OSS, Inc.

OPEN SOURCE SOLUTIONS, Inc.
International Public Information Clearinghouse

Speech to Surveillance Expo '94, 11 August 1994, McLean Hilton, Virginia

NATIONAL AND CORPORATE SECURITY IN THE AGE OF INFORMATION

MR. ROBERT D. STEELE, PRESIDENT
Direct Telephone: (703) 242-1701

It is impossible to establish corporate electronic security measures in a vacuum. Sound corporate electronic security is unaffordable and unenforceable unless the Nation as a whole provides for the security of the digital environment, unless the Nation itself has a national information strategy with embedded communications and computing security policies and practices.

This speech is about how you need to get your Chief Executive Officers (CEO) to understand the fragility of the international communications & computing industry, and of our national and global information infrastructures. If our CEOs don't focus on this, and lobby aggressively for a national information strategy which includes electronic security standards, electronic security testing, electronic security education, electronic security law, and electronic security tax incentives, then you individually are engaged in "mission impossible", and destined for catastrophic failure at some point in your future careers.

This speech is also about how you need to quickly develop a legal strategy for being able to prove due diligence with respect to electronic security on your part, and lack of due diligence on the part of your communications and computing suppliers of both products and services.

There is going to be a tidal wave of legal liability suits in the next five years. You need to rapidly establish internal testing, auditing, and documentation procedures that will protect you in court from stockholders claiming you have failed to protect proprietary information; and also help you to win damages from suppliers whose deficient products allowed your systems to become infested by electronic cockroaches, many of which will destroy or degrade data and performance.

At this time, our Nation has a communications & computing house built over a sinkhole. It is simply not safe to work and play in cyberspace, and it will take at least five and perhaps ten years of concerted effort to rectify generations of neglect.

An entire generation of hardware and software engineers has emerged for whom the word "security" has no meaning, with the result that it is virtually impossible to purchase and administer complex systems which support proper security. At the same time, corporations have been slow to realize that they are buying infected or deficient communications and computing products, while also failing to recognize and document financial losses stemming from electronic defects. It is my impression that most corporations do not have adequate testing and auditing procedures in place. It should concern you that one organization--one which I consider very computer-literate--found over 500 viruses in a single year inside of shrink-wrapped products delivered directly from the factory.

Locking the doors and avoiding external contact is not the answer. Organizations are finding that in an era of distributed information, the old solution for security--system isolation and physical security--is simply not feasible. In the age of information, security comes from knowing that what is worth protecting, is worth protecting well. Proprietary information should be in an isolated system with full TEMPEST protection, access controls, and access audit trails. At the same time, one must understand that in the age of distributed information, security can also be found in speed, a speed of collection, processing, and dissemination that cannot be achieved in a closed TEMPEST environment. Connectivity to content is at the heart of corporate competitiveness today, and misguided security policies and practices which attempt to protect employees by cutting off access to the external world are in fact the death knell of the corporation.

Let me elaborate on that for a moment, for I have found that corporations are making the same mistake the U.S. intelligence community is making. Any given organization deals in two kinds of information: 20% of it is internal, precious, and considered proprietary or classified. This information merits exceptional security. 80% of the information, by contrast, is not only routine, but actually has a barter value. This includes basic market survey information, customer data, and so on. Where organizations go wrong is in mixing both kinds of information on the same system.

They lose twice. On the one hand, because the proprietary information is in the larger system, and the larger system is simply too large to TEMPEST and manage according to well-established safe C4I practices, the corporation does not properly protect its secrets. They are out there with the general information population, and can be gotten to.

On the other hand, because the secrets are on the main system, the corporation lives in fear of being penetrated, and therefore prohibits or seriously constrains external connectivity, thereby handicapping employees who might otherwise have established effective electronic access to customers, suppliers, advertisers, and others, as well as data held by others outside the company.

In the Information Age--when information is a substitute for time, space, labor, and capital--the survivability, security, integrity, and reliability of information becomes the most fundamental foundation for national security and national competitiveness. *The National Information Infrastructure (NII), and the larger Global Information Infrastructure (GII) of which it is the core, must provide the knowledge workers of America with a safe working environment. In keeping with international labor standards, the worker whose labor depends on the NII must be assured that the product of their labor is protected.*

We have a house built over a sinkhole! While I will address service and product reliability, I must first express my grave concern over the total vulnerability of our society--of every aspect of our commerce, banking, and trade as well as the other sectors addressed today--to interruption of services and the destruction of data.

It is my view that the civil infrastructure for our national communications and computing is of such enormous importance to our survival and prosperity as a Nation, that a Presidential initiative should be immediately undertaken to shift one billion dollars a year from the Department of Defense to the NII, in order to provide for a minimal level of "rear area security".

Working with hackers from Europe, New York, and the West Coast, I have over time formulated a simple list of the top ten targets in the United States of America--targets easy to destroy, targets whose destruction would bring this country to its knees in three to seven days.

Among those targets I include satellite dishes associated with the Global Positioning System, which incidentally also provides computer time synchronization as well as the precision guidance for advanced munitions; satellite dishes associated with our major intelligence and defense activities; the telephone switch in Virginia which serves the National Capital Area; computer-directed telephone and power grid transfer points, and the computers associated with our major banking and financial institutions. The ease with which these vital services can be interrupted cannot be understated. A single day's failure in banking costs billions of dollars in lost interest, penalties, and recovery.

Taking a really mundane example, let me note with anxiety that all of our most important cable crossings, which coincidentally are also the easiest to damage accidentally, have large signs at their point of exit and entry to the water--signs which say, in effect, "cut here".

It is of concern to me that we have an entire generation of communications and computing engineers who have gone from studies to striving to standards, all without ever having to consider security requirements. It has been a free ride with no accountability. Unfortunately, while the Internet and other elements of cyberspace have been evolving in dramatic fashion, they have also been creating an electronic environment of such complexity that we are now vulnerable to catastrophic failures. What Charles Perrow calls the "normal accidents" of highly technical systems are upon us. Government has failed to provide the leadership and the funding necessary to nurture a robust gamut of security standards in the private sector.

There is a growing constituency of respected authorities and leaders of public thinking who are gravely concerned about the dangers that are proliferating in cyberspace. It includes not only my friends Alvin and Heidi Toffler, Paul Strassmann, and Winn Schwartau, whose most recent books have served to sensitize not only our own public, but also foreign governments and corporations as to the opportunities and risks inherent in doing business in cyberspace. Both our own public, and our political and economic partners around the world, are looking for leadership, and they are all focused on security rather than connectivity, as the litmus test of a credible NII/GII.

I will also tell you, in my capacity as a student of war and peace in the age of information, that I believe the greatest threat to our infrastructure is not from other nations, but rather from financially-motivated individuals. Individuals taking short positions on specific information-intensive companies, who can then cripple those companies by degrading or destroying their data; and individuals able to exploit a specific company's vulnerabilities and then hold its electronic environment hostage to ransom, come to mind. It should concern all of us is that the ability to wreak subtle and not-so-subtle havoc is no longer restricted to those brilliant individuals called hackers--the spread of shareware has placed enormous power in the hands of fools.

Consider the implications of this power in the hands of someone who knows how to buy short on the stock-market, and is able to select a corporation whose information infrastructure is a critical aspect of its profitability. Degrade performance, destroy data, and reap the dividends, all the sweeter for being able to bet against the market with the confidence of one who knows when the electronic attacks are going to have their effect.

I have chosen to focus on the issue of interruption of services, and the need for a billion dollar a year realignment of funds from Defense to the NII, because I believe that the underlying survivability of the system is a precondition for its security, integrity, and reliability. It would be a significant error on the part of the Administration, and of Congress, to allocate millions or billions of dollars to the development of information warfare capabilities against others, as we are now planning, while ignoring the urgent unfunded needs for security within our own electronic environment. We live in the proverbial "glass house"!

You cannot survive interruption of services which stem from a basic government failure to provide a safe working environment in cyberspace. This is why your CEOs must be mobilized and must lobby for a national information strategy act which provides funding for basic security measures throughout the electronic network that is now the life-blood of our productivity. Between 40 and 60% of the Gross Domestic Product is considered to be information services work, depending on who is counting what. This means that 40 to 60% of our productivity is at risk--is vulnerable to a total shut-down of the electronic transportation links which do not have a fraction of the security common to the physical transportation links that supported our national power during the industrial age.

Apart from the fundamental issue of electronic survivability, we have the issues of reliability, integrity, and content security which are being addressed by the NII Security Committee, where I was one of nine people testifying on commerce and banking concerns this past 15 July 1994. The fact is that we are, as Dr. Vint Cerf, President of the Internet Society has put it, "behind the eight ball" on national information security standards, testing, law, and practice, and it is your corporations that are going to pay the price when we have a series of electronic Chernobles across the country.

We have entered an era when corporations are going to live or die based on their ability to rapidly exchange electronic knowledge and information with one another. However, neither our legal system nor our economic model have kept pace with electronic democracy and electronic productivity. Worse yet, it is simply not safe to work and play in cyberspace.

In consultation with Bill Caeli in Australia, Winn Schwartau in Florida, and a couple of others I choose not to name, I have come to the conclusion that we must all work hard to get our respective Governors, Senators, and Representatives to insist on the immediate realignment of $1 billion a year from the Department of Defense budget to the National Information Infrastructure budget. I recently testified to this effect before the newly formed NII Security Committee, and was asked how I would propose the billion a year be spent. Following is my response:

-- 100 million a year to establish and operate a joint government-private sector consortium, completely independent of the Administration, to establish security and privacy standards. The Internet Society model for standards development is much superior to the traditional process, and could serve as the foundation for this consortium. I would endorse the idea of having The Internet Society, in association with the IEEE, administer the consortium. I would like to see the DoD Office of Net Assessments assume a greater role in evaluating our vulnerability, and to create a special office in the Federal Bureau of Investigation which is dedicated to electronic counter-intelligence in direct support of the private sector. The first thing they should all look at is the proposed backbone for the NII, which I understand is incapable of coping with ultra high speech cryptographic data streams.

-- 150 million a year to establish independent testing and certification laboratories to verify the efficacy of information security products. I am gravely concerned by the number of viruses contained in shrink-wrapped products (both hardware and software) reaching the consumer, and I speculate that the legal profession is about to reap a bonanza from product liability lawsuits. These funds should also be used to nurture beta sites in the private sector, as a means of ensuring--as the Internet model ensures--that standards are in fact effective and practical in a real-world context.

-- 150 million a year for an aggressive, high profile, education and awareness program aimed at both the government and the private sectors as to the risks and vulnerabilities of the NII, and methods of protection. It is not humorous to note that the comparison between "safe C4I" and "safe sex"--

electronic AIDS is being spread in cyberspace by electronic cockroaches, and we have no established program for maintaining sanitation and security in our electronic working environments. The U.S. financial sector should be the first customer for in-depth threat briefings and hands-on demonstrations of both remote data theft and active data destruction technologies.

-- 250 million a year to establish electronic privacy guidelines and models, and to implement them across critical government systems such as the Internal Revenue Service, Social Security Administration, and Veterans Administration. These funds would also be used to provide incentives--prior to imposing sanctions--on private sector databases. As Winn Schwartau has noted, privacy begets security. I will note as a corollary that security nurtures productivity. Thomas Jefferson would be the first to state, quite firmly, that our laws in this area are archaic and need immediate and comprehensive definition. The Administration has abdicated its responsibility for maintaining civil rights in cyberspace; this is something I expect will come up in November 1994 and again in November 1996.

-- 350 million a year to rapidly overhaul or rebuilt security components in those government and public service systems (including telephone and power switching stations, and financial industry computers) which have open access and are extremely vulnerable to destruction of data or interruption of services. I find it absolutely frightening to contemplate the ease with which this Nation, and its major defense, governance, and private sector enterprises, can be brought to its knees by a few individuals armed with either talent or second-hand shareware. I also find it troubling to learn of our plans for major investments in developing information warfare capabilities against others, at a time when we live in a proverbial "glass house". Our "rear area security" is non-existent, and yet our national security leadership is proceeding as if nothing were amiss--just another Sunday in Hawaii.....

Lacking a coherent strategy for the enhancement AND PROTECTION of the central resource of our economy--KNOWLEDGE--the United States of America risks losing both its political and its economic leadership in the decades to come. Our failure to adopt a national information strategy and provide for "safe C4I", is analogous, to use a Cold War example--to not having had a strategic nuclear deterrent and a conventional army. There is an arms race going on in cyberspace, and we are not competing effectively.

Our non-profit educational corporation is the original and leading advocate for a national information strategy. It is our view that both our national security and our national competitiveness are at risk because the NII, a most worthy undertaking focused on connectivity, has failed to articulate objectives and find funding for three other critical elements of the national information strategy, one of which concerns us today: communications and computing security. We are the authors of draft legislation, "The National Information Strategy Act of 1994", and we are firmly committed to helping the President and Vice President enlarge the NII/GII so that communications & computing security is a deeply embedded and ever-present aspect of our national security and our national competitiveness.

You are the platoon commanders in this electronic war, and right now you have no higher headquarters, no artillery, no air cover, and a three day supply of rations and ammo.

"Have a nice day..."

NOTE: For a copy of draft legislation, and talking points for the Vice President, call (703) 242-1700 or fax (703) 242-1711. A copy of both are available in cyberspace, at <oss.net>, accessible via gopher, wais, or ftp.

THIRD INTERNATIONAL SYMPOSIUM: NATIONAL SECURITY & NATIONAL COMPETITIVENESS: OPEN SOURCE SOLUTIONS Proceedings, 1994 Volume I - Link Page

Previous	Private Enterprise Intelligence: Its Potential Contribution to National Security
Next	Correspondence to Mr. Marty Harris on the National Information Infrastructure Security Committee

Return to Electronic Index Page