

The Mag (nificent) Ten
How to Secure Your Networks
ISW 2000 Position Paper

James C. Settle
CEO
Settle Services In
Technology, LLC
P.O. Box 2235
Springfield, Virginia
22152-2235
703-569-0011
703-569-0012 (fax)
settle@compuserve.com
www.settleservices.com

Background:

I retired from the FBI in April 1994, having headed the FBI's revamp of computer crimes in late 1990. I founded the FBI's first National Computer Crime Squad and ran it as a prototype from 1992 to 1994.

From 1994-1996, I established a network security group at I-Net, Inc., in Bethesda, Maryland. This group worked with major corporations helping them to secure their global networks.

From 1996 to the present, I established my own company (Settle Services In Technology, LLC, which is primarily a penetration testing company, does incident response, and computer/network forensics for litigation. Settle Services In Technology, LLC (SST) works with large corporations helping them to secure their Internet and global networks.

ISW Position:

Information survivability can be greatly enhanced using existing technology and at a minimum cost to large corporations (less than \$500,000).

First, we must return to the basics and do them right this time.

Second, be suspicious of the snake oil salesmen, ala Cliff Stoll's 1994 book. Anyone with something to sell probably is not going to contribute toward enhancing information security or survivability.

We can get there without PKI, IDS, and firewalls.

How to do this ! The following is The Mag 10 which will get us there.

The Mag(nificent) Ten (Ten Ways To Secure Your Network)

1	Prepare corporate network/computer security policy (Buy the British Standards Institute, BSI, Standards and plagiarize them)
2	Test your own network using ISS, CyberCop, CyberTrace, Axent Technologies, Pingware, Nmap, Sara, Satan, or Saint. Fix the findings, then retest after step 3
3	Hire third party company to do independent third party testing. Then fix the findings
4	Deploy network monitoring tool, ie: Sara, Satan, Saint, ISS, CyberCop, CyberTrace, Axent Technology, or Pingware
5	Deploy transmission and storage encryption
6	Fix static passwords, install password management program and cracking programs
7	Obtain dynamic passwords for mobile users and key personnel
8	Run war dialers. Do reverse directory lookups on hits.
9	Establish an incident response group
10	Require connecting business partners to prove, before they connect to your network, that they conducted penetration testing, and the fixes were made. Also, you can test their network at any time.

A simple solution? Yes!

Here is the reality factor. Based on my experience over the past decade, only one company is doing more than two of the ten items. This experience looked extensively at about 50 corporations and government entities. A less intensive review was done of over 1,000 different systems. Our work over the past 6 years is in the commercial world and also with government agencies. Only one company came close to doing most of the ten things. The real world is, with the exception of the one company, dozens of major multi-national companies and government organizations do two or less of the ten steps. About the only thing most companies

and government agencies do is have computer/network security policies.

The tendency is to knock the role of the end-user. The reality is all the sophisticated software, hardware, and security professionals catch almost 0% of intrusions. Fact is most problems are discovered and found by end users. Even while I was in the FBI from 1990 - 1994, investigations established system administrators/network managers had no idea they were being intruded upon. Recently, a large client had a major IDS vendor run a pilot while SST was conducting open testing and assisting in plugging holes. The IDS vendor happily told the client at the end of the pilot program, they had caught SST and produced logs of over 500 highest level IDS alarms. After checking the logs, the client found not one single alarm for the IP address being used by SST. This was open testing, where nothing was being hidden, yet there was not a single detection by the IDS.

Researchers need to understand that most academic research has little practical value to the business community. If it is not priced at \$50.00 or less per copy, industry is not going to purchase it. A good example is bio-metrics. Computer/network security does not contribute to the financial bottom line of companies. If I have a company with 40,000 nodes (typical in large corporations), why will that company buy software for each node at \$100 or higher cost per node. An example is a large company which considered Kerberizing two applications. The cost was estimated at \$1 million per application. The project was cancelled based on the expense.

Summary:

Information survivability can be greatly enhanced using existing technology and at a minimum cost to large corporations. Much of the problem out there today is directly related to not getting the basics of network security done right the first time. The solutions are simple, inexpensive, and effective.