

98-26

COMMODITY FUTURES
TRADING COMMISSION
RECEIVED

OFFICE OF THE
SECRETARY

(2)

Jul 2 11 20 AM '98

CFTC
COMMENT

The Leslie Analytical Organization inc

June 30, 1998

Chairperson Brooksley Born and
Each Commissioner
Commodity Futures Trading Commission
1155 21st Street, NW
Washington, D.C. 20581

COMMODITY FUTURES
TRADING COMMISSION
RECEIVED FOR
PUBLIC RECORD
Jul 2 1 31 PM '98

Dear Chairperson Born and Commissioners:

For the continuation of today's orderly and responsible U.S. and world financial systems, one of the major pillars is confidence in the market for trading U.S. Treasury issues. Having served as a broker-analyst since 1949, when I graduated from Merrill Lynch's eighth trading class, I am deeply troubled by the news that you may be about to permit a privately owned company by the name of Cantor Fitzgerald to establish an in-house electronic market exchange for U.S. Treasuries.

Concerns among some of us market analysts are based on the following:

1. Won't such a development require the New York Cotton Exchange and the CFTC to establish new large supervisory groups to oversee the financial integrity of such a private market and its employees and its owners and its board members and its clearing operations? The record of recent years demonstrates that both a large Japanese bank and a giant British bank were unable to maintain reliable supervision over their employees' activities in copper and currencies. This error created costs of several billion dollars.

2. When electricity and satellite transmissions are disrupted by power failures or terrorists or atomic plant breakdowns or by bank and currency and government collapses, what financial resources and legal depth will there be in this new organization and its members to cover the trading disruptions and costs of out-trades and errors?
3. Hackers are attracted to money and the challenge of stealing funds from established electronic accounts. The new financial and legal troubles resulting from this activity, it seems to me, will have to be adjudicated by you members of the CFTC.
4. Are we all becoming too much obsessed by the philosophy of competition... as well as by the developments of the electronic marketplaces in Europe? I submit, their markets have yet to be subjected to the experiences of time and crises trading volume jam-ups. Should America move cautiously until the more novice exchanges demonstrate the ability to survive abnormal international and unpredictable financial stresses?
5. Margaret Thatcher, the former prime minister of Britain, states that when the Euro is adopted as a common currency in six months, the currency system of Europe will collapse within three years. If she is correct, will the fledgling electronic markets of Europe and their sponsors be able to financially survive such an enormous worldwide trade crisis? How well will they serve during a major Japanese or Russian or Chinese financial crisis?

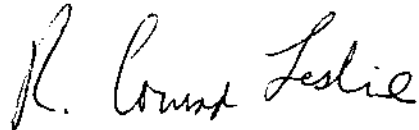
6. Foreign governments, such as Iraq or Iran or Russia or China, can develop their own interests in manipulating and creating turmoil in American bond and currency markets. The world's international and domestic banks and insurance companies and other investors in U.S. Treasuries benefit from an open outcry market by the transparency presented when brokers are buying or selling...and their volume. Also, the announced "price discovery" and the avoidance of "order matching." Such integrity insurance will not be as clear to the public world via private electronic markets. (Only Cantor's money interests will be "in the know.")
7. Enclosed are a number of news items and alerts from some financial market analysts which warn us that in contrast to the futures industry, some of America's banking and insurance computers are not yet formulated to move into the Year 2000...and will not be ready because they are operating with difficult-to-update old main-frame IBMs. A GAO report is noted regarding the lack of some government preparedness by the Social Security and IRS and Medicare divisions. A spokesman for Vanguard, America's second-largest mutual fund observes, "If somebody hasn't started yet (to adjust), it is very doubtful they will be able to finish on time." The Russian government has just issued a press release which says it may not be prepared to fully resolve the problems of conversion by the Year 2000. Earlier this month, Representative Steven Horn, California, announced his latest report card for Federal agencies struggling to correct the dreaded Year-2000 problem...is an F.

Chairperson Born/Commissioners
Page 4
June 30, 1998

Your attention is directed to the observations presented in the enclosed overview of the developing "world crisis" as seen by Gary North, Ph.D.

Is there wisdom in delaying your decision regarding the creation of an untested, electronically traded market system for U.S. Treasuries for two years until the middle of the Year 2000?

Respectfully submitted for your consideration,

A handwritten signature in cursive script that reads "R. Conrad Leslie". The signature is written in dark ink and is positioned below the typed name.

R. Conrad Leslie

Enclosed are some pertinent copies of late newswire stories and analyses relating to the above subjects.

Y2K no cause for panic *Chicago Tribune* 1/26/98

Financial planners are concerned about Millennium Bug, but caution against making rash investing decisions

I'm not dumping all my stocks and mutual funds, pulling money out of the bank or hoarding gold. And I don't believe all electric power will go out, planes will fall out of the sky and our computer-dependent world will come crashing down at 12:00:01 a.m. on Saturday, Jan. 1, 2000.

But neither do I dismiss the warnings of those who fear that the Millennium Bug—computers reading the date 01/01/00 as Jan. 1, 1900 instead of 2000 and going haywire—will create massive disruptions, cause businesses to fail and throw the world into a major recession.

The tough job is separating the facts—and the valid concerns raised by many people familiar with the problem—from the self-serving hype of those who stand to profit from mass panic over this "Year 2000" or "Y2K" problem.

"One of the things that detracts from the possible seriousness of this is the bunch of newsletter promoters running around talking about Armageddon," said Henry Montgomery, a certified financial planner in Minneapolis.

Montgomery's views typify those of most financial planners interviewed for an article about the Y2K problem in the most recent issue of the *Journal of Financial Planning*, a magazine for financial professionals put out by the Institute of Certified Financial Planners in Denver.

One of the planners' concerns is that scare headlines and predictions of a financial meltdown will prompt nervous investors to make rash—and improper—decisions.

"It's definitely a concern, but we're not in a position to start screaming fire," said David Lull, a certified financial planner in Denver.

Let me make it clear I am no expert on computers or the Y2K problem. I've been reading so much and talking to so many people about it, though, that I feel I have taken—no pun intended—a crash course. And it has been enough to tell me Y2K is not a problem we can dismiss lightly.

"We are very, very worried about the Year 2000 problem," said Mary Schapiro, president of NASD Regulation, the self-regulatory arm of the National Association of Securities Dealers, which oversees the nation's brokers.

While the major brokerage firms "are in pretty good shape" with their preparations, many smaller firms are not and will need to step up their efforts, Schapiro said.

Time is against them. The experience of many who've dealt with the issue is that the Year 2000 problem cannot be fixed quickly.

Take Vanguard, the nation's second largest mutual fund group. The company, which is already running new "2000-compliant" computer code, began working on the Y2K problem with a handful of workers in late 1996 and now

has more than 100 employees and outside consultants assigned to the project.

"We knew it would take time and that's why we started as early as we did," said Brian Mattes, a spokesman for the Vanguard mutual funds. "And we are very glad we did. If somebody hasn't started yet, it is very doubtful they will be able to finish in time."

That's one of the biggest challenges of the Y2K problem—the deadline cannot be pushed back.

And we've already seen a sneak preview of the some of the possible havoc—credit cards that expire in 2000 have been rejected by many store computer systems, and some systems have crashed trying to process multivear contracts that extend beyond December 1999.

Now imagine, beginning in 2000, that computers refuse to spit out checks, including tax refunds. That electronic deposits, including Social Security and dividend payments, are never made. And buy and sell orders for stocks, bonds and mutual funds are not executed.

Now add this problem: Companies spend so much money trying to fix their computers that even if they succeed—and just as importantly, the companies with which they do business also succeed—the cost will eat up their profits.

Or, in the worst of cases, drive them out of business.

Most of the planners interviewed for the *Journal* article are more optimistic than that. They do not anticipate widespread computer failures that would cause a major collapse in the American economy. Disruptions here and there, yes. But not the dire forecasts of some observers, including Deutsche Morgan Grenfell's chief economist, Edward E. Yardeni, who has predicted a 60 percent chance of a 1973-74 type recession worldwide.

That doesn't mean the planners are not worried, particularly about the ability of businesses and governments in Asia and Europe to be "2000 compliant" by the year 2000.

That, too, is a concern of many money managers.

"The biggest danger that I see is foreign companies and foreign banks that are technologically behind the United States, will fail to solve the problem and accidentally trigger trouble for us," said L. Roy Papp, manager of the Papp mutual funds. As the economic troubles in Asia have shown, disruptions overseas can have a very adverse impact on the U.S. economy.

So what to do? Nothing drastic for now, but keep informed. Much more will be known in the next few months as many computer users and businesses test their readiness and keep studying the issue.

The Day the World Shuts Down:

A Special Report on the Year 2000 Computer Crisis and What It Means for You.

A Report from Bruce Tippery, Publisher

Newsweek calls it "the day the world shuts down," and "the event that could all but paralyze the planet."

What in the world are they talking about? They're talking about what is popularly being referred to as "the Year 2000 computer bug," or "the Y2K problem" for short. You've probably heard at least a little bit about it through the conventional media. But if you are not *thoroughly familiar* with the Y2K problem, you need to get familiar with it — **FAST!**

I want to give you a brief overview of the critical nature of this looming global disaster, and the dramatic — and potentially dangerous — changes it's going to make in your life over the next 12 months and beyond... My hope is that the Y2K crisis will mark the beginning of the end of centralized, authoritarian government around the world. My fear is that we face truly difficult times.

In a nutshell, the Y2K problem is **the trigger that is about to cause a massive, date-sensitive worldwide computer crash** — a crash of such gargantuan proportions that it will literally bring down governments. It may even bring down ours. (I'm not exaggerating. Stick with me here. Please. You're in for quite an eye-opener.)

Why This Tragedy Is About to Unfold...

This tragedy is about to occur for one simple reason: lack of foresight. You see, back in the 1960s, the programmers who wrote the original — but now antiquated — code for mainframe computers tried to do their bosses a favor. They tried to save them some valuable computer memory by leaving off two little digits from dates programmed into the tens of millions of lines of code required to run each computer.

For example, the year 1965 was shortened to "65," the year 1977 was shortened to "77," and so forth. A harmless shortcut, it would seem. Until you reach the year 2000, which the world's mainframe computers have been programmed to read as "00" — at which point, they will automatically revert back to the year 1900!

You see, programmers in the 1960's never thought that business, government and finance would still be dependent upon the same giant mainframe computers in the year 2000 that they were using back then. They assumed everything would change in a decade or so. So they didn't worry about the date shortcuts they had imbedded into the millions of lines of code each computer runs on. Unfortunately, their assumption was dead wrong. We are still using the same old mainframes. Only now, our society, and the entire western

industrialized world, is so dependent upon those very mainframes that without them, nothing can run the way it was originally programmed — no government agency ...no banking or financial institution ...no major businesses ...no significant electric power or utility company ...no telephone or communications company ...no commercial airline company ...no commercial broadcasting company ...not even the U.S. military can be run without those mainframes!

That's right. These are the very same mainframe computers that now control the vast majority of America's financial, political, business and even military infrastructure, as well as that of every major industrialized nation, including Japan, the Asian powerhouses, western Europe, and most of Russia. So what's going to happen? Let me explain: When the year 2000 rolls around, many (if not all) of these behemoth computers will revert back to the year 1900 — and wreak havoc on every date-sensitive transaction they are programmed to make. Other mainframes will just freeze up, causing a total disruption in the flow of critical financial and business data from around the world. And still others will begin to spew out corrupt data that will wreck the internal calculations of every computer they trade information with, not just nationwide, but globally!

How serious is the situation? It is critically serious. Right now, I'm going to give you a brief synopsis of how Y2K is likely to affect you personally. After that, I'm going to reveal three dirty little secrets about Y2K which your federal and state governments don't want you to know yet — suppressed information that spells doom for much of the world's financial, business and political infrastructure *long before the year 2000 arrives*. First, let me give you an idea of how you will most likely be affected by the Y2K problem:

- Your local bank is controlled by a powerful mainframe computer. *In all likelihood, that computer is about to crash!*
- Your local city water supply system is controlled by a powerful mainframe computer. *That computer, too, is about to go down!*
- Your local and regional electric power grid is controlled by a powerful mainframe computer. *These computers, because of software design and computer chips designed to fail, are on schedule to malfunction!*
- Your local natural gas supply is controlled by a powerful mainframe computer. *You guessed it, that computer is about to crash!*
- Your favorite commercial airline is controlled by a high-

tech guidance system which is in turn controlled by a powerful mainframe computer. *That computer won't make it either!*

- Your brokerage firm is controlled by a powerful mainframe computer, which keeps track of all of your stock, mutual fund and other investment accounts. *You can kiss that computer goodbye (and quite possibly the information it contains — your investment records!*
- Your local hospital's intensive care unit, neonatal unit, X-ray equipment, CT scanners, patient-record databases, blood bank dating systems, and prescription dispensing systems are all controlled by programmed computer chips, millions of which are programmed incorrectly. *In all likelihood, those computers won't work after 1999!*
- Your local police department's emergency 911 system is controlled by a powerful mainframe computer. *In all likelihood, that computer is about to crash!*
- Your local telephone company is controlled by a powerful mainframe computer. *Will it work after 1999? Unlikely!*
- Every major retail store in your town (your local Wal-Mart, your local J.C. Penney, your local Sears, your local Home Depot, your grocery store, etc.) stocks goods that are brought in by railroad. Today, old-fashioned manual switching yards no longer exist. Instead, the nation's railways are controlled by mainframe computers. *These systems, too, are programmed not to work after 1999!*

Are you beginning to get the picture? I hope so. Because what you are facing is a world suddenly devoid of the modern necessities and conveniences that you, and everyone you know, have grown dependent upon. Things like a ready food supply. 24-hour-a-day telephone service. Safe and reliable banks and investment services. Clean water pumped to your house. Electric power to your home and office. A high-tech health care system. Rapid-response police, fire and emergency services. All of this, and much more, are about to be severely disrupted — maybe for months, maybe even for years.

It just can't happen, you say? Well, that was my knee-jerk reaction too. Until I started reading the data for myself. Here are just a few of the startling facts that are being kept hidden from you:

When the Hawaiian Electric utility system in Honolulu recently ran a series of special tests on the computers that control the city power grid to see what would happen on January 1, 2000, *the power system simply stopped working!* Listen, most other U.S. cities haven't even started *thinking* about the power problems they face in relation to Y2K, much less testing their power grids under a Y2K scenario. And because a "fix" for an average mainframe computer takes not months, but *years* to complete, many experts agree that it is already too late to solve the problem in time.

(For example, the Social Security Department has had computer programmers working for five straight years on their Y2K problems. So far, they have fixed only six million lines of the 30 million lines of code their computers run on. With just over a year left before the year 2000 rolls around,

*how are they going to get the other 24 million lines of code fixed in time? Ask them yourself. They won't answer you. They can't. Without a miracle, the task is impossible. Furthermore, Social Security faces an *additional* 30 million lines of code in state administered computer systems outside of their direct control which must also be fixed for the entire system to work!)*

Here's another frightening little tidbit you need to know about: The Nuclear Regulatory Commission is also getting nervous about Y2K. *Very nervous.* In a recent internal memo, they warned that Y2K-related computer glitches could affect "security control," and "radiation monitoring" as well as the agency's ability to calculate the public health hazard posed by radioactive fuel releases. When the computers that run the nation's nuclear power plants cannot reliably monitor the regulatory compliance of those plants (remember, we're talking about *nuclear* energy here, every aspect of which is heavily controlled by the federal bureaucracy), they will be closed. Nuclear power plants supply 20% of America's power — in some regions, 40%. (Even more frightening is the fact that our electricity is provided by a power Grid — an interconnected, interdependent system for electricity transfer. A falling tree in Idaho recently caused outages in California. Now we face the likely probability of wide-spread, chain-reaction power-grid shut-downs because of systems failure!) I don't know about you, but I don't see very well in the dark!

And What About the Banks?

As Newsweek reports, "*Banks and other financial institutions generally will go bonkers if they don't fix the year 2000 problem.*" In their worst case scenario, the magazine states, "*The entire financial infrastructure, including the stock market, will go haywire. Balances, records and transactions will be lost.*"

Please listen carefully: Even the Senate Banking Committee is quietly but *urgently* warning the nation's banks to prepare for the distinct possibility that errant computers might erase the last 99 years' worth of bank records!

It is all too likely that we're talking about a *complete meltdown* of this nation's banking and financial system. And according to the experts, the rest of the world is in the same boat. In fact, virtually every major industrialized country is *far behind* the U.S. in attempting to deal with the Y2K problem.

Once again, please listen to me carefully: Today, not one bank in the *entire western civilized world* has officially stated that it — and its interconnected web of operations — is Y2K compliant. If one was, that bank's entire board of directors would be gleefully shouting that information from the rooftops. But I don't hear any shouts, do you? If you see bankers on the rooftops, trust me, it's because they're getting ready to *jump*.

Even the Federal Reserve System, our nation's central bank, is not Y2K compliant. How far along are they? Once again, please listen to me carefully: They have not even started working on the problem. They are "assessing" the problem. (Again, consider Social Security: they began

working on their Y2K compliance problem nearly six years ago. The last tangible report I have as of June, 1996, says they were not even one-third of the way done (Sept. 15, CIO Magazine). The likelihood of them finishing the needed repairs in time is about as high as the likelihood of Ronald Reagan running for President again. They will not be ready in time. The Social Security system will go down, less than half repaired. The Federal Reserve System hasn't even *started* repairs. They're busy *assessing*. My best guess: they will go down *completely unrepaired*. There is simply not enough time left to complete repairs, and they know it.)

As Senator Daniel Moynihan (D-NY) recently asked in a private letter to President Clinton, "...what happens to the economy if the problem is not resolved ...Are corporations and consumers not likely to withhold spending decisions and possibly even withdraw funds from banks if they fear the economy is facing chaos?"

They will withdraw funds from banks all right. They will do it in droves. By the tens of millions.

As economist and Y2K expert Dr. Gary North states, "*Today, we face the mother of all bank runs. Even if some miracle happens and an optimistic 80% of the mainframes this country runs on could be fixed in time — and believe me, it would take a miracle — the remaining 20% of non-compliant computers would still send corrupted data into the compliant mainframes and wreck all of their data. The problem is self-perpetuating. The simple truth is this: If you can't fix all of the computers, there's no use in fixing any of them because of the data corruption problem. And at this point in time, they simply cannot fix all of these computers. The banking system is doomed. And you had better get prepared for it — now — while there is still time!*"

3 Deadly Secrets You're NOT Being Told...

Most experts — including those quoted by Newsweek — argue that Y2K-related computer problems won't start until January 1, 2000. Of course, that's when the computers will innocently roll over from the year 1999, and start reading the new year as 1900 instead of 2000.

But there's something you need to know about *right now...* something you're *not being told*. It is this: you're not going to have to wait until the year 2000 for these devastating disruptions to begin. That's because they are all ready starting, as you will see in just a moment. In fact, there are three deadly Y2K secrets that are being held back from the public by the government and the conventional media. Without this knowledge, you and several billion other unsuspecting individuals are going to end up trapped in the midst of a snowballing crisis that could destroy literally everything you've ever worked for *long before the year 2000 ever gets here*. Here's what I'm talking about...

Secret #1:

The "Fiscal Year" Secret...

Many state governments work in terms of fiscal years. And somewhere around the summer of 1999, when their computers begin calculating data for the fiscal year 2000 (this

starts on July 1, for example, for the state of New York), pandemonium is going to break loose when computers start reading the date as "fiscal year 1900" instead of "fiscal year 2000."

So what's going to happen? Well, let's look at the issue of date-sensitive state government contracts as just one prime example. When state government mainframes begin to misread the dates on independent vendor contracts, thinking them to be over 100 years old, they will simply consider the contracts expired, invalid or obsolete, and will *automatically cancel them!* Since many mainframes are programmed to automatically delete out-of-date files, these contracts will simply no longer exist. I'm talking about the sudden disappearance of all data on literally tens of thousands of state government contracts, nationwide! Vendors will not get paid. Services will grind to a halt.

Please take about 30 seconds for a crucial mental exercise. Imagine for yourself the utter chaos that will break loose in the business and financial markets, as tens of thousands of state government contracts around the country are unceremoniously, and erroneously, canceled and deleted. Will this be the wake-up call that will send the private sector markets crashing? Then, take another 30 seconds to think about the effect of this snafu on the state you live in. Law enforcement, fire fighting, transportation. We take most state and local government services for granted. **And remember, this initial failure is going to happen in the summer of 1999, well before the year 2000 ever gets underway!** (IMPORTANT: These "Fiscal Year" failures may be your final warning tip-off indicator for the coming Y2K crash — or it may be too late to take steps for your personal protection. My advice? Take steps now, before these preliminary breakdowns take effect!)

Secret #2:

The "Code 99" Computer Shutdown Secret...

Another big secret the government does not want you to find out about is the unsolved problem concerning computers that are programmed to interpret the digits "99" as meaning "cease all computer functions." You see, back in the 1960's, programmers needed a simple way to shut computers down for maintenance or repairs. Not thinking very far into the future, they used "99" as the code for that command — the same two digits that would someday represent the year 1999! Talk about lack of foresight! **This means that, without warning, many of the world's mainframe computers are simply going to shut themselves off on January 1, 1999 (when the computers roll over from 1998), a full year before people are expecting any problems.**

Which computers? It doesn't much matter (there is such massive data exchange, all it takes is one computer to corrupt the entire financial information system). What really matters is what will happen to the world's financial markets, the world's political systems, and the world's business infrastructure when this sudden disruption in the flow of key financial and business data strikes. How will you get money from your bank, if its computers have shut down? Will your

local ATM work? What happens to your local water supply when the mainframe computer that regulates it suddenly shuts down for no apparent reason? How will you and 40,000 other customers buy groceries when the computer that controls the automated price scanners, the cash register and the store's inventory system quits functioning?

And think about this: State government computers will be making their fiscal year 1999 calculations during **summer 1998**. What's going to happen at that time when a government computer reads the "99" as an order to shut down operations? As you can see, the "year 2000" problem is really a "year 1998" problem. You may have less than 6 months to prepare. Clearly, this high-tech thunderstorm is moving in *FAST*. In fact, faster than you can imagine.

Secret #3:

The "Forward Calculations" Secret...

The third big secret I promised to tell you about is what I call the "forward calculations" secret. This is the secret that has already set the Y2K problem in motion, years ahead of schedule. You see, the truth is, computers throughout the U.S. and around the world are *already* beginning to show the initial signs of systems-wide failure. **But what's happening is being quietly swept under the rug, out of fear of mass public panic.**

Here's what you need to know about this situation: Most mainframe computers are programmed to make calculations years into the future. Consider, for example, the computers that control the data for this country's major insurance companies. They must calculate mortality rates, insurance costs and contractual liabilities years ahead of time. It's an integral part of that business. But what happens today when an insurance company's computer begins to calculate rates and costs into the year 2000 and beyond? You guessed it. Much like the "fiscal year" problem, the computer reads the "00" as 1900 instead of 2000. Suddenly, the computer interprets your policy as being over 100 years old ...your account is interpreted as being obsolete ...and *zap* ...*your insurance policy is automatically canceled and deleted!*

(Another important warning: As with the world's banks, not a single major insurance company on the planet has yet announced that it is Y2K compliant. Not one. They are not even talking about the problem publicly. Why? Well, if you knew that the insurance company you've been paying premiums to for the past few decades had less than 36 months ...maybe even only 12 months ...before all of its data crashed, would you keep paying your monthly premiums? Wouldn't you cash in your policy? And if you were one of those major insurance companies, would you be a "good guy" and tell your hundreds of thousands of customers worldwide about the serious nature of this problem, *knowing in advance how they would react?* I think you know the answers to those questions.)

Stories about the "forward calculations" problem have recently surfaced in a number of small city newspapers here in the U.S., and around the world. But the stories have been "de-emphasized" by the major media in order to help forestall the

inevitable public panic. For example...

- Already, computers in Britain that keep track of food inventories for large food chains have begun incorrectly calculating the age of tons of fresh beef held in storage. In one recent case, the computers in charge of tracking beef inventories thought the beef was over 100 years old, and triggered an order for the destruction of the entire inventory!
- Here in the U.S. an errant state prison computer, confused by quirky dates, miscalculated the parole date of prisoners, and freed them prematurely!
- In numerous parts of the country, people with new credit cards who were issued expiration dates of 2000 and beyond found their accounts canceled or their cards locked out when they made a charge — sure enough, the computers are reading the "00" in the expiration date as "1900"!
- Elderly people born before the year 1900 are already having their insurance policies canceled. In one recent case, a woman born in 1897 had her health insurance canceled because the insurance company computer could only read her birth date as 1997 — in essence, the computer thought she hadn't even been born yet!
- In Kansas, a 104 year old woman was recently sent a computer generated notice from the education board, notifying her to enter kindergarten!

The Problem Worsens...

And the problem is much worse than it appears on the surface. Why? Because even now these wayward computers are regularly *exchanging data* about you with hundreds of other computers that also contain important data about you. (For example, the computer at your credit card company exchanges data about you with the computer at your bank. And the computer at your bank exchanges data about you with the computer at your brokerage house. And the computer at your brokerage house exchanges data about you with ...well, you get the picture, right?) And when they exchange data, *any bad data about you in the errant computers will corrupt the good data about you in the computers they just "spoke" to.* Like the 104 year old woman mentioned above, one day you could be receiving your latest Social Security check, the next day receiving your notice to enter kindergarten. Scariest still, all your savings — everything you've worked so hard for over the years — could be mixed up, scrambled, lost because of bad information entering your bank's so-called "compliant" computer system. A bank error is hard enough to straighten out in the best of times. When virtually every bank customer is lined up at the door and federal bank regulators you have never met are put in charge, how likely is it that you will be able to withdraw your savings — let alone enough cash for this week's groceries? Now, multiply the corrupt data problem by every financial institution you deal with, every public utility that provides you with service, and every insurance company whose policy you hold — all within virtually the same exact period of time!

And the truly scary part is, there is no reliable way to stop this from happening. No quick fixes. No special software to alleviate the problem. And nowhere near enough experienced

programmers to find the tens of thousands of date-sensitive lines of code, hidden among the literally millions of lines of code that run each one of the world's mainframe computers.

Even Newsweek says, "*Forget about a silver bullet. It seems that in most mainframe programs, dates appear more often than "M*A*S*H" reruns on television — about once every 50 lines of code, with many computers containing millions, if not TENS of millions of lines. Typically, it's hard to find those particular lines, because the original programs, often written in the ancient COBOL computer language, are quirky and undocumented.*"

(As a brief aside, what about our country's computer-dependent, high-tech military infrastructure? Surely the Department of Defense will come up with a solution to this problem in time. Well, not if you believe what Assistant Secretary of Defense Emmett Paige, Jr., recently said, when he testified before Congressman Steve Horn's subcommittee on Government Management, Information and Technology. He warned matter-of-factly: "*We face a firm deadline and there is no 'silver bullet' product in the marketplace to find, fix, and test all of the changes required.*" Could this be why both Newt Gingrich and Al Gore recently went to Red China, bowing and scraping like penitent altar boys before the butchers of Tiananmin Square? Could this be why Congress is again timidly voting to grant Red China "most favored nation" trading status? Don't forget, Red China has the largest standing army in the world, and a navy replete with highly effective WWII-era battleships that are not — I repeat, *not* — computer-dependent like ours. Today, our high-tech Navy can hold the Chinese navy in check. But in another 36 months ...24 months ...12 months???)

Acceleration of Public Awareness

There's yet another important reason we may not have until the year 2000 to prepare for the massive disruptions in government services, banking, the investment markets, business, public utilities and much more. It has to do with the acceleration of public awareness of the Y2K problem.

Until very recently, the public has been kept completely in the dark on Y2K. The U.S. government has done everything in its power to forestall the inevitable public panic. But slowly, the word is leaking out. And within a matter of months, it is going to be forced out. You see, at least several federal agencies have finally realized they have a fiduciary responsibility to warn the public of the danger — particularly as it relates to businesses and financial markets regulated by the government.

For example, Arthur Levitt, Chairman of the U.S. Securities and Exchange Commission, recently sent an urgent letter to registered investment advisors, informing them that they are obligated under U.S. securities laws to begin "*discussing Year 2000 issues*" with all of their clients, particularly if they are "*not confident that they will be able to perform smoothly.*" Apparently, the SEC has decided to divert the blame to the "private sector." After all, they are the ones who's only reason to exist is to protect investors. So what's going to happen when brokers and other investment advisors

begin complying (probably in mid 1998) with the SEC's recent mandate? How many investors will suddenly begin to grasp the magnitude of the problem, and react by pulling their money out of stocks, mutual funds, bonds and money markets? And what effect will this have on *your* investments? You can bet that as the public catches on to the full implications of the Y2K crisis, the result will be sheer panic.

Furthermore, as if to compound the "acceleration of public awareness" problem, legislation is about to be introduced in early 1998 by Senator Bob Bennet (R-UT) that will force publicly held companies to tell their shareholders how far behind they are in Y2K compliance, and what this could mean to shareholder investments. As shareholders discover the true extent of this looming danger to their investment nest eggs, do you really believe they will leave their life savings in harm's way? Highly unlikely. They will do exactly what *you* would do — they will begin pulling their money from the markets. Pandemonium will reign. And that pandemonium will trigger what Gary North calls "the mother of all bank runs."

What's more, as the government begins to further mandate public awareness of the looming Y2K crisis, the conventional news media will finally begin to sink its teeth into the story. Already, in-depth stories outlining the severity of the problem have appeared in Newsweek, The Wall Street Journal, The Financial Times of London, and England's prestigious The Economist. But these are not the news sources the vast majority of average Americans depend upon. *It is when this story finally becomes a staple on the ABC, CBS, NBC and CNN nightly news broadcasts — and believe me, it will, and soon — that the inevitable public panic will strike full force. The sudden acceleration of public awareness will see to it.*

The big question is this: Will you be prepared in *advance* of the panic? Do you even know where to start? (I give a few basic guidelines at the end of this letter. Be absolutely sure to read them. Also, be sure to read the accompanying letter that tells you how to get a copy of the extensive **Y2K Preparation, Protection and Survival Kit** that I've prepared. It will help you better understand how to fully protect yourself and your family so you're not caught in the mass public panic that is sure to ensue as the general public catches on to the seriousness of the Year 2000 situation.

Consider just a few of the things the general public is about to learn as their awareness of this brewing maelstrom accelerates:

- The Center for Disease Control has been unable to confirm whether or not the anti-contamination systems for lethal viruses, bacteria and other deadly disease-carrying organisms they have in storage will be operational in the event of Y2K-related power grid problems. These pathogens include some of the most ghastly and terrifying biological agents known to man. Will the CDC be able to keep them under control? So far, they can't say for sure one way or the other!
- New York's State Comptroller now admits that not one of the 81 state agencies he oversees have even completed their Y2K compliance studies, much less begun repair work on their systems. He says the state does not have sufficient funds to

complete the task by February 1999, when their systems must be loaded for the next fiscal year. Barring a miracle, New York computers will begin crashing a full 10 months before the Year 2000 rolls around!

- New York is not alone in its heel dragging. A November 1997 survey conducted by the State and Federal Summit Meeting on the Year 2000 Problem revealed that less than 11% of state and federal agencies have even finished the "planning" stages of their Y2K compliance drives. Only 28% had started the "problem definition" phase of the work, and only 27% had started the "information gathering" phase. (Remember, it has taken the Social Security Administration nearly six years to complete only one-third of their needed repairs. The vast majority of federal and state government agencies have not even made it to the *planning* stages, much less started repairs!)
- Washington state's Department of Financial Institutions recently sent an urgent memo to the Boards of Directors and Chief Executive Officers of all state banks, warning them to expect a significant rise in Y2K-related bankruptcies among their business customers that could threaten *"the safety and soundness of banks in this state."* It read, in part, *"Many experts believe there will be a rise in bankruptcies among businesses failing to complete timely Y2K renovations... Most businesses will feel the effects in their cash flows, which may impair their ability, to manage and service debt."* The department also firmly warned the bankers, *"We want to convey to you the seriousness of the problem... Y2K poses challenges of unprecedented urgency and complexity... [It] represents a challenge of major proportions that will not go away."*
- In November 1997, Federal Reserve Board Chairman Alan Greenspan quietly admitted that the nation's banks absolutely must be 100% compliant. He stated that even 99% compliance would not do. Congressman James Leach, Chairman of the House Committee on Banking and Financial Services followed up by stating, *"It takes little imagination to picture the ricochet effects that malfunctioning computer systems could have on important bank operations ...all financial institutions must be ready; federal and state regulatory agencies must be ready; data processing service providers and other bank vendors must be ready; bank customers and borrowers must be ready; and international counterparts must be ready."* Yet to date, not a single bank in the entire U.S., Canada, or Europe has officially stated that it, and its interconnected web of operations, is Y2K compliant. Perhaps this is why Congressman Leach concluded his speech by stating, *"Despite reasonable efforts by institutions to correct Year 2000 issues, it seems inevitable that some unforeseen problems will arise."*
- States are already quietly passing legislation giving themselves full legal immunity from lawsuits due to Year 2000 related problems such as suits over lost welfare benefits. Nevada has passed such legislation, West Virginia is on the verge of passing it, and other states are sure to follow suit as the enormity of the problem dawns on them.
- The Social Security Administration now admits it has absolutely no contingency plans for a Y2K failure. Furthermore, as this report was going to press, the Social Security Administration had just admitted that an additional 33 million lines of computer code — in 50 different state administered Social Security programs — have been discovered. Since it has already taken the agency nearly six years to complete repairs on just a *portion* of the original 34 million lines of code found in their computers, it seems all but inevitable that the Social Security system will collapse.
- Programmers qualified enough to make Y2K repairs are scarce. First Chicago National Bank now admits it is having so much trouble finding even remotely qualified programmers, they have been forced to hire programmers from the former Communist Bloc countries. Pen Hollist, senior vice president of First Chicago admits he doesn't plan on going to bed the evening before January 1, 2000. *"We will set up a command center at the bank, and we have a crisis plan just in case,"* he recently told a group of fellow bankers.
- Virtually none of the major telephone companies around the world are Y2K compliant at this late date in the game, including those in the U.S., U.K., Australia, Canada, New Zealand, Sweden, Ireland, South Africa, and Norway. Some U.S. phone companies have yet to even inventory the computers that run their telephone exchanges, and have no way of knowing if they will be compliant or not by January 1, 2000. The Financial Times of London recently warned that *"Some nations may be shut out of the international phone system in 2000 and beyond"* because of Y2K glitches in the embedded microprocessors built into all telephone exchanges.
- CitiCorp recently publicly criticized that the vast majority of its telephone and other telecommunications service suppliers have *"no common millenium compliance definition, no consistent way of achieving compliance, have started too late to achieve compliance, have provided nebulous, misleading and incorrect information in regards to compliance, and have been unaware of the totality and extent of the vital changes that need to be made."* Analysts warn that if Citicorp's telecommunications systems go down, Citicorp goes down!
- U.S. Comptroller of the Currency Eugene Ludwig recently warned that the Y2K problem is *"more serious than we had imagined,"* and further stated banks and financial firms who have not yet developed a compliancy plan *"may find that help is unavailable at any price."* Ludwig concluded by saying that *"even among larger banks, where the problem seems to be well understood, the steps being taken to meet it were often found to be inadequate."*
- Reuters news service recently reported that *"If only 5% to 10% of the world's bank payment systems do not work on January 1, 2000, it will create a global liquidity lock-up."* Translation: the entire world banking system will collapse if even a tiny fraction of the banking payment systems fail.
- Canada's Auditor General recently told the Canadian Parliament *"We are concerned that if progress continues at the rate we have observed, it will likely be too slow to overcome the Year 2000 threat. Systems that support major government programs and essential services may fail, and continuous delivery of these programs and services could be at risk."* Bob Moman, general manager of IBM Canada, confirmed the problem stating, *"The government must channel all of its resources into the Year 2000 project, or all systems will fail."*
- The Chief Information Officer for the IRS stated in October

that the tax agency is working feverishly to correct its 120 mission-critical systems, but sheepishly admitted that he doubts the IRS will find all of the lines of code needed to be fixed in time.

■ Joel Williamson, spokesman for the U.S. Government Accounting Office recently testified before the Government Reform and Oversight Committee that, "It is becoming increasingly clear that agencies will likely be unable to correct all non-compliant systems before 2000 ...contingency plans MUST be prepared so that core business functions can continue to be performed even if systems have not been made compliant. "Translation: We've got to figure out how to run the government without these failing computers — somebody, please ...help!

■ The Electrical Power Research Industry recently published a guidebook to help power companies cope with Y2K problems. Here's how the report ends, "Unfortunately, not everything is going to work, regardless of how well you do your job. It is a good idea to have a standby staff ready and waiting on January 1, 2000, and to be ready to deploy them as required." Translation: Get ready for chaos.

■ A recent survey of U.S. Public Utility companies revealed that fully one-third of the nation's utilities had not even started to correct their Y2K problems, and another third are severely behind. All utilities depend upon computers for the generation, distribution and transmission of their respective capabilities, such as electricity, water and natural gas. According to former State Representative Porter Davis (R-Oklahoma City), authorities now expect 20% of utilities to fail.

■ Reuters News Service has recently quoted oil industry experts as warning that the Y2K problem could shut down North sea oil platforms and paralyze the oil industry, if date-sensitive embedded chips used in the platforms are not checked and replaced. Unfortunately, many of these microprocessor chips are deep below sea level. According to Reuters, the problem is exasperating oil industry experts because "A single offshore oil platform may contain over 10,000 of these date sensitive chips" and there's little chance all of them can be found. David Trim of Shell Oil's Year 2000 Team warns that a worldwide "commercial meltdown" is a real risk. "We're talking about something akin to the aftermath of a war," he told Reuters.

What's going to happen when the conventional news media begins reporting these facts to the American public? As one observer states, "It will take only 72 hours for frightened consumers to strip supermarket shelves bare. Bank depositors will rush in droves to withdraw their savings. Jittery investors will pull completely out of the market. Wall Street will be in turmoil, and the panic will spill over to every industrialized country on earth."

What all of this means is that the threshold of public awareness — and its resulting public panic — will most likely be reached sooner than the computer crisis itself — much sooner! With this in mind, a wise person would "panic early, panic small." That is, don't wait to get mauled in the mass public panic that will unfold as consumers catch on to the true extent of the crisis. Act now, while there is still stability and calm in the markets (the stock market and the supermarket). Make sure you have long since prepared by the

time everyone else is asking in panic "What should I do?"

In short, because of the growing acceleration of public awareness of Y2K, you don't have very much time to prepare for what will soon be known as the greatest social, political and financial crisis mankind has faced since the great plagues of the 14th century that wiped out one-third of Europe. Only instead of a deadly bacteria, you, me and several billion other hapless souls worldwide now face a devastating virus — a computer virus that is all too able to lay low western society and transport the major industrialized nations back into the pre-high tech world of the 1940's and 50's. And if the banks (our system of payments) implode, we could be faced with the lower tech world of the 1840s and 1850s.

How long has it been since you've had to cook without a gas or electric stove? How long has it been since you've gone without air conditioning and heating? How long has it been since you've had to store water in drums, or haul it indoors from a well (If you're fortunate enough to *have* a well!)? How long has it been since you've had to travel on foot? How long has it been since you've had to live without a refrigerator or freezer in which to store perishable goods? How long has it been since you've had to grow your own food? These are questions you had better be thinking about, because we face multiple systems failure in the Y2K crisis! The risk to our accustomed way of life is extensive.

Here are some more questions you need to have the answers to right now: When the computers go down, what's going to happen to the company that runs your pension fund ...the agency responsible for your government retirement, your Social Security check, or your government bond investments? How about the bank in charge of your mortgage ...or the institution which holds your mutual funds?

The banking collapse alone will be enough to destroy the economy. Here are a few more questions you need to start asking yourself right now: "How is the company I work for (or run) going to survive when the banking system goes down?" "Who's going to even bother showing up for work, if the banks can't process paychecks or access accounts?" "How am I going to buy food for my family?" "What am I going to use to pay my bills, when my bank has shut its doors?"

What Can You Do to Protect Yourself?

A very important question. Yet, the answers are not simple. First, despite the fact that everyone who has researched the Year 2000 Computer Crisis realizes that it is a significant problem, no one knows exactly how bad it will be. The estimates range from expensive (as in *trillions* of dollars) to a full — and chaotic — break-down of society. Personally, I hope and pray the crisis will be solved relatively easily and without the social turmoil that is all-too possible if government services, our banking system, and our nation's power grid break down.

The fact is, no one knows exactly what will happen. That's why I believe that you should make reasonable preparations for what can happen and not just prepare for what you hope (perhaps too optimistically) will happen.

Forget Gore

Vice President Al Gore likes to pose as the administration's resident expert on technology. But that image doesn't count for much on Capitol Hill.

At a press conference on June 1, Rep. Steven Horn, California Republican, unveiled his latest report card for federal agencies struggling to correct the dreaded year-2000 problem. His verdict: an F.

He laid the blame at the feet of President Clinton, saying he had not used the "bully pulpit" to alert the American people and his Cabinet secretaries to the problem.

"He should give a fireside chat," said Mr. Horn, chairman of the House subcommittee on government management, information and technology. "Franklin Roosevelt would have done it. Dwight Eisenhower would have done it. Harry Truman would have done it. Ronald Reagan would have done it. Now Bill Clinton needs to do it."

But what about Mr. Gore, a reporter asked, who fancies himself something of a "techie." Can't he lead the charge?

Mr. Horn leaned across the podium and fixed the reporters with an icy stare.

"Congress only deals with presidents," he said firmly. "The vice president — under the Constitution his only role is to preside over the Senate."

About that bridge . . .

Steve Forbes, the once and perhaps future presidential candidate, scolded the Clinton administration for not moving faster to fix the year-2000 computer problem.

"At this pace, the bridge to the 21st century may not be open when we get there," Mr. Forbes said.

Computer glitch may snarl Medicare boost

Chicago Sun Times 6/29/98

WASHINGTON POST

WASHINGTON—Medicare may put off giving more money to physicians and hospitals if computer software repairs for the Year 2000 problem aren't made on time.

A government internal memo, dated June 11, indicated that Year 2000 repairs and reprogramming for legislative changes to the Medicare program could not be done at the same time.

The computer problem facing the Medicare program is among the most complex in the federal government. The Health Care Financing Administration, which sets Medicare policies, relies on 60 contractors to operate and

maintain databases and software programs that process 900 million payments a year for nearly 33 million Medicare beneficiaries.

The contractors, mostly health insurance companies, operate seven different systems, with more than 22 million lines of software code, that use dates to make treatment and billing calculations.

The Year 2000 problem stems from the use in many computer systems of a two-digit dating system that assumes that 1 and 9 are the first two digits of the year. Without reprogramming, the computers will recognize "00" not as 2000 but as 1900, which will cause the computers to shut down or malfunction.

The Health Care Financing Administration

fears the contractors will not be able to finish repairing their computers if they also have to reprogram them for the annual Medicare payment increase scheduled for January, 2000.

At a House hearing earlier this month, John J. Callahan, an assistant secretary of health and human services, said the Clinton administration would ensure that doctors and hospitals do not encounter "cash flow problems or what have you" in the event Medicare computers malfunction on Jan. 1, 2000.

The health care finance agency, for example, could advance money to doctors and hospitals in 1999 to cover the opening months of 2000, or pay them at current rates and then make up any shortfall after computers were reprogrammed.

15:54 04 Jun RTRS-Lawmakers concerned over electronic futures trade

By Tom Doggett

WASHINGTON, June 4 (Reuters) - Members of Congress are worried that a proposal to develop the nation's first electronic exchange for trading futures contracts on U.S. Treasury securities may result in a market that could be easily manipulated.

The Commodity Futures Trading Commission is reviewing the proposed electronic market, which would be jointly developed by the New York Cotton Exchange and Cantor Fitzgerald LP.

The electronic exchange's futures contracts would be based on the value of the U.S. Treasury's 30-year bond, 10-year note, five-year note and two-year note, and would compete with similar contracts listed at the Chicago Board of Trade, as well as threaten the "open outcry" method of trading done there.

In separate letters received by the CFTC in the last week, members of Congress have told the agency they are concerned that, in part, Cantor may have too much control over the electronic exchange and the CFTC may not be able to keep close tabs on how the market would operate.

"The unprecedented system proposed...presents a host of serious issues that must be answered satisfactorily before the commission grants approval," four key Democratic senators said in a letter to the CFTC this week.

The letter was signed by Senate Minority Leader Tom Daschle of South Dakota, Tom Harkin of Iowa, Patrick Leahy of Vermont and Tim Johnson of South Dakota. All four are members of the Senate Agriculture Committee, which oversees the CFTC.

The lawmakers said they are worried that Cantor's influence over the electronic exchange would be too strong, as the firm's employees would operate the terminals for executing trades on the exchange and disseminate the pricing data.

Similar concerns were raised by other lawmakers. The chairman and a ranking member of the House Agriculture Committee told the CFTC they are worried that Cantor would control eight of the 13 directors on the exchange's board.

"That concentration of dominant market power in one firm raises possible anti-competitive and conflict-of-interest concerns that could undermine public confidence," said Republican Representatives Bob Smith of Oregon and Thomas Ewing of Illinois.

The two lawmakers suggested the CFTC hold off acting on the proposal until Congress can rewrite the federal trading law to accommodate electronic markets like the one being proposed.

"We presume you would share our concern that the commission not establish any precedents in this area that would complicate the reform process by offering a blueprint for others to follow in connection with futures trading in other commodities," Smith and Ewing said in their joint letter.

Realizing that 100,000 futures industry jobs are at stake in Chicago if the electronic exchange is successful, 20 members of the Illinois congressional delegation sent a joint letter to the CFTC expressing doubts about the proposed market.

"The significant substantive issues that this application raises...are compounded by the possible two-tier market it could create in U.S. Treasury securities futures and related options, at the expense of traditional exchanges where those instruments are already being traded," the delegation said.

NYCE President Joe O'Neill downplayed the concerns raised by the lawmakers, which he said are similar to issues already brought up by the CBOT.

"The concerns raised in those letters have been asked (by the CFTC) and answered (by us)," O'Neill told Reuters.

The CFTC last week resumed its review of the proposed exchange after the NYCE and Cantor provided additional data that agency staff wanted on how the market would operate.

As for who would control the electronic exchange, O'Neill said the NYCE board would handle all the decisions relating to regulation, compliance issues and clearing of trades at the exchange, while Cantor would be responsible for marketing the exchange and designing its contracts.

O'Neill also said he expects the electronic exchange will be running by early summer and he pointed out that CFTC staffers have said the market proposal is among their "top priorities."

((Washington energy desk, 202 898 8320

[B] US CME boss says electronic trading a regulatory nightmare
STORY:12156d

By Roger James, Bridge News

London--Jun 16--CEO of the Chicago Mercantile Exchange Rick Kilcollin warned today a profusion of electronically traded futures markets will prove a regulatory nightmare as markets become more globalized.

Talking at a conference in London, Kilcollin said the trend toward electronic futures trading, as epitomized by the recent decision by the London International Financial Futures and Options Exchange to introduce screen-based trading by mid-1999, carried regulatory hazards that were already causing headaches in the US.

"The whole electronic trading issue will have a very fundamental effect on regulation of the futures markets," he said.

"If the exchange becomes simply a website on the worldwide web, accessed by screens anywhere on the globe, then it is going to become a nightmarish issue for regulators."

He said that in the US such issues were already being raised about documentation for regulators of transactions carried out on foreign terminals.

Listing the numerous recent examples of mergers and strategic alliances among the world's smaller futures exchanges, he said the trend toward globalization was rapidly increasing the problems facing futures-market regulators. End

Bridge News, tel: +44-171-842-4218

Send comments to Internet address: debt@bridge.com

REUTERS

Friday, 26 June 1998 11:57:36

11:52 26 Jun Russia doubts millennium bug can be fixed by 2000

By Philippa Fletcher

MOSCOW, June 26 (Reuters) - Russia, criticised for being slow to react to the millennium computer bug threat, outlined the measures it was taking on Friday but said it doubted the problem could be fully resolved in the time left.

The State Telecommunications Committee, assigned to coordinate a programme to check computers in state bodies to ensure any dates expressed in two-digits do not cause malfunctions when the century ends, said work began last month.

"At the moment, all-round work to resolve the '2000 problem' throughout the state is being carried out in line with a Russian government order from May 30, 1998," it said in a statement.

The committee was responding to questions put by Reuters after U.S. defence officials and analysts expressed concern Russia was being slow to respond to the threat.

Asked if it thought the problem could be resolved on time, the committee said not entirely and cited a software research company saying a final resolution would take half a century.

"The Russian State Telecommunications committee considers that the '2000 problem' cannot be resolved entirely in the remaining time," the committee said in a statement.

"A final decision will come in 50 years time and will require changing date codes in about 60 million software products throughout the world," it added, quoting an agency called Software Productivity Research.

U.S. defence officials have issued several warnings of the nightmare scenarios which could ensue if Russian early-warning computers malfunction because they have not been programmed to work properly into the next millennium.

They said U.S. Defence Secretary, William Cohen had offered Russian Defence Minister Igor Sergeev help to handle the problem and even proposed sharing early-warning information to prevent nuclear weapons being set off by mistake.

The American Chamber of Commerce in Russia weighed in earlier this month, saying any delay in tackling the problem could have catastrophic consequences on business in Russia and pledging to help the government sort it out.

At a news conference on June 17, they expressed regret that officials from the State Telecommunications Committee had not been there to respond to their concerns.

Experts say Russia may face less of a problem than Western nations because it has far fewer computers and because older Soviet computers were designed differently.

The Telecommunications Committee said it would draw up an inventory of all computers owned by federal and regional bodies to see to what extent they were vulnerable to the problem.

A training centre was being established and a testing and certification system worked out, it said.

The cost of the programme had yet to be established but had been estimated at between \$100-\$500 million.

The Committee did not say whether it had enough money to cover those costs, which come amid an economic crisis in Russia and may well rise as the deadline draws closer.

The U.S. Pentagon alone expects to spend \$2.9 billion on the most pressing aspects of the millennium bug problem by mid-1999.

For related news, double click on one of the following codes:

[G] [C] [D] [E] [M] [O] [T] [U] [MTL] [GRO] [SOP] [J] [NEWS] [RU] [US] [EMRG] [EEU] [LOC] [DPR] [TEL] [LEN]

Friday, 26 June 1998 11:52:20

ENDS (01MY2400137)

Wednesday, 20 May 1998 13:21:39

REUTERS:202997561

13:21 20 May RTRS-Satellite mishap shows vulnerability of systems

Business Regarding Electronic Trading and Settlements of positions and margins -
Wednesday, 20 May 1998 13:43:11

By Jonathan Wright

WASHINGTON, May 20 (Reuters) - When a U.S. commercial communications satellite went out of control on Tuesday evening, it could have been the start of a Space Wars scenario dreaded by the U.S. military.

It turned out a computer had malfunctioned, putting the satellite at the wrong angle to the earth and cutting off services to millions of Americans.

No foul play was suspected.

But other possible causes are very much on the minds of U.S. military planners as they try to keep up with the rapid explosion of space systems for civilian and military purposes.

"Hundreds of satellites circle the globe. Nearly half of those 600-plus satellites are American. They represent an investment of more than \$100 billion," said General Howell Estes, commander of U.S. Space Command.

"This investment must be protected -- from natural and man-made threats, accidental and intentional threats," he added, writing in a commentary broadcast on the Internet.

Their commercial value aside, many of the satellites have a military function -- for communications, navigation, reconnaissance and intelligence gathering.

Increasingly the civilian and military functions are interwoven, complicating the task of protecting U.S. military assets and denying the use of similar assets to an enemy.

Take pagers, for example -- one of the services worst affected by the malfunction of the Galaxy 4 satellite, operated by PanAMSat of Greenwich, Connecticut. Between 20 million and 45 million pagers went out of service.

U.S. soldiers in Kuwait now carry similar pagers on which to receive early warning of an attack. The system depends on a commercial network, possibly on a satellite like the Galaxy 4.

"There's always a trade-off when you decide to rely on the commercial. It's cheaper in the short run but it does leave you somewhat more vulnerable," said Lawrence Korb, senior fellow at the Brookings Institute and a former defense official.

"The military probably does have backup for its most vital systems. But it leads to the whole issue of will a potential enemy try to blind us by going after our satellites before the conflict starts. How do you protect them?" he added.

The U.S. military does have two promising space war attack systems, the Kinetic Energy Anti-Satellite System (KE-ASAT) and the MIRACL ground-based laser, but these remain hostage to international and domestic politics, clearly frustrating space scientists and their military customers.

KE-ASAT has been living off funds granted by Congress over the administration's opposition. But President Bill Clinton, wielding his newly acquired power to veto specific projects, has cut the \$38 million from the 1998 budget.

"If there's money available in 1999 we could conduct a proof of principle flight within 18 months. I would need \$65 million to do two flight tests," said Dick Fisher, director of the Missile Defense and Space Technology Center in Alabama.

In the test flight, a rocket would take a "kill vehicle" up into space. The kill vehicle would then capture and drag a satellite down toward the atmosphere, where it would burn up.

The U.S. military fired the MIRACL laser at a satellite last October but has been coy about the outcome, on the grounds that it does not want to discuss how vulnerable its own satellites might be to enemy attack.

"Any threat to our use of space is a threat to our nation's security. As we have protected national and economic security on land, sea and air for more than 200 years, we must be prepared to defend our interests in space," said Estes.

"From computer hackers tampering with satellites, to electronic jamming of satellite signals, to actual anti-satellite weapons -- man-made methods already exist to challenge America in space," the general added.

Jamming has already happened, during a commercial dispute in early 1997 between Indonesian and Tongan companies, disrupting television broadcasts in parts of Asia.

Korb said the United States had little to fear in the short term from potential space aggressors. "We are pretty far ahead and the question is whether the United States can set up a regime where you don't militarize space, where we promise not to shoot down other people's satellites," he said.

In the meantime, the greatest threat of all probably comes from a much more mundane source -- space debris.

The U.S. government calculated last year that, with more than 35 million pieces of man-made debris orbiting the Earth, the planned International Space Station has a one-in-five chance of having a serious collision over 10 years.

"Our satellites need to be designed to survive collisions with the debris we can't see, and maneuver out of the path of debris we can see," General Estes said.

SECURITY

HOW SAFE IS THE NET?

or an electronic marketplace

For most businesses, not safe enough. So they're building their own private networks

The first sign that someone is tampering with GTE Corp.'s global data network is a warning message that appears on a computer monitor nicknamed "Prozac." Every second or two, another one pops up, indicating that an uninvited guest is logging onto the network that GTE operates for National Semiconductor, CVS, Taco Bell, and 300 other corporations and government agencies.

Most of the time, it's GTE engineers making

adjustments to the network—something the two men who watch the screen can tell by glancing at the color-coded messages. But every so often, a speaker in the corner of the cramped room calmly intones, "Red Alert," and the guys straighten up in their chairs. Eyes narrowing, they quickly type commands that might catch an intruder from the "demilitarized zone" outside the network's hardened firewalls.

With so much talk about the billions to be made in E-commerce, you would think the Net already was secure for business. Not exactly. While some transactions, including E-mail and simple home banking, can be protected through basic encryption, the secure environment that businesses need to carry out lots of confidential transactions still doesn't exist.

Indeed, concerns about security run so deep that they are slowing use of the public Internet by corporations. Fear, says Jack Danahy, director of security services at GTE Internetworking, "is having a negative effect on the rate people are adopting the Web" for business-to-business transactions. The reality is that fewer than one in seven companies is willing to link its critical applications to the Net, according to a recent survey by the Open Group, a consortium of global companies pushing for security standards.

Most experts believe the delays are temporary. E-commerce, after all, was developing well before the Internet's recent explosive growth and has been steadily building momentum. Today, while awaiting better Internet security, companies continue to invest in private networks that, in reality, run on the public telecommunications system—just as General Electric, General Motors, and IBM have done since the 1970s.

LICENSE TO HACK. Then there's the ultimate private network—SWIFT, the international bank settlement system based in Brussels. With responsibility for nearly \$3 trillion in electronic money transfers every day among the world's 3,000 largest banks, SWIFT Chief Executive Leonard Schrank says he never considered using the public Internet. Instead, SWIFT is spending hundreds of millions of dollars to link member banks with dedicated fiber. The result looks more like a fortress than the long-heralded Information Superhighway. "Security is the primary driver," says Schrank. "That's different from the Internet, which was built as an academic exercise."

Promoters of the Internet and cyberspace in general view such private networks as perhaps necessary but backward. For one thing, they are expensive. And because they don't take advantage of the most celebrated attribute: ubiquity. Businesses are willing to forego ubiquity to maintain security. "Without a common set of specifications and products that guarantee security and reliability, the Internet may simply become an interesting public-access network," says



NET FACT

More than 80% of companies say security is the leading barrier to expanding electronic links with customers and partners

Info

It's ti

Smc

retri-

Anc

Pl

No

or f

For

visit

or f

n

Filr

Michael Sullivan-Trainor, an analyst at International Data Corp. in Framingham, Mass.

How hack-prone is the Internet? Even cocky security consultants admit that in time, determined hackers can surmount any barrier. Private networks have higher walls, but they are not impregnable. Last year, a group of Texas hackers snatched unlisted phone numbers and personal credit information from private networks run by SBC, GTE, MCI, and Sprint—and wreaked \$500,000 of damage. But what scared telephone companies and the FBI most was the group's ability to gain control of core programs, known as root access, enabling the transgressors to reroute calls from FBI crime centers to sex chat lines in Hong Kong and Moldova.

The good news is that so much talent is being dedicated to improving computer security.

UNKNOWN ACCOUNTS added to your system. Hackers may have created a back door onto your network.

EXCESSIVE LOG-ON FAILURES With enough knocking, hackers can force some doors on your intranet to open—and some accounts don't automatically close after a certain number of attempts.

UNEXPECTED CRASHES or reboots of the computer. Some hacks require the addition of new code, followed by a reboot to load it. If you didn't just reboot your system, who did?

MISSING LOGS or gaps in records. Sometimes, hackers can only cover their tracks by deleting portions of files. Gaps, then, become the telltale tracks.

HEAVY TRAFFIC after midnight. Do you do a lot of communing with your Asian office? If not, think about why your midnight-to-sunrise traffic suddenly exceeds your daylight loads.

SYSTEM LOGS that quickly fill up. Each company is different, but these critical logs are usually spare because only a few people have access. If a hacker is impersonating a "sys-op," you'll see it here.

DATA: PRICE WATERHOUSE SURVEY

Netscape, Microsoft, IBM, Cisco, and Lucent have all made it a research priority. And startups are turning it into a market. Its leaders include Checkpoint Software, Network Associates, VeriSign, Security Dynamics and its RSA subsidiary, and Entrust, which have a combined market cap of about \$11 billion.

E-PASSPORTS. Their primary strategy emulates the military doctrine of deterrence: make it so expensive for interlopers to gain access that it simply isn't worth the cost. Companies do this by constructing concentric layers of encryption, using quick-changing passwords, and adopting devices known as digital certificates. The certificates act as electronic passports, strictly limiting entry to different areas of the network.

None of these defense schemes is cheap, however. And in the end, says GTE's Danahy, "You're protecting yourself against a risk that you can't quantify all that well." Barclays Bank PLC, for instance, calculates that it costs about \$800,000 a year to maintain each of its three major fire-

walls. "Even for a large corporation, that's a major expense," says Paul G. Dorey, group operational risk director for Barclays.

Many companies now sell off-the-shelf firewall products. But the systems must be customized, since no two companies will make the same decisions about which employees or outside customers should have access to different areas on the network. Monitoring and maintaining the firewalls also soaks up plenty of human resources. As for digital certificate systems, implementation costs run about \$185,000 for a large business and nearly as much each year to keep current. Meanwhile, user authentication, which relies on rapidly changing passwords, can cost as much as \$4 million to roll out across a big organization.

ARE YOU CERTIFIED? But, if you're doing business across the Internet, your security is only as good as that of your E-commerce partners. Many companies hooking partners up to an extranet now specify the types of routers, firewalls, and security procedures each partner must employ to safeguard the extranet connection before turning it on. Cisco Systems Inc. is going one step further. The networking giant sends its own security engineers to examine a partner's defenses and holds the partner liable for any security breach that originates from its computers.

Federal Express Corp.'s challenge is to maintain security as it manages 60 million electronic transactions every day. Some 140,000 employees use its systems, which have all sorts of information that must be kept confidential: account numbers, container contents, and even home addresses of senior executives at customer companies. "A loss of trust would be very expensive," says Tom Buss, FedEx's senior manager for data protection.

In May, the company began distributing digital certificates to all its employees. These unique IDs cling to the owners wherever they roam in FedEx's vast computer system, and they are required each time a user seeks access to certain computers or records. They raise barriers against internal hackers, who are at least as common as attackers from the outside. One big advantage of certificates, Buss says, is that employees need to remember only a single password to activate their digital certificates when they log on at the beginning of a computer session. After that, access—or denial—is automated and invisible.

Even if such approaches spread rapidly, however, they represent only a partial fulfillment of the promise of Web commerce—the promise of ubiquitous access at low cost. That leaves many companies waiting for stronger assurances before moving more of their business online. Says Sullivan-Trainor: "Business folks can't walk into the Internet naked and expect it to give them the kind of coverage they need to do business." For now, at least, companies have to bring their own suits of armor.

By Paul C. Judge in Boston

In
but
today
it's
just
about
win



Part of the
Electric

COMMENTARY

By Neil Gross & Ira Sager

CAUTION SIGNS ALONG THE ROAD

Business, consumers, and techies are grappling with the Net's perils

Companies are tearing up the track in the race to realize Internet-based electronic commerce. That's fine. Fortune will certainly favor the swift. But it pays to consider some of the yellow flags that have flashed along the roadway—and others that will be spotted before long.

The Net already feels jammed at times, even though E-commerce is still in its infancy. And there are other obstacles. Technical standards remain to be worked out. Security is much on executives' minds. And there are cultural questions that cut to the core of how people choose to amuse themselves. How

many after-work hours will ordinary consumers be willing to spend shopping online? The Net has already demonstrated a capacity to correct its own errors. E-commerce will certainly not be derailed. But there will be jolts and delays along the way.

Congestion is the most obvious challenge. By the year 2000, the number of devices equipped to tap into the far-flung Info Highway will shoot to 233 million, up from 16 million in 1995, according to market researcher International Data Corp. (IDC). Nearly 46 million people will be buying goods and services over the Net, up from 4 million who do so now. A decade after that, IDC envisions 1 billion wired consumers—with Net links to countless information appliances in the home, from smart TV-set-top boxes to refrigerators that alert the service shop when they need repair.

REROUTING TRAFFIC. Yet congestion is mainly a technical problem—exactly the kind of thing smart engineers can finesse. They're already handing out fast cable and digital-phone modems to consumers who are cursing slow 28.8-kilobit Internet access. Businesses also will learn to avoid logjams on the Web by using backup computer servers and by routing some types of traffic at odd hours or along less-traveled pathways. Through such steps, companies can probably cope with "flash crowds," which IBM researcher Steve R. White expects to occur as more businesses mount widely publicized online sales and other events.

Security and privacy are knottier problems. Today, Net security is practically a contradiction in terms, says Jack Danahy, director of security services at GTE Internetworking Services. "The Internet is a medium developed to provide wide access to information," he points out. "But security means being able to restrict access selectively."

Worried about hackers and internal snoopers, your network managers probably seal off access to certain areas of the company using "fire walls" and other techniques. But open Internet standards weren't designed with such secrecy in mind. And when companies take ad hoc measures, they wind up sporting a host of incompatible software systems, making communications more cumbersome. Here again, the techies will probably rescue us. Security

NET FACT

Offline sales of services worth \$4.2 billion were affected by online data in 1997, says Cyber Dialogue/Find SVP



For
sam
solu
the
com

is a hot research pursuit in Silicon Valley and in dozens of academic computer-science labs.

This is not to suggest that business managers can sit back and wait for the gear heads to cook up all the necessary fixes. E-commerce is too critical to be left under the stewardship of any one group. Besides, not all the solutions can be digitally crafted. Academics and engineers will have a hard time resolving issues about personal privacy, which are more social than technical. Information wants to be free, we are repeatedly informed by the rapt disciples of Internet bard John Perry Barlow. But whose information do they mean? The growth crime of the new millennium, according to Net-savvy crimefighters, is a sinister offense called "identity theft," in which crooks sniff out your Social Security number and a few other stray bits of data, then assume your identity and acquire credit cards and bank loans in your name. Not exactly what Barlow had in mind.

Should we forbid companies to stockpile personal data on individuals? Probably not. Enforcing such a ban would be nearly impossible. And if it were imposed, it would present an entirely different kind of threat to E-commerce. Internet businesses have had a hard time dreaming up models for revenue streams that can actually deliver profits. One of the most promising business approaches involves tracking people's preferences online and tailoring products to those users, or else selling the information to others who wish to do so. Throttling the flow of data—if it's even possible—would shut off one of the most promising Net-based business opportunities.

CLEAR LABELS. Fortunately, there are less radical solutions. Indeed, like a living organism, the Net has already spawned features that may thwart the worst privacy abuses. The model here may be TRUSTe, a body created by the Electronic Frontier Foundation to make clear how different Web sites deal with user privacy. The purpose is not to prevent sites from tracking visitors' explorations. The group audits Web sites, and then permits them to display so-called Trust-

marks that clearly identify each site's privacy policies, so that Net users will be able to make informed decisions.

In the same ad hoc fashion, groups of tech-savvy businesspeople hope to resolve the most rancorous debates over technical protocols. Right now, the lack of common standards threatens E-commerce in several ways. Thousands of corporations, for example, are automating their manufacturing, shipping, and warehouse activities by installing sweeping enter-

prise programs from the likes of Oracle, SAP, and PeopleSoft. These programs don't swap data with one another easily. And neither do the companies that install them.

Where ad hoc associations can't tread—deep inside corporate board rooms—pressure to become more efficient may be the best safeguard against threats to E-commerce. Many companies, for example, show worrisome signs of transporting bad business practices directly onto the Net. Gartner Group Vice-President Vinnie Mirchandani has a favorite example of this. Even when dealing with trusted suppliers, he says, manufacturers often require repeated checking of purchase, shipping, and receiving documents to make certain they match. Typically, each such match may cost the company \$150 in labor, tools, and re-

views before the purchase order gets issued. Freewheeling Internet communications offer a means of slashing this redundancy—but businesses aren't taking advantage of it. "Companies simply don't trust their suppliers," complains Mirchandani.

Well, they must learn to, and they will. In the 1980s, companies rushed to reengineer flawed business practices, spurred by nothing more than the need to compete more effectively in a global economy. If Net-based businesses don't tear up old approaches to orders and inventories, they'll soon find that competitors who did so are racing past them. Learning, in the end, is what this whole business is all about.

Neil Gross and Ira Sager write about computers and information technology.



PRIVACY Encryption helps. But with more personal data flooding online, consumers fret about crimes such as "identity theft."

STANDARDS Businesses running crucial corporate-software programs from Oracle, SAP, and Peoplesoft cannot swap data easily. Robust standards are missing.

CONGESTION You think today's traffic jams are bad? Wait until 2000, when 233 million devices are wired to the Net—15 times the number in 1995.

BOOKKEEPING Businesses must streamline their order and payment processes before attacking E-commerce. Most just carry old ways onto the Net.

QUALITY Networks, which businesses are ever more dependent on, crash

CULTURE Millions of people are already glued to PC screens all day. Many will balk at additional hours of screen-gazing for home shopping and entertainment.

NET FACT

Companies may invest \$23.6 billion by 2002 to upgrade their E-commerce systems, according to ActivMedia

Code Breaker Cracks Smart Cards' Digital Safe

N.Y. Times 6/22/98

By PETER WAYNER



Peter DaSilva for The New York Times

Paul Kocher of Cryptography Research holds a smart card and a modified reader he developed to help decipher the digital code of the cards that are used by banks and financial institutions.

To the companies in the smart card business, Paul Kocher may be too smart for their own good.

For the last year, Mr. Kocher's four-man consulting firm in San Francisco has kept big credit card companies and banks on edge by sharing details of his discovery of a way to break into the newest version of smart cards — credit-card size devices that contain a tiny computer chip and can be used for a variety of purposes including storing so-called digital cash.

Although Mr. Kocher's intent has been to warn the industry and sell it possible solutions, his expertise, in the hands of thieves, counterfeiters or impostors, could compromise the security safeguards of smart cards, which are coming into widespread use in this country and in Europe.

The cards are at the center of the plans by the banking and credit card industries to cut costs and improve customer convenience by replacing conventional magnetic-stripe cards with ones that not only can act as a debit or automated-teller-machine card but can also be loaded with digital cash that would function as legal tender wherever merchants have digital-cash decoder terminals.

Public confidence in the technology will be crucial to the industry's plans. And that may help explain why, since word leaked of Mr. Kocher's break-in

methods two weeks ago, the industries promoting smart cards have tended to play down his technique by calling it a "laboratory attack" that could be replicated by perhaps a handful of people around the world.

"Chip cards are the most secure technology around," said Steve Schapp, the executive vice president of Visa International in charge of developing smart cards. "They are very hard to break."

Mr. Kocher and his colleagues were able to crack the digital code designed to make the smart cards tamper proof by drawing mathematical inferences from the fluctuating electrical power consumption of the chip. It is a sophisticated type of analysis, but the rudimentary "laboratory" — in this case a three-room office suite, some garden-variety PC's and several thousand dollars of electronics equipment — indicates that it does not require elaborate tools to crack what is supposed to be a highly secure digital safe.

As details of the technique circulate, as they invariably do in the hacker underground, imitators will almost certainly try to duplicate Mr. Kocher's experiment. For his part, Mr. Kocher, who at 25 is already a well-known expert in code breaking, said, "As the expertise becomes more widely available, the threats will become more than academic."

Peter Neumann, a computer scien-

Continued on Page 2

sounds like a Cantor Fitzgerald statement

Code Breaker Cracks Digital Smart Cards

Continued From First Business Page

tist at SRI International, a research group in Menlo Park, Calif., said the approach had "enormous potential as another technique for breaking weakly designed and badly implemented devices."

Though already in wide use as bank cards in Europe, smart cards in this country have been mainly used so far for controlling access to buildings and protecting against fraudulent use of new types of cellular telephones. But American banks have begun experimenting with the cards, as Chase Manhattan is doing in a test of Mastercard International's Mondex system on the Upper West Side of Manhattan.

Banks trust that the computer chips embedded in tamper-resistant packaging will act like a virtual branch office, dispensing money and crediting accounts to the right people.

But if someone could break through the card's defense, then that person could conduct fraudulent transactions, load counterfeit digital cash onto the cards or create various other forms of mischief.

So even as smart-card executives seek to play down the threat posed by Mr. Kocher's discovery, and they stress that no known break-ins of his sort have occurred in the real world, the industry knows it must continuously improve smart-card software and hardware.

"In a sense, this is an arms race; the attackers will always get better," said Richard Fletcher, the head of strategy and planning of Mastercard's Mondex smart-card division.

"The only defense and the best defense against future attacks is to keep moving and keep changing."

Gerald Hubbard is the vice president of marketing in the United States for Bull Smart Cards, a company that says it has shipped more than 120 million money-carrying smart cards throughout the world. He said that his company had known about the Kocher type of attack for more than four years and had in-

Virtual guards are sought to protect digital money.

stalled safeguards to thwart it. But, Mr. Hubbard said, "You can never say a card is 100 percent immune."

In fact, some other industry executives expect it to take perhaps two years before there will be smart cards and related hardware that will be impervious to Mr. Kocher's type of attack. Mr. Kocher said he had approached the smart-card industry last year with the details of his discovery because he knew that criminals might also use the same tricks. But he said that he did not publicize his findings so that the industry would have time to adopt defenses, including techniques for which he has filed for patents and is now licensing to the companies.

He publicly announced the smart-card security flaw two weeks ago, only after The Australian Financial

Review published an article about his break-in technique.

Mr. Kocher's company, **Cryptography Research**, analyzes and tests computer security hardware and software for many of the leading computer companies. His discoveries of flaws in supposedly secure technologies have drawn attention in the past — as in 1995, when he found that he could break into smart cards by simply timing how long it took them to process data.

In the case of this newly disclosed smart-card problem, Mr. Kocher and his colleagues found that the cards' consumption of electrical power could disclose vital information about the secret key that protects the money or other data on the chip.

By watching the monitor of an oscilloscope, a device that measures the power use on a screen similar to the way a cardiac monitor displays a patient's heart action, Mr. Kocher's team was able in some cases to use the electrical pattern from a single transaction to decipher the key to the code. In other cases, they were forced to use more sophisticated statistical techniques to analyze the results from as many as 1,000 transactions.

Mr. Kocher said his team had spent at least as much time looking for solutions as it had in identifying the security flaw. A possible remedy involves masking the transaction in digital noise by adding meaningless random calculations that would consume random amounts of current.

Another possible solution, which according to Mastercard officials is being incorporated in the latest version of its Mondex smart-card software, is to vary the order of the

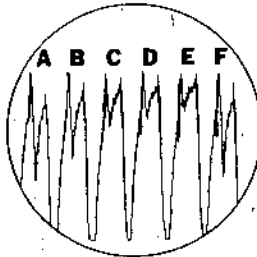
Cracking the Code

By monitoring the power consumption of smart cards, an expert in electronic security has discovered a way to crack the code that protects information on the cards — credit-card size devices that contain a tiny computer chip and can be used for a variety of purposes, including storing so-called digital cash. Here is how the security code can be breached.

Source: Cryptography Research

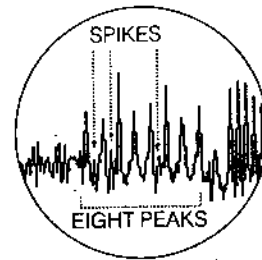
LOOKING FOR PATTERNS

When the card is in use, its microchip performs a number of operations, each of which requires different amounts of power. By hooking the card up to an oscilloscope, a machine that records power use, the distinctive patterns from each operation can be recorded. Above are six operations done by a smart card in 1.68 microseconds. As recorded by the oscilloscope, operations A and F are identical, as are C and D. This series of peaks occurs whenever the card performs that series of operations: If one peak is omitted at some point, it would indicate an important change in the computation.



DOING MORE ANALYSIS

Because looking at the pattern created by a number of computational cycles is not enough to figure out the security codes, other types of analysis are needed, like the example above. Each point on these peaks depicts an average of four cycles like the ones above. The sequence of eight peaks indicates a part of an encryption operation that protects information on the card. The presence or absence of spikes between these peaks gives analysts a piece of the encryption key, of which further, similar analysis may reveal additional pieces.



The New York Times

operations in the software to make it more difficult to identify patterns in the consumption of power.

A banking industry goal with smart cards is to cut costs by eliminating the need for central approval of a debit or credit transaction. By some estimates, the marginal costs for clearing a smart-card transaction are well under a penny.

Credit card transactions, however, typically require a long-distance computer network and a large central data base for examining each deal, and the transaction eventually means billing a customer and cashing the payment checks. These steps add up to 25 cents a transaction, on

average, compared with about a penny for a smart-card transaction, in which all the authorization information — and even the money itself — can be contained on the card's chip.

To create an audit trail that might help track fraud, however, Visa International's smart-card system uses merchant terminals that report transactions to a central data base at the end of each day.

"We don't feel it is a good idea to have the security depend upon the chip itself," said Philip Yen, a senior vice president of Visa International. "We think it's more important to have complete system security."

Mr. Fletcher, of Mastercard's

Mondex, contends that including any sort of central control runs counter to the purpose of a smart card — giving customers the ability to use the money on a card just like cash.

"The critical point of any digital cash system is that you're off line," he said. "There's no on-line link at that point. You're critically dependent upon the card's security."

As the banks debate the security trade-offs, there is one certainty: Paul Kocher and others like him will continue to look for chinks in the smart-card armor. And as Mr. Kocher likes to remind the industry, "We have not yet encountered a card that couldn't be broken."

Researcher Discovers Flaw in Software Used on Web to Encrypt Transactions

By DON CLARK

9/26/98

Staff Reporter of THE WALL STREET JOURNAL

A researcher at Lucent Technologies Inc.'s Bell Labs unit has discovered a software flaw that could allow thieves to decode electronic-commerce transactions under some circumstances.

The researcher, Daniel Bleichenbacher, said he found a way that a well-equipped computer hacker could decode the contents of an Internet session protected by the standard encryption scheme used in most World Wide Web commerce. But the attack requires a special connection to siphon off Internet traffic, and the ability to send about a million specially crafted messages to a Web site operator. By analyzing electronic responses to the messages from the Web sites, an attacker could get information that could be used to decode an intercepted session, Mr. Bleichenbacher said.

Though the attack hasn't yet been used, Mr. Bleichenbacher's notification triggered feverish activity by makers of software used on server machines to manage Web commerce. The software companies, including Netscape Communications Corp., Microsoft Corp. and Security Dynamics Technologies Inc.'s RSA Data Security Inc. unit, said they have already begun to distribute software code that is believed to fix the problem.

"We are taking it very seriously," said Debby Meredith, a Netscape senior vice president of customer satisfaction. "We were on the phone all day yesterday with customers, all day today and we'll be on the phone again tomorrow."

The security of electronic commerce is a sensitive issue, in part because the market is taking off rapidly. Sales through Web sites are taking a growing share of the market for books, airline tickets, securities and several other product categories. Consumers this year are expected to spend \$3.3

billion over the Web, Forrester Research Inc. estimates, and business purchases are running at several times that rate.

Software makers have sold hundreds of thousands of Web server programs that use a standard encryption scheme known as secure sockets layer, or SSL, which relies on technology developed by RSA. Netscape said it has already supplied the fix to some of its largest electronic-commerce customers, including BankAmerica Corp. and Charles Schwab Corp.

"There are a series of interlinked Web sites that will provide customers with upgrade patches to fix the problem," said Scott Schnell, an RSA vice president. "If all goes well we will have nipped this thing in the bud before a significant attack ever takes place."

To intercept an electronic-commerce transaction, a computer hacker would need a physical connection to one of the server computers that passes messages along the Internet, such as the machines operated by Internet service providers, Mr. Bleichenbacher said. To decode an intercepted message, the attacker would send about one million messages back to the electronic-commerce server, and then examine the error messages that server sends back in response.

Mr. Bleichenbacher said he developed a mathematical formula that was able to analyze the error messages to generate software code needed to unscramble the original message. Besides the difficulty of generating one million messages, executives at RSA and Netscape noted that the sheer volume of messages would make it easy to detect an attack.

Mr. Bleichenbacher said he had only demonstrated the attack in a laboratory setting. But RSA's Mr. Schnell said that the company's researchers had validated the dangers of the discovery.

STORY:1a253f

From the National Journal

Washington--Jun 12--An informal survey of 10 large utilities found only 2 had completed a full assessment of the potential problems that might occur when their computers reach the year 2000, Sen. Robert Bennett, R-Utah, chairman of the Special Senate Year 2000 Technology Problem Committee said today.

*

*

*

That survey also showed none of the utilities have gotten assurances from their suppliers and vendors they had addressed the Y2K problem. "I am genuinely concerned about the prospects of power shortages as a consequence of the millennial date change," Bennett said. He added the private sector is just beginning to realize the related year 2000 problems of faulty embedded computer chips and the industry's reliance on other entities that may not be prepared. Bennett released the survey at the committee's first hearing today while committee members laid out their future agenda.

Deputy Energy Secretary Elizabeth Moler told the panel the government must play a facilitating role in helping the private sector address its year 2000 problem, as it has been doing with an energy working group that includes the DOE, Federal Energy Regulatory Commission and the industry's North American Electric Reliability Council. "Let me emphasize that the federal government cannot solve this problem," she said. "It is up to the industry itself to do so."

FERC Chairman James Hoecker said the industry has yet to determine the impact of the year 2000 problem, in which computers read the last two digits of the year as 1900. "Compilation of this information has been inadequate. Larger utilities and some industry associations have promoted awareness of year 2000 issues," Hoecker said. "The state of awareness and planning of small utilities and cooperatives is less certain." Committee ranking member Christopher Dodd, D-Conn., urged both the government and industry to give the panel as much information as possible. "You need to put us on notice up here so we can be doing smart things legislatively," Dodd said. End

'Good' hackers being recruited for front line of computer security

By Robert Trigaux
St. PETERSBURG TIMES

Chicago Trib.
4/22

Ira Winkler doesn't mince words about the inability of U.S. businesses to protect themselves against hackers.

"I can teach a monkey to hack a computer system in two hours," sniffs the former technology director of the International Computer Security Association.

One-time Tampa consultant Jack Kerivan became so concerned his hacking tools could fall into the wrong hands that he designed his break-in programs to self-destruct every 30 days.

Scott Ramsey, who set up Ernst & Young's national computer security team, gives corporations a B- for their security efforts but a D+ for execution. "It pays to be paranoid," he warns.

Good-guy hackers—known as "ethical" or "white hat" hackers—are part of a fast-expanding and cocky breed of security troubleshooters delivering a blunt message to U.S. companies. With malicious hacking on the rise, corporate computer networks increasingly linked to the Internet are as easy to penetrate as fists punching through Jell-O.

Long in denial, corporate America is starting to listen. Company-approved test attacks by ethical hackers are cropping up nationwide. So far, their efforts are rarely unsuccessful.

In San Antonio, ethical hackers at Cisco-WheelGroup Corp. spring their attacks on corporate customers from a "war room" run by ex-military types from the Air Force Information Warfare Center. From a windowless room in the New York suburbs, IBM's security squad launches its hacks on dozens of corporate customers. In Miami, an Ernst & Young team recently hacked with ease into the network of a high-tech client in the Tampa Bay area.

Work is plentiful. Nearly two of every three companies responding to a recent Computer Security Institute/FBI survey say they experienced unauthorized use of their computer systems in the past year. That's up from 50 per-

cent in the 1997 survey and 42 percent in 1996. And while company computer systems were hit both internally and externally, companies' Internet connections were cited increasingly as a frequent point of attack.

But security expertise does not come cheap. Ethical hackers, especially those backed by big corporate and consulting names, regularly charge \$20,000 to \$200,000, depending on the depth of their attack and the size of the business client's network.

American companies spent about \$6.3 billion on computer security last year to combat computer fraud, theft of proprietary company software and industrial espionage, according to the research firm DataQuest. The market is expected to double to \$13 billion by 2000.

Security experts say companies simply will have to pay to play on a secure Internet.

Besides assaults from malicious hackers, companies face threats from disgruntled workers and ex-employees. Competing businesses—under the buzzword "competitive intelligence"—increasingly are snooping on-line for information to help make a big sale or gain a technological edge.

Corporations in some industries also must guard against intrusions from tech-hungry foreign governments—in particular China, France, Israel, Japan, Germany and Russia—that converted their cold-war spy machinery into "economic espionage" units.

French intelligence allegedly has spied on U.S. companies by electronically snooping on U.S. businessmen flying on Air France between New York and Paris. And Germany's Federal Intelligence Service had been successful in economic espionage by using a top-secret computer facility outside Frankfurt to break into data networks and databases of companies and governments around the world, according to a report by Edwin Fraumann, an FBI agent.

The big fees paid for corporate security are attracting hackers with more troubling credentials.

Many are swapping their old black-hat ways for white-hat paychecks, jumping into the potentially lucrative corporate computer security business.

Among the "reformed" is Yobie Benjamin, a hacker for 20 years who now works as the technical security guru at Cambridge Technology Partners, a Massachusetts network consulting firm. Best known for finding flaws in Microsoft's Windows NT operating software, Benjamin says he hires white-hats, though many are reformed street hackers now in their 30s.

Large companies don't seem to mind. Last month, Benjamin's company invited data security managers from three dozen Fortune 1,000 companies to attend "New Hack Tour," a seminar on the latest hacking trends. They were dismayed to hear of dozens of new network hacks making the rounds.

Six years ago, a massive party was thrown by a young computer bulletin board operator who goes by the name Dark Tangent. That party evolved into the DefCon annual convention, the biggest hacker gathering in the country. And Dark Tangent, who in real life is Jeff Moss, now provides security consulting for San Jose's Secure Computing Inc.

The trend of hackers-turned-consultants makes for some lively debate.

"Would you trust an ex-burglar or an ex-arsonist?" Ken Lindup, a senior consultant at security specialist SRI Consulting, asked at a recent security conference.

Lindup gives a thumbs down to hiring once-nasty hackers to wander through company computer systems. Avoid the temptation, he advises.

On the flip side, many traditional hackers suspicious of Big Brother aren't happy about their brethren defecting to the security establishment. Complained one hacker: "It's like Anakin Skywalker (Luke Skywalker's father, before he became Darth Vader in Star Wars) being seduced by the Dark Side of the Force."