



Larry Clinton
COO
Internet Security Alliance

Subcommittee on Information Technology and Information Policy of
Committee on Government Reform
U.S. House of Representatives

Hearing on
Protecting Our Nation's Cyber Space: Educational Awareness for the Cyber Citizen

April 21, 2004

“I’m very busy. Do I really need to read this?”

That, Mr. Chairman, is the first line of the “Common Sense Guide to Cyber Security for Small Businesses” which the Internet Security Alliance released on its web site last month.

We decided to begin our publication in this unusual way because, during the course of the extensive market research we did in preparing the document, we re-learned a critical fact. That is, education is far more than simply raising awareness or disseminating information.

Education, resulting in behavior change, requires motivation.

In the next few minutes I’d like to tell you about the educational activities we have undertaken at ISAlliance. And while we are delighted to present this record to you, I think what is more important is what we have learned about **how** to conduct an educational campaign. As the Bible teaches us, give a man a fish you feed him for a day, teach a man to fish, and you feed him for a lifetime.

By way of background, the Internet Security Alliance was founded in April of 2001, five months prior to the events of 9/11, because even then we saw a growing need for improved information security. We are not, largely, a policy shop. We are interested in practical methods to achieve pragmatic behavior change resulting in improved security.

We are collaboration between the CERT/cc at Carnegie Mellon University and the Electronic Industries Alliance here in the DC area. ISAlliance is unique in that we are an international organization with membership from 4 continents and multiple sectors of the economy. The ISAlliance membership primarily comes from the Internet user community spanning such diverse sectors as banking, insurance, entertainment, traditional manufacturing, as well as telecommunications, security and consumer food products.

For the past three years we have provided our members under strict non-disclosure agreements, the absolute best Internet threat and vulnerability information in the form of several hundred technical e-mails each year from the CERT/cc. We also provide regular meetings on technical security issues.

We have taken this information and produced a series of best practices which are provided free of charge on our web-site as well as giving our members unique opportunities for discounts on education, training and insurance to provide market incentives for improved cyber security. We believe that only the creative use of the market forces can provide the continued motivation that will lead to maximum information security.

Realizing that corporate computer security needed to begin at the top, we published our first best practices manual in July 2002; “A Common Sense Guide for Senior Managers.” The document was very well received. It was abstracted in the draft National Strategy to Secure Cyber Space and endorsed by organizations as varied as the National Association of Manufacturers, the US India Business Council and TechNet. We followed that up in 2003 with a

new best practices document, equally well received “A Common Sense Guide to Home Users and Mobile Executives.”

Based on this work, the ISAlliance was asked at the National Cyber Security Summit in December 2003 to produce another best practices document, this time targeted to small business users.

This was a timely request. Small Businesses are particularly vulnerable to cyber attack. Earlier this year research found that one out of every three small businesses was affected by the MyDoom virus, fully twice the rate of larger businesses. Obviously, larger organizations have more to lose in terms of absolute dollars; however, the smaller margins smaller businesses operate on vastly magnify the impact an attack can have on a small business.

Computer World recently quoted the effect a computer attack had on the owner of one company that had once been valued at over a million dollars, “My business is gone, and my wife’s business is gone. Now we just hope we can hang on to our house.”

Despite the extent and impact cyber attacks are having on smaller businesses there was very little help being offered to this community. The very first conclusion reached by the Best Practices task force you formed, Mr. Chairman, as part of the Corporate Information Security Working Group, was “Available IS guidance as a whole ... is spread over a wide continuum of abstraction and not readily scalable to meet the varying needs of large, mid-size and small organizations.”

Most of the best practices documents that have been written, including our previous efforts, in the cyber security field are written the same way. An information technology expert is asked to tell the target audience what they need to know. We decided to approach the project in a different way, in a market driven way. We decided to ask the target audience what they needed to know and how we could best motivate them to act.

We were delighted with the cooperation we received from virtually all the major trade associations who hold small businesses as primary clients. We coordinated with the National Association of Manufacturers, The National Federation of Independent Businesses and the US Chamber of Commerce. Each of these organizations agreed to gather for us a group of their membership and we conducted 10 focus groups, involving nearly 100 actual small businesses to discuss their cyber security needs.

By listening to our target market we learned a great deal, some of which I would summarize here.

First, we learned that while certainly sympathetic to national security needs, in real life not many small business owners were going to go to the time and expense of improving their cyber security based on the type of public policy appeals common in the existing literature. We needed to speak to their personal needs, not the broad national need.

Second, we learned that many small business owners were not intimately familiar with computer security technology and saw much of the existing material as excessively technical jargon. We learned that this material was unlikely to be read, let alone acted upon.

Third, we learned that although most small businesses were aware of the generalized needs for cyber security, there was an unrealistic hope that it wouldn't hit them, either because they are too small to be noticed or because they have taken rudimentary steps in the direction of security. Since many attacks are generalized to the network, and perpetrators are evolving their methods to circumvent initial defenses, we know that this is a very dangerous misconception.

Fourth, we learned that even if we could convince small businesses that they needed to be more proactive toward cyber security, much of the material available to them was irrelevant. Much previous material was written for technical experts presumably on staff. Small businesses often don't have IT staffs. So, for example, they don't want a "how-to" instruction on configuring their network, they want a "how-to" section on how to evaluate a consultant to come in and do it for them. That calls for a very different type of book.

Finally, we learned, again, that to achieve long-term behavior change we needed to do more than simply share information. You noted it yourself in the letter inviting us to today's hearing Mr. Chairman. You said "For example the Blaster worm infected over 400,000 computers world wide in less than 5 days...despite the fact that the patch that would have prevented infection had been available for over a month." The information was there, the necessary behaviors were not.

We learned from the small businesses we spoke with that they were aware of the potential of cyber attacks, but they are also aware of the costs both in time and money to constantly keep up with the ever evolving threats and vulnerabilities. Attempting to address the needs of small businesses and cyber security without realistically addressing the costs of their full participation is shortsighted and will ultimately be ineffective.

Having been educated by our audience, we produced a document that I believe looks like no other in the field, including our own previous work. To speak to the small business's personal needs we provided a list of real case studies drawn from the media, listed on the FBI website, or reported directly to the Internet Security Alliance during our research.

These are actual cases of small manufacturers, contractors, credit unions, hotels; diners, limo services, law firms' accountants and venture capitalists have all had their businesses severely hurt by cyber attacks. They describe a wide range of situations we believe the typical small business owner can relate to. We call these sections "this could happen to you."

We utilized a true expert, Carol Woody from the CERT/cc, to outline a simple, but by no means simplistic, "12-step program" of cyber security for small businesses. Each section provides step-by-step information including why they need to take the step, how to get started, who needs to be involved, the degree of technical skill required and, specifically, dealing with cost.

Understanding that many small businesses, for whatever reason, were reluctant to resolve cyber security issues on their own, we added a totally new section on selecting a consultant.

Although the booklet is both unique and barely a month old, we are delighted with the reception it has already received. In addition to being available through the Internet Security Alliance web site, and the National Cyber Partnership web site, it is also being provided through the National Association of Manufacturers site and the Electronic Industries Alliance site. I'm told the US Chamber of Commerce anticipates endorsing the publication shortly and is linking its members to the publication. The Financial Services Sector Coordinating Council, an alliance of 28 financial services trade associations and companies that work together to improve critical infrastructure protection and homeland security will be making the guide available to its members. Additionally the financial sector is holding a series of meetings with thousands of its members where the guide will be highlighted.

Additionally, we are in contact with a wide range of other associations to assist in distributing the publication.

However, more important than the product we produced is what we learned about how to produce it. For too long, cyber security has been thought of as an "IT problem" with an "IT solution." While obviously there are technology elements to cyber security it is also a management problem. It is an economic problem. It is a cultural problem. And, to adequately address it we need to listen to the IT people of course, but also to the users, the educators, the marketers and the economists. We need a broad, market centered, and incentive-laden approach to the issue, rather than a narrow, techno-centered dogmatic approach.

Speaking as a former teacher, who is married to an elementary school teacher with two school aged children, I can assure you, education takes more than providing information. Some students are motivated by praise, some by pride in good grades, some by the prospect of tangible rewards. Few are motivated by threats. Computer users are no different. Creative thinking needs to be done on the issue of incentives. I understand that today we are here to discuss the straightforward issues of education. But I would urge the chair to consider another hearing soon to discuss the complex issues of developing market incentives as a compliment to educational initiatives.

Mr. Chairman, the Internet Security Alliance congratulates you on all you are doing to spread the word about information security. We also are proud to be before your committee today with several of our colleagues with whom we are working together in this effort. And while we believe we are working hard and learning more and more how to be more effective, we are also aware that there is still much work to be done. For example, we as yet have no funding to make the guide I have spoken of today available in hard copy.

For this we look forward to greater participation from both industry and government. There is a great deal of work to be done on technology, on education and on developing appropriate incentives. We look forward to continuing our work together.

Thank you.

The Executive Board of the ISAlliance is made up of representatives of the following corporations: AIG Insurance, Ceridian, Cable & Wireless, the Frank Russell Company, ITT Industries, Mellon Financial, National Association of Manufacturers, Norsk Tipping, Nortel Networks, Northrop Grumman Mission Systems, Raytheon, RedSiren, SINTEF, Sony, TATA Consulting, VeriSign, Verizon, Visa.

For more information, please contact:

Larry Clinton: 703.907.7028
2500 Wilson Blvd, Arlington, VA 22201
www.isalliance.org