GIAC
CERTIFICATIONS

Global Information Assurance Certification Paper

Copyright SANS Institute
Author Retains Full Rights

This paper is taken from the GIAC directory of certified professionals. Reposting is not permited without express written permission.

Interested in learning more?

Check out the list of upcoming events offering
"Security Essentials: Network, Endpoint, and Cloud (Security 401)"
at http://www.giac.org/registration/gsec

Information Assurance, the Second Job That Must Become Second Nature
Barbara Catenazzo
20 December 2000

As part of an organization's Information Assurance Program, I know that it is necessary for each of us to protect the information we're responsible for at whatever level we're responsible for it. It's my job to get the word out. Raise the awareness that our data, systems, and networks must be protected; let everyone know the implications of not using Information Assurance techniques and getting them implemented. Force feeding anti-virus updates and software patches is just not enough. The unaware user will still open that questionable e-mail or respond to that 'socially engineered' 'innocent' question.

We are repeatedly told that Information Assurance is everyone's job, that our data and systems are only as secure as the weakest link in our program, but, Information Assurance is a second job for most users and capturing their interest in the subject is a challenge. Security in any way, shape, or form makes their 'real' job harder. It cramps their style, slows them down, and may even bring them to a complete halt. The fact that without it, they could still be slowed down, stopped, or even lose everything, is sometimes a very hard sell when things are going well and they are up against suspense's and/or that bottom line. It's the other guy that's going to be affected by the next attack.

Information Assurance personnel may use Information Warfare's battle cries of 'Remember Melissa' or 'Remember the I Love You Virus' to catch a user's attention. To get them to use Information Assurance techniques, awareness must be raised and the implications of not using those techniques understood.

Raising awareness has been made easier by news stories that broadcast the affects of viruses, denial of service attacks, and the hacking into the computers and computer systems of highly visible organizations and government agencies. Also consider the stories about the individuals who have become victims just by making a purchase on the Internet from their home computer. But it's not enough. Users won't remember when an intriguing e-mail arrives that peaks their curiosity and they fall for the assault on their data, system, or network, to say nothing of the next precocious kid, disgruntled employee, or obnoxious hacker or cracker who just wants to see how far they can get or really cause damage.

Raising awareness has to change the mindset to one that questions absolutely anything out of the ordinary, no matter how small or seemingly harmless. Information Assurance training that includes the signs of trouble gives users an edge. Absorption in their 'real job' won't keep the flag from being raised in their mind when something isn't quite right. Then, even more importantly, they will take the time to report it and allow the network and information Assurance personnel to follow up.

© SANS Institute 2000 - 2005 Author retains full rights.

How do I raise everyone's Information Assurance awareness, including, incidentally, that of the boss and the computer/network professionals? Anyone in the organization who uses a computer, stand-alone, networked, using the backbone, or connected to the Internet, needs to be aware of what is considered acceptable and secure use.

I've been told that security training is boring. Well, it can be, especially if the same presentations and methods of presentation are used repeatedly, but it doesn't have to be. In Information Assurance training, the same points need to be stressed, the ones that get us in trouble often and easily: poor passwords, protecting passwords, access, using screen savers, password protecting screen savers, don't open e-mail attachments from unknown sources, and don't pass on virus hoax information or chain letters. Take advantage of your organizations intranet, web site or local area network (LAN) to send out a 'Tip of the Day' or Week, something short, sweet, and hopefully catchy to make people take notice. Games and contests can peak some interest or request users to submit their own thoughts. Comb the Web for training material, videos, articles, posters, thoughts, and ideas. You'll find mounds of it, but sift through to find what will suit your needs. Will any of it keep the users from making the same old mistakes? Maybe not, but the point is to keep them aware of what they can do to protect their data, systems, and network.

Keeping training materials up to date is important. Use what is relevant to your organization. Keep it in tune with your organization's Security Policy and the User Agreement or whatever you use to give a user authorization to use the computers and/or network. Since this policy and agreement spell out what the organization's Information Assurance security team feels is important and every user should comply with, you want to keep them aware of what is expected and allowed, as well as what is not allowed.

We are already aware of the great source of information provided by SANS Institute Online at www.sans.org/newlook/home.htm, the SANS Global Incident Analysis Center at www.sans.org/giac.htm, and the SANS Information Security Reading Room at www.sans.org/infosecfaq/index.htm.

The Smart Computing in Plain English magazine and their website at www.smartcomputing.com offer articles on many security related subjects, information for all the users, at home and work. You'll even find some information to pass on the organizations computer, network, and Information Assurance pros.

Another good source of Information Assurance information and training material is the Defense Information Systems Agency (DISA). Their information assurance site at www.disa.mil/infosec/iaweb/default.html has links to the many CERT sites with their most current information. Besides Information Assurance Training, this site offers links to PKI, virus info, and tools for your pros.

Many schools and universities offer various levels of information assurance

© SANS Institute 2000 - 2005 Author retains full rights.

training and development. The site: securityinfo.berkeley.edu offers a wide range of topics under security and PC support.

The commercial site www.zdnet.com also offers various levels of information assurance training subjects along with daily news features to keep you up to date.

I'd like to have an organization really enthusiastic about their information assurance responsibilities, but I'll accept an organization that keeps their information, systems, and networks secure.

References:

Air Force Information Assurance Course Information Systems User

Air Force Information Assurance Course Information Systems Administrators

Air Force Instruction (AFI) 33-119. "Electronic Mail (E-mail) Management and Use." 01 March 1999

AFI 33-129. "Transmission of Information Via the Internet." 01 August 1999

AFI 33-202. "Computer Security." 22 June 2000

AFI 33-204. "Information Protection Security Awareness, Training, and Edurcation (SATE) Program." 26 April 1999

AFI 33-223. "Identification and Authentication." 01 June 1998

"Computer Security Framework and Principles." 25 March 1998 Version 0.3. URL: http://securityinfo.berkeley.edu/reports/framework/framework.html (4 December 2000)

"Computer User's Guide to the Protection of Information." URL: http://security.isu.edu/isl/usrguide.html (1 December 2000)

Dorsey, Michael A. "Security training enforces information superhighway." 23 January 1998. URL: www.af.mil/news/Jan1998/n19980123_980095.html (1 December 2000)

"FSS' security awareness program see also this page… URL: http://www.fss.umn.edu/aware.htm (1 December 2000)

Gompert, David C. "Keeping Information Warfare in Perspective." URL: http://www.rand.org/publications/RRR/RRR.FALL95.cyber/perspective.html

Goslar, Martin. "Stumbling toward protection, finding few answers." Special to ZDNet.

© SANS Institute 2000 - 2005, Author retains full rights.

21 September 2000. URL:
http://www.zdnet.com/enterprise/stories/main/0,10228,2630824,00.html (6 December 2000

"Information Security Awareness Education." URL:
http://falcon.jmu.edu/~dixonlm/index2.htm (1 December 2000)

"Practice Brief: Information Security: A Checklist for Healthcare Professionals (Updated)." URL: http://www.ahima.org/journal/pb/00.01.html (1 December 2000)

© SANS Institute 2000 - 2005, Author retains full rights.