Global Information Assurance Certification Paper

Information Systems Security: Lessons Learned

What is it, whose job is it & why should you care?

Jon Miller, *cio.ny@usa.net*
September 4, 2000

Before the explosive growth of the industry that gave us the personal computer, information systems were seen as giant behemoths residing in a place that not many people had physical or logical access to. These systems were the domain of the "high priests of data processing" as a friend would call them. Many people believed that the information in these data vaults, the "big iron" as mainframes were often called, could never be compromised. Anyway, there were those guardians of the data, the ***high priests,*** that protected access on the physical and logical planes and who "made sure" that the information remained secure. Right?

As a child growing up in the 1950's, I enjoyed many of the movies that depicted the above scenario with great dramatic license. In one movie, there were two supercomputers that became "self aware" and fought for global dominance over their human creators. In more recent times, movies such as "The Net" and "The Matrix" depict identity theft virtual reality, and the myriad of issues and resulting mayhem that can be wrought when computers are intentionally misused or when they go awry "on their own"…

As we traverse our changing computing environment, we must take stock in what these advances in technology have provided in terms of benefit as well as in terms of the potential for misuse. We all rely on computers for a great deal of our everyday lives, both at work and at home. In this paper, I'll begin to discuss what information security is in our lives, who should be doing something about it and why.

Before we can be secure in our new environment, we need to understand it. The National Information Systems Security Glossary defines Information assurance as

> ***"Information Operations (IO) that protect and defend information and information systems by ensuring their confidentiality, authentication, integrity, availability, and non-repudiation. This includes providing for restoration of information systems by incorporating protection, detection, and reaction capabilities."***[i]

By way of illustration of what, for me, was an information systems security epiphany… I had been a long-time user of the Internet, dating back to when SLIP or PPP connections to the Web were "too expensive" for me to justify. I used a dial-up account from a local ISP and worked with a shell account. From this perch, I used Elm and Pine and other

command-line character-based Unix tools to manage email and FTP, GOPHER etc… All was well in the world…

I didn't have much on my PC that I thought anyone (but me) would care about, so I thought I was pretty safe. Not many people were using the Internet 20 years ago compared to its use today. I moved up to a SLIP account and was finally able to see the Web in all it's graphical splendor… I was amazed by the amount of information available and the places I could get into with just a little bit of work.

That was then… Now, I have broadband Internet access at home through my cable provider and am surfing at "light-speed" compared to my old 1200 baud modem. I still thought I was pretty safe. My epiphany came when I installed a personal firewall and began to see the probes and scans directed at my very own computer! As the popularity of the Internet grew it also attracted many who would use it for their own gain (nefarious or not). The number of Internet users will quadruple from 36 million in 1997 to 142 million by the year 2002: an average annual growth rate of more than 50%[ii]. Safe… what was I thinking?

A similar "awakening" came to a colleague of mine who felt it was too risky to open our Agency LAN to the Internet when I told him we were already exposed to Internet based threats. He would insist I was wrong and was being paranoid… until he got an email saying "I love you", along with many others in our email directory. Not being a technical type - but a skeptic – he asked a technician what a .vbs attachment was…

Well, we all know what that "I Love You" message was all about by now, (don't we?) and have taken steps to prevent such occurrences in the future – at the cost of time and productivity. "No harm done" he said. But our email system was down for two days for cleansing and protection installation. Our vulnerability was a link with another Agency's email system (who has free access to the Internet).

Given that what I continue to think - that what I have to protect on ***my*** personal computer is not very valuable to others, and would cause me little more than an annoyance in time spent rebuilding if damaged, my personal firewall seems to suit my needs. However, I value my privacy and time, and would not take kindly to someone coming in uninvited (and undetected) to my home ***or*** my computer, even if no damage was done. If you spend any time on the Internet, you should be concerned with who's there with you… Since my own "awakening" I find myself preaching the value of information security to all who would listen.

What we know now, is that we're not inherently safe from those who would probe, scan and attack. What has to be realized is the value of your information relative to the amount of protection you are willing and able to provide. Clearly, if the information you house is worth $10,000 you will not spend $15,000 to protect it. Stop and think for a moment… what is your information worth? What would the consequences be if that information was compromised?

Imagine if your ideas were stolen and re-marketed by someone else… a denied patent, a missed market opportunity because a competitor beat you to the marketplace because they found out when you planned to announce a new product. Or, an employee who was really a plant from another organization… It has been estimated by the FBI that more than 80% of computer security breaches are inside jobs.[iii] This figure includes accidental damage as well damage done by "disgruntled employees".

It's not that we all need to become paranoid workers, but the right amount of paranoia in the carrying out of your computer and other data operations wouldn't be a bad thing. Finding that right balance of freedom in information access and the provision of security to ensure that only those with a valid need to have it are essential. The placing of too tight restrictions on data access can lead to data strangulation. This is a situation in which staff has to jump through unnecessary hoops to get the data they need to do their jobs. This practice (through unfortunate personal experience) can be more damaging to productivity than the loss it seeks to prevent.

Americans are becoming more and more worried about their personal privacy as the Internet continues to grow with the increasing amount of electronic goods and services available via this new medium. Interestingly enough, although this interest is high, not many are doing much to ensure their own safeguards.[iv]

How often have you heard the story of someone calling to get their password changed or "reactivated" because they forgot it while on vacation. I know I've heard it too often with the result being the provision of the requested information because a "name was dropped" or some peripheral personal information was gleaned prior to the request (only to make the request seem real. This method - the practice of Social Engineering - to obtain information as discussed at the recent SANS JCSC, is an extremely prevalent, non-technical way of getting information that can be used to compromise a system, and is as dangerous as a brute force attack on a password list.

As with CIO and CISO positions now taking root in the corporate landscape, there are those in government who feel that the US needs a similar position to coordinate information privacy issues. Many have seen this past year or two as a bumpy ride in the digital revolution with a bit of a growing up process going on as entities that were used to do doing business in traditional ways make the move to electronic commerce.[v]

With the increased use of electronic commerce in business as well as in government, it makes little sense to assume that someone else is taking care of the business of information security. Think of it in terms of your personal life… would you leave your car with the key in the ignition & doors open? Or your home? Assuming for a moment that there are places that you could do this without fear of theft, the community of the Internet is truly global, in that a threat can come from within a few feet, down the block, across the nation or from the other side of the world.

We all need to play a role in information safety, from those who configure and monitor Intrusion Detection Systems firewalls and routers, to those who are end-users of this

technology. The most well defended system can be brought to its knees by a casual user's pasting of a login & password above a terminal (because they always forget – or it's easier for others not to have to login on their own).

For any casual user who might be saying, "OK, but why should I care?" I simply point out that a terminal session left unattended can be an invitation to personal disaster. Let's say Alice walks away from her terminal for lunch and does not log off. Let's also say that Bob, who is angry with Alice, decides that "Alice" should sent a nasty note to the CEO… Would you want to be Alice when the CEO's office calls for an explanation?

The Computer Security Institute recently released a survey indicating that 90% of its respondents detected cyber attacks with 273 organizations reporting more than $260,000,000 in financial losses.[vi]

Clearly, if we are all to be successful in protecting our information infrastructure there must be an emphasis on proactive measures rather than relying on reactions to attacks. This means more training for staff in the areas of information security practice and awareness and the commitment of required resources by management to get the job done.

The cost of apathy in this area can be devastating. Many feel that there is a very real possibility of an "electronic Pearl Harbor", many scoff at the notion. The recent and well publicized DDoS attacks against Yahoo, CNN, eBAY Amazon.com and others portend a frightening future if history's lessons are not heeded. In his Article, DDOS, The High Cost of Apathy, Winn Schwartau talks about how these warnings were ignored continually, but in the wake of these new attacks, Congress has begun debate on how this could have happened and to explore the consequences and possibilities of future events.[vii]

So, why should ***you*** care? Only because the Nation's surface and air traffic control systems are performed with computers. Our financial systems rely on computers. Our communications systems rely on computers. Our medical systems rely on computers. In fact our nations national security depends on our information systems' infrastructure.

With the ***bad guys*** having near anonymity and remote control hacking tools with more computing power at their fingertips than most countries had two generations ago… what can we possibly do to stop them?

While on the surface it may appear that this is a daunting or even futile effort, the same tools and techniques use by those who would tear down the infrastructure can be focused and used against them to defeat them. The establishment of the National Infrastructure Protection Center by Presidential Directive, within the FBI working in concert with Computer Emergency Response Teams (CERTS) and organizations such as the SANS Institute, and the collaborative effort of all concerned with the stability of our information infrastructure is how we'll prevail.

We need to continue to train and impress upon our computer technicians, users, managers, supervisors and peers that information security is truly everybody's business.

[i] National Information Systems Security
(INFOSEC) Glossary, NSTISSI No. 4009, Aug 1997

[ii] NSA - National InfoSec Education and Training Program
http//www.nsa.gov:8080/isso/programs/nietp/index.htm

[iii] 3Com Corporation, Technical White Paper: "Enhancing Enterprise Security, An Overview of Network Security Issues & Technologies", 1999
http://www.3com.com

[iv] Rohde, Laura, The Standard, "Study: US Surfers want Guaranteed Privacy", August 21, 2000
http://www.thestandard.com/article/display/0,1151,17854,00.html

[v] Associated Press, August 21, 2000, "Lawmaker Pushes for Government Privacy Guru"
http://news.cnet.com/news/0-1005-202-2576006.html

[vi] The Computer Security Institute, "Computer Crime & Security Survey", Mar. 22,2000
http://ww.gocsi.com/prelea_00321.htm

[vii] Schwartau, Winn, "The High Cost of Apathy", March, 2000
http://www.infosecuritymag.com/march2000/news&views.htm

Additional References:

1. Palumbo, John, "Social Engineering: What is it, why is so little said about it and what can be done?" July 26, 2000 SANS Information Security Reading Room
http://wwwsans.org/infosecFAQ/social.htm

2. Conf. Material, SANS Joint Computer Security Conference Orlando FL., 03/2000
http://www.sans.org

3. Vacca, John R., "Entering Your Network" Biometric systems enhance IT Security by preventing unauthorized access", Internet Security Advisor, Jan / Feb 2000

4. Zone Labs (Personal Firewall Product Information) – Zone Alarm
http://www.zonelabs.com

5. Gibson, Steve, Shields Up Scanning Utility & FAQ - Gibson Research Corp.
http://www.grc.com

6. Federal Bureau of Investigation, National Infrastructure Protection Center
http://www.nipc.gov

Last Updated: July 20th, 2017

Upcoming Training

SANSFIRE 2017	Washington, DC	Jul 22, 2017 - Jul 29, 2017	Live Event
SANS San Antonio 2017	San Antonio, TX	Aug 06, 2017 - Aug 11, 2017	Live Event
SANS Prague 2017	Prague, Czech Republic	Aug 07, 2017 - Aug 12, 2017	Live Event
SANS Boston 2017	Boston, MA	Aug 07, 2017 - Aug 12, 2017	Live Event
SANS New York City 2017	New York City, NY	Aug 14, 2017 - Aug 19, 2017	Live Event
Community SANS Omaha SEC401*	Omaha, NE	Aug 14, 2017 - Aug 19, 2017	Community SANS
SANS Salt Lake City 2017	Salt Lake City, UT	Aug 14, 2017 - Aug 19, 2017	Live Event
SANS Virginia Beach 2017	Virginia Beach, VA	Aug 21, 2017 - Sep 01, 2017	Live Event
SANS Adelaide 2017	Adelaide, Australia	Aug 21, 2017 - Aug 26, 2017	Live Event
SANS Chicago 2017	Chicago, IL	Aug 21, 2017 - Aug 26, 2017	Live Event
Community SANS Trenton SEC401	Trenton, NJ	Aug 21, 2017 - Aug 26, 2017	Community SANS
Virginia Beach 2017 - SEC401: Security Essentials Bootcamp Style	Virginia Beach, VA	Aug 21, 2017 - Aug 26, 2017	vLive
Community SANS Pasadena SEC401 @ NASA	Pasadena, CA	Aug 23, 2017 - Aug 30, 2017	Community SANS
Mentor Session - SEC401	Minneapolis, MN	Aug 29, 2017 - Oct 10, 2017	Mentor
SANS San Francisco Fall 2017	San Francisco, CA	Sep 05, 2017 - Sep 10, 2017	Live Event
SANS Tampa - Clearwater 2017	Clearwater, FL	Sep 05, 2017 - Sep 10, 2017	Live Event
Mentor Session - SEC401	Edmonton, AB	Sep 06, 2017 - Oct 18, 2017	Mentor
SANS Network Security 2017	Las Vegas, NV	Sep 10, 2017 - Sep 17, 2017	Live Event
Community SANS Albany SEC401	Albany, NY	Sep 11, 2017 - Sep 16, 2017	Community SANS
Mentor Session - SEC401	Ventura, CA	Sep 11, 2017 - Oct 12, 2017	Mentor
Community SANS Columbia SEC401	Columbia, MD	Sep 18, 2017 - Sep 23, 2017	Community SANS
Community SANS Dallas SEC401	Dallas, TX	Sep 18, 2017 - Sep 23, 2017	Community SANS
Community SANS Boise SEC401	Boise, ID	Sep 25, 2017 - Sep 30, 2017	Community SANS
Baltimore Fall 2017 - SEC401: Security Essentials Bootcamp Style	Baltimore, MD	Sep 25, 2017 - Sep 30, 2017	vLive
Community SANS New York SEC401	New York, NY	Sep 25, 2017 - Sep 30, 2017	Community SANS
Rocky Mountain Fall 2017	Denver, CO	Sep 25, 2017 - Sep 30, 2017	Live Event
SANS London September 2017	London, United Kingdom	Sep 25, 2017 - Sep 30, 2017	Live Event
SANS Baltimore Fall 2017	Baltimore, MD	Sep 25, 2017 - Sep 30, 2017	Live Event
SANS Copenhagen 2017	Copenhagen, Denmark	Sep 25, 2017 - Sep 30, 2017	Live Event
Community SANS Sacramento SEC401	Sacramento, CA	Oct 02, 2017 - Oct 07, 2017	Community SANS
SANS DFIR Prague 2017	Prague, Czech Republic	Oct 02, 2017 - Oct 08, 2017	Live Event