA trying to penetrate security, so there is no way to determine which airports had the worst security. We can't even compute a nationwide security breach rate, since the FAA won't say on a national level how often they tried to breach security but were stopped by alert guards."

Citing vague security concerns, the FAA refused to answer even rudimentary questions about the data.

Years before the terrorist attacks, Elizabeth Marchak of *The Plain Dealer* (Cleveland, Ohio) pushed preparation for aviation disasters. Never, she wrote in a conference handout that's available from the IRE Resource Center, use data on deadline you've never seen before.

By their very nature, databases are incomplete, according to Marchak, and it takes some experience to fully understand those limitations.

Online aviation data

There are a few shortcuts, thanks to the World Wide Web, that allow reporters to look up simple information about aircraft, pilots, accidents and incidents. So part of preparing for disaster coverage is conscientiously bookmarking Web sites. Numerous IRE tipsheets show Web addresses that would help. Again, though, the searchable online databases are incomplete and limited. It pays to read the fine print even on a government Web site.

The FAA Flight Standards Service Web site promotes itself as providing safety-related information, and in fact, it's a place worth bookmarking. Reporters can look up airworthiness directives and recent service difficulty reports, search for pilot schools, and link to search pages for accidents and incidents, both from the FAA and the NTSB.

Another FAA Web presence: the FAA Civil Aviation Registry, where a reporter can look up ownership of an aircraft, by registration number or serial number.

A non-government but useful Web site comes from Aviation Research Group/US Inc. You can sign up to receive preliminary accident information via e-mail for free. According to the company's Web site, several times a day it downloads the FAA's preliminary accident files, then sends out automatic notifications to e-mail subscribers. You can choose categories and filters, too. For example, you can choose to receive only notifications of all multi-engine airplanes, or just single and multi-engine jets, or just helicopters.

Like the databases residing on a reporter's desktop or a newsroom's network, though, Web-based or e-mailed data have limitations, too. The FAA's lookup information on service difficulty reports, for example, only go back to 1995. The actual database of SDRs, though, goes back to 1974. One can look up ownership of particular aircraft through the FAA Civil Registry Web search, but it's problematic to summarize and count how many airplanes of a certain type are owned by a particular company.

readme.txt

Links

FAA Flights Standards Service:
av-info.faa.gov/

FAA Civil Aviation Registry:
registry.faa.gov/

Aviation Research Group/US Inc.:
www.aviationresearch.com

Preparation is key

The Web searches can be excellent starting points, especially on deadline, but only in a limited way. They don't take the place of actually obtaining and understanding the data.

And that should take place not in the heat of a disaster, but beforehand, when authorities are less harried and, in the case of the FAA, might be more open.

"The FAA database taught me a lesson for the future," Campbell says. "When getting government databases, always find out how the data is compiled. In the case of the FAA database, we know that airport security guards, airport security coordinators and FAA inspectors all must have filled out reports. There is undoubtedly a manual telling these folks how to fill out reports, explaining for example when to charge multiple violations for a single offense. But we don't have that manual, and it's extremely unlikely post-Sept. 11 that the FAA will give it up."

Jeff Porter can be reached by e-mail at jeff@nicar.org

challenge

continued from page 16

at the Seattle-Tacoma airport and to show how many test objects — pipe bombs, hand grenades, pistols — the screening system let through.

Finding answers

We decided against comparing Seattle's results to other airports because at that time we had no way tell how frequently the FAA tested each airport. We were concerned that FAA inspectors in some jurisdictions might be more diligent than in others, making comparisons impossible.

We knew from the book *Flying Blind, Flying Safe* by former DOT Inspector General Mary Schiavo that Sea-Tac screeners had detected explosive devices only 12 percent of the time in tests – one of the worst performances in the nation.

The data show the security system working when real weapons are discovered, usually because a passenger fails to declare a gun in a checked bag or has one in their carry-on. Guns were frequently discovered in checked bags at Sea-Tac, even though few checked bags are put through X-ray machines or bomb-detection devices. We used these violations to calculate the number of firearms found at major airports and computed a rate based on domestic enplaned passengers. Sea-Tac ranked second in the country in 1999.

Supplementing the enforcement data, local police records and other sources showed that the FAA seriously underreports incidents involving weapons. Port of Seattle records showed gun violations, mostly minor, occurring almost every day at the airport — everything from a passenger failing to disclose that a weapon has been stored in a checked suitcase to trying to walk through the metal detector with a concealed handgun strapped to an ankle holster.

Finding sources

Besides reporting the data, we interviewed a 38-year-old screener, Teuila Tuitele, who said that the training she received inadequately prepared her for the job. She had some classroom training during her first week and passed a multiple-choice test asking how she should handle irate passengers or what to do if she detected a weapon on the X-ray machine. She was shown and tested on how to identify suspicious bomb-like shapes. She said screeners needed only an 85 percent detection rate to get assigned a job.

It is not uncommon for a screener to sit at the X-ray machine for two or even three hours without a break. "Sitting there more than 30 minutes you fall asleep," Tuitele said. "It's like watching the TV."

Justin Mayo can be reached by e-mail at jmayo@seattletimes.com

David Heath can be reached by e-mail at dheath@seattletimes.com

readme.txt

Data

The IRE and NICAR data library offers these databases that can pinpoint information:

FAA Enforcements A database of FAA enforcement actions against airlines, pilots, mechanics, and designees.

FAA Service Difficulty Reports: A database of maintenance incidents collected by the FAA for the purpose of tracking repair problems with commercial, private, and military aircraft, and aircraft componentry.

FAA Accidents and Incidents: A database of mainly U.S. flights where there was an accident or an incident, including crashes, collisions, deaths, injuries, major mechanical problems or costly damages.

FAA Aircraft Registry: A listing of all aircraft and aircraft owners registered in the United States.

FAA Airmen Directory: The FAA Airmen Directory is a listing of pilots and other airmen, including the type of certificate(s) they hold and their ratings.

NASA Air Safety Reporting System: A database of anonymous reports of airplane safety submitted by pilots, flight attendants, air traffic controllers and passengers.

For more information about the database library's collection, including purchase prices, go to ***www.ire.org/datalibrary/databases/***. To order data, contact NICAR at **573-884-7711** or download an order form at ***www.ire.org/datalibrary/orderform/orderform.pdf***

SPOTLIGHT: TERRORISM

Fighting the airport

By Alan Judd and Maurice Tamman, *The Atlanta Journal-Constitution*

Ben DeCosta runs the world's busiest airport, Atlanta's Hartsfield International. So on Sept. 26, when *The Atlanta Journal-Constitution* reported on Hartsfield's history of security breaches, DeCosta was not happy.

In DeCosta's view, the story, based on the Federal Aviation Administration's database of security violations, did nothing more than confirm the worst fears of air travelers days after terrorists hijacked four planes to attack New York and Washington.

What's more, he said, "they have no right to have their worst fears confirmed."

DeCosta's comment typified the official reaction to unsettling post-Sept. 11 revelations about the safety of the nation's air travel system. After the *Journal-Constitution* and many other newspapers wrote stories off the database of violations, the FAA quickly pulled it from its Web site.

(This shouldn't have been surprising; a few years ago, after several stories appeared on the alarming rate at which airport security screeners failed to detect fake bombs and other weapons planted by the FAA, the government declared the information to be "security sensitive" and restricted public access.)

Aviation focus changed

Before Sept. 11, reporting on commercial aviation often focused on matters of convenience: flight delays and limits on carry-on baggage.

After Sept. 11, when news organizations began examining the far more important issues of safety and security, the new scrutiny made the people who run the air travel system more than a little uncomfortable.

In Atlanta, DeCosta virtually accused a reporter of being unpatriotic for reporting on the security breaches.

Noting that passenger loads on airliners had dropped by 40 percent the week after air travel resumed, DeCosta said: "What the public needs is more than your newspaper gives them. You have a special responsibility not to exaggerate and exacerbate an already bad situation. Get people to focus, instead of scaring the hell out of them."

Not that officials were going to make our reporting on anything at the airport easy.

Barricades to reporters

Reporting about the airport required access to concourses and terminals, but airport officials would not allow the press access beyond the security gates leading to the terminal trains and gates.

In the week after the attack, we attempted to document how little business was being done at what we routinely describe as the world's busiest airport. That required getting behind the security checkpoint.

We solved the problem by purchasing unrestricted full fare tickets. The reporters, however, had to be careful. The reporters needed to order the ticket online for a flight within a few hours of the period they would be working behind the lines.

The reporters did not check in, but presented a printout of the Web page ticket confirmation page. In one case, the ticket cost $987.

After that, it was through the metal detectors, past the security guards and out to the terminals.

It's quite remarkable that reporters were considered such a security risk that they were not allowed out to the terminals. Meanwhile, any shlub with a home computer and a printer could re-create a confirmation Web page, print it out and have complete, unfettered access to the terminals.

After passing in and out of the terminals at will, the reporters had to get in line at a ticket counter, before their flight was scheduled to depart, and get a refund.

Airline employees

With passengers jittery about flight in the days that followed the reopening of airports, it was clear airline employees were worried. While airport officials were useless, airline employees were polite, friendly, even plaintive.

In one case, a Delta employee behind one counter pleaded with a reporter not to cancel his round trip ticket to Orlando.

He asked several questions about why the reporter was not flying.

Do you know flying is safe? Do you know there are no delays? Yes it was expensive, but why not go?

Then he squinted suspiciously at the black-haired, bearded reporter. He waited a few seconds, before pressing a key on his keyboard. A receipt printed out.

"You will receive your credit within 30 days," he said.

Maurice Tamman can be reached by e-mail at mtamman@ajc.com.

Alan Judd can be reached by e-mail at ajudd@ajc.com

readme.txt

Have you or one of your colleagues recently published stories using CAR, either one of particular note or someone's first CAR story after attending an IRE and NICAR Boot Camp? If you have a story idea, we'd like to hear from you. Please contact Managing Editor Jeff Porter at ***jeff@nicar.org*** or by telephone at **573-882-2127**.

INTRANET

Cheap, easy solution

By Andy Crain, (Sarasota) *Herald-Tribune*

Your boss asks you to build "one of those intranet things." It's a top priority and must be finished quickly, your boss says, patting you on the back. And oh yeah, there's no money in the budget for this.

Impossible? Actually, no.

Developing an intranet, one that's hooked up to databases and full of all sorts of dynamic features, is well within the capabilities of even the most overworked CAR grunt. All it takes is a Web server and ColdFusion Express, the free, trimmed-down version of the popular and expensive Web application server.

You'll have the support of an easy-to-learn language, great documentation (the kind that comes with commercially distributed software, which is ColdFusion's main enterprise) and a huge ColdFusion programming community. Best of all, you can get away with all this without spending a penny.

At the (Sarasota) *Herald-Tribune*, I created such a system without a single software purchase. Reporters and editors query research databases, search in-house and AP stylebooks, share sources, request and assign photos, participate in discussion forums, and more.

Big hits, low cost

In an average week, the site responds to just under 5,000 page requests and sends 150 MB of data to over 160 distinct addresses, using free software and Microsoft Access databases. Even the hardware's low-budget: an old PC running Windows 95 with 32 MB of RAM.

The popular intranet model is to build "dynamic" Web pages that change and present different views depending on information stored in a database.

Doing this typically requires a Web server, which sends out pages formatted in HTML in response to user requests, for example the clicking of a link to a new page; a database server, which stores the always-changing information that is presented in these pages; and some sort of "glue" to link everything together.

You could hook up an enterprise database server, such as Microsoft's SQL Server, with Microsoft's IIS Web server and use ASP to build dynamic, database-driven pages. All well and good, if you have the cash to pay for it.

Or you could try an open-source solution. A combination of a MySQL database server, an Apache Web server, and PHP to build the pages and link everything together packs just as much punch, but with a much more appealing price tag: $0. The downside is a much steeper learning curve and cumbersome, sometimes spotty documentation. Although this solution has a lot going for it, if you're pressed for time, it's probably not the right one.

Enter ColdFusion Express, which combines all the benefits of a commercial solution with one of the more appealing features of open-source software (it's free).

ColdFusion Express Server (download it at *www.macromedia.com/software/coldfusion/trial/cf_server_express.html)* is distributed as a teaser for Macromedia's ColdFusion Server. Presumably, the company hopes that you'll ultimately purchase their flagship product, which goes for between $1,300 and $5,000.

ColdFusion limitations

As a result, ColdFusion Express lacks some of the features of the full-blown product. For example, there's a cap on the number of simultaneous connections to the server. ColdFusion Express supports a maximum of five.

This isn't as bad as it sounds. Connections last mere milliseconds, so dozens, even hundreds, of users can be clicking around via ColdFusion Express at the same time.

Also, there is limited native driver support for databases.

If your data is in Oracle, IBM's DB2, Informix, SQL Server, or some other high-end database, you'll need the cash-money version of ColdFusion. ColdFusion Express works only with desktop databases and has native drivers for Microsoft Access, Paradox, dBase, FoxPro, Excel or Lotus Approach.

With drivers for Access and other database systems, ColdFusion Express becomes a virtual database server, running queries itself and returning results. You don't even need Access on the server; ColdFusion reads and processes .mdb files directly. Many times, ColdFusion will process some complex queries faster than Access.

Anyone familiar with HTML will feel at home with ColdFusion, which is completely tag-based. A ColdFusion application is nothing more than a typical HTML document with ColdFusion tags inserted in among the HTML tags. Requests for ColdFusion pages are sent first to the ColdFusion Express Server, which will process the tags, query databases and whatever else it's told to do, and then return the results to the Web server as HTML.

Andy Crain can be reached by e-mail at andy.crain@heraldtribune.com

readme.txt

Links:

To download ColdFusion Express Server go to: ***www.macromedia.com/software/coldfusion/trial/cf_server_express.html***

To browse the documentation, including a great ColdFusion tutorial included in the software go to: ***futurecar.umd.edu/CFDOCS/***

For more on ColdFusion, go to: ***www.macromedia.com/software/coldfusion/***

tests

continued from page 1

Information Act request for data on teacher certification. In the end, we made some startling discoveries – such as the existence of a special education teacher who had failed 24 of 25 tests. (In Illinois, teachers must pass a Basic Skills test – which contains sections on reading, grammar, math and writing – and a subject matter test in the area in which they plan to teach.)

Needy schools

We learned that the largest proportion of flunkers were concentrated in the neediest schools: those with the poorest and lowest achieving students, and those with the highest percentage of minorities. We also identified 635 full-time teachers who had never passed the Basic Skills test required for a regular Illinois teaching certificate.

But the road to these findings was bumpy. It took us five months to figure out what data existed and convince the state the give it to us. Nobody we interviewed was able to answer questions on all the data. And nobody had ever conducted the analysis we were attempting. We would find someone who could explain one aspect of the database to us, but who had almost no knowledge of the rest. What's more, outdated records and duplicates had to be identified and corrected. We were also under a unique deadline: I was solely responsible for the analysis and was expecting my first child at the end of the summer.

Our biggest hurdle was pulling together the information we needed into a usable database. The data resided in several different departments at the state Board of Education. One file contained the names of every person who had taken a test since 1988, which tests they took, when they took them and whether they passed or failed. Raw score data was available in a separate file for tests taken since July 1999. Another database listed the certificates held by each Illinois teacher.

A fourth file contained information on each teacher's assignment—where and what they were teaching. A fifth file—one we already had on hand from a previous project—gave us important information on each public school in Illinois, including breakdowns by race and income.

Another file from a previous FOIA provided us with the most recent student scores on state exams. This file, which contained records for each Illinois student (minus names and Social Security numbers), allowed us to examine the correlation between teacher performance on certification tests and student achievement.

Linking the tables

Individually, the data didn't tell us much. Together, they had the potential to give us powerful information on the state's teaching force. But there was a problem: The only way to merge the teacher test score databases and the files on teaching assignment and certification was by linking the fields containing the teachers' Social Security numbers. And the state is prohibited from releasing test score data, which meant they could give us a file with scores, but couldn't tell us to whom they belonged.

So we decided to ask the state to replace the Social Security numbers of everyone who appeared in a database with random numerical identifiers. To do this, they needed to merge all the files, assign the identifiers, strip out the Social Security numbers and names, then split the data back into manageable, linkable files. After several months of FOIAs and negotiations, we took our plea, in person, to state Superintendent Glenn "Max" McGee. We argued, in part, that the release of this data would perform a tremendous public service. McGee agreed to give us the data—for free. We agreed not to use the data to identify individuals.

They posted the data for us on an FTP site as simple text documents. I imported them into Paradox, my preferred database manager. Using the identifiers, I was able to link the individual files. I ended up with data on nearly 166,000 tests taken by more than 67,000 public school teachers. Although the focus was on teachers, I also examined a larger file that included administrators and other educators.

Power with SPSS

But the real power came when I pulled in poverty, race and student achievement data for each Illinois school. I did this part of the analysis in SPSS.

I began with poverty, dividing all Illinois public schools into five equal groups based on the percentage of low-income students at those schools. I threw out the three middle groups and compared the lowest income and highest income schools using several simple measures, including the percentage of teachers who had failed at least one test. We also compared the percentages of teachers who had failed Basic Skills tests, the percentage that had never passed a Basic Skills test and the percentage that had failed two, three, five and 10 or more tests.

I used a similar method for race and achievement. With the latter, I used a statistical method called standardizing to create a composite score for each school based on its students' performance on state tests taken the previous year. (I needed to standardize the data because I was lumping together third-, fifth- eighth- and tenth-grade scores on math and reading tests, and not all schools had all four of those grades. The eighth-grade math test, for instance, was the most dif-

readme.txt

Story

The *Sun-Times* series on testing teachers is available in the Resource Center, **story #18367**.

To order, call the Resource Center at **573-882-3364** or go to ***www.ire.org/resourcecenter/***

The series is also available on line at ***www.suntimes.com***.

ficult, and we didn't want to penalize schools that had an eighth grade).

The startling results: The lowest-income, lowest-scoring, highest-minority schools were about five times more likely to employ teachers who failed a competency test than the highest-income, highest-scoring and lowest-minority schools.

Improving teacher quality

The data was rich and offered many other avenues for analysis. We used it to rank schools and districts based on the percentage of teachers who had flunked a test, and to identify districts that were using loopholes to hire teachers who had never passed a Basic Skills test. We pulled out examples of teachers who had flunked multiple tests, and examined raw score data to determine precisely which types of questions they had gotten wrong. An analysis of teaching assignments showed us that bilingual education teachers were disproportionately likely to have failed tests. And an examination of the raw score data showed us that since 1999, more than a quarter of all teachers who had passed the Basic Skills had come within only five points of failing.

The response to our three-day series, which ran in September, was tremendous. In late October, a state legislative committee began hearings to explore ways to improve teacher quality, especially in the neediest schools. The state Board of Higher Education scheduled a discussion of the series to examine the implications for colleges of education. The Chicago Board of Education promised to post on their Web site the percentage of teachers who are certified. They are also began insisting that full-time substitutes obtain their certificates—and thus pass the Basic Skills test—within two years of being hired. Gov. George Ryan called an education summit in part because of our series.

Oh, and we made our deadline: The series ran exactly a week after my daughter was born.

Becky Beaupre can be reached by e-mail at beaupre@suntimes.com

problem

continued from page 19

make sense of it once it was in our hands. Even if we had all the data, we had no idea of the relationships between all the tables, and it could have been a Herculean task to figure it out.

The Courier-Journal decided the best solution would be to pay the $600 the city said it would cost to hire the former employee to write a program that would pull from the database just the records and fields we wanted in a single, flat file. As an added bonus, we got the records in Access format, which wasn't a requirement of the law.

This database showed River City Properties had a large number of complaints at its city complexes as well, although that finding ultimately played only a small part in our series.

Stories and results

River City officials had long argued that complaints were not a fair barometer by which to judge the condition of its properties. Large and numerous apartment complexes naturally generate more complaints, company officials contended.

The newspaper found, however, that River City's 25 percent share of all complaints filed with the county health department during the period far exceeded the company's share of the rental housing market in the county, as determined by census data. The company's share was less than 4 percent.

After the newspaper published a three-part series about River City Properties and the health department in October, the company publicly pledged to do a better job and the health department admitted that it was under funded and understaffed. Officials said the issues may be addressed when city and county governments merge in 2003.

R.G. Dunlop can be reached by e-mail at rdunlop@courier-journal.com

Mark Schaver can be reached by e-mail at mschaver@courier-journal.com

Tech Tips...

continued from page 17

Query

Borstate	No	Yes	Pct
AS	179	41	0.1864
RI	88	16	0.1538
SC	1770	303	0.1462
GA	2007	289	0.1259
PR	5349	732	0.1204
FL	10345	1394	0.1187
CA	36787	4752	0.1144
HI	1666	207	0.1105
MO	1922	221	0.1031
IL	2074	237	0.1026
NH	132	15	0.1020
AZ	340	38	0.1005
LA	2367	251	0.0959
KS	642	61	0.0868
NM	139	13	0.0855
SD	718	67	0.0854
IN	410	38	0.0848

In the first record, AS stands for American Samoa, a U.S. territory with 19 percent of the loans defaulting during the time period. Those California numbers show up at No. 7 in this calculation, with 11 percent.

States, of course, make up a simple example. Reporters can filter and cross-tab by city, zip code, even type of business to compare and calculate, filtering before or after running the cross-tab command. The SBA disaster loan data table contains 731,352 records, far beyond Excel's pivot table capability.

Of course, even a well executed cross-tab doesn't relieve the reporter of reading the fine print about the data. The table lists the state of the borrower, not necessarily the location of the damaged property. The majority of the most recent loans, including those in the days after the Sept. 11 attacks, haven't had time to run into serious trouble.

Jeff Porter can be reached by e-mail at jeff@nicar.org

Uplink Info

A newsletter of the National Institute for Computer-Assisted Reporting

Editor
Brant Houston
brant@ire.org

Managing Editor
Jeff Porter
jeff@nicar.org

Associate Editors
Amy Sherrill
amys@nicar.org

Mike Sherry
mikes@nicar.org

Art Director
Lisa Triefenbach
lisa@ire.org

Editorial Phone
573-884-7711

NICAR is a joint program of Investigative Reporters and Editors, Inc. and the Missouri School of Journalism.

NICAR services include supplying journalists with government databases, training programs, tipsheets and data analysis.

Director of Publications
Len Bruzzese
len@ire.org

Advertising Coordinator
Pia Christensen
pia@ire.org

Subscription Administrator
John Green
jgreen@ire.org

Subscriptions
IRE members $40, nonmembers $60

Uplink Address:
IRE-NICAR, 138 Neff Annex
Missouri School of Journalism
Columbia, MO 65211

Postmaster: Please send address changes to IRE-NICAR.

Investigative Reporters and Editors, Inc.
138 Neff Annex
Missouri School of Journalism
Columbia, MO 65211

NON-PROFIT ORG.
U.S. POSTAGE
PAID
Jefferson City, MO.
Permit NO. 89