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 Bootcamp Style (Security 401)"
at http://www.giac.org/registration/gsec

# TOWARD GLOBAL SECURITY

**Paul Tremer**

**Version 1.2e**

**July 20, 2001**

© SANS Institute 2000 - 2005 Author retains full rights.

© SANS Institute 2000 - 2005 Author retains full rights.

Tracing the roots of information security back centuries ago to the times and practices of Greek and Roman cryptographers, Julius Caesar, as established in the Kama Sutra (fourth century AD), by Arab scholars (seventh century AD), during the European Renaissance, the trial and eventual execution of Mary, Queen of Scots in the 1500's, critical secret and decoded warfare/political communications throughout history, and to more modern day mathematicians, engineers, scientists, educators, technologists, curious cybergeeks and hackers,[1] methods to secure and transmit confidential communications among peoples and nations around the world throughout time have evolved or revolved to the point of practice today.

Once again, we are at the crossroads. Whether humanity will proceed to achieve ever greater global accomplishments with a logical balance of secure information and technology development and transfer, or instead perish, will depend on decisions, defenses, knowledge and practices established today and in the near and foreseeable future. Countries, leaders, governments, corporations, educators, and technologically informed and savvy individuals around the globe must capture the power of information, ideas, and new technologies through secure ways, means, policies, and practices. Obtaining good and intended outcomes or deriving optimal solutions must prevail over evil acts. The world is developing and interacting at an exponentially expanding and rapid pace, and this process must occur through secure and protected methods to ensure the best outcome possible. Without identifying and understanding the ever-changing risks at stake, the challenges of acceptable information and technological security balanced against that risk, and the harmful consequences of certain individuals, foreign governments, and rival corporate competitors committing and conspiring to commit evil actions worldwide, current and future life and progress is threatened. A persistent commitment to balance security needs against risk must be the course of action taken globally. "The future is at once unpredictable and predictable. Information warfare will happen. It will happen many times. When it will happen, how severe the attacks will be, and who will launch the first major attacks are not predictable. The threat of information warfare is like the threat of nuclear war. There will always be hope that it does not occur, but the only logical defense is to be prepared…economies can be laid waste in information warfare just as the planet could be turned into a wasteland after nuclear attack. Once again the United States and allied nations of Europe and Asia have no choice at all. They must once again become the defenders of peace and freedom."[2]

To achieve maximum security and progress successfully, those individuals developing and promoting secure policies, procedures, standards and guidelines must be proactive, not reactive. We must think and act like a hacker. We must realize that humans have limitations, but also intentions – some good, others not so good, but instead bad. We must learn from the past to protect current and future endeavors. We must weigh costs against benefits. We must balance security against acceptable risk and opportunity levels. It is important to realize that many of today's attacks against and misuse of information assets are committed by insiders to an organization, rather than from outsiders. According to the Computer Security Institute's (CSI) 2001 Computer Crime and Security Survey, "ninety-one percent [of respondents] detected

© SANS Institute 2000 - 2005 Author retains full rights.

employee abuse of Internet access privileges (for example, downloading pornography or pirated software, or inappropriate use of e-mail systems). Forty percent of respondents detected system penetration from the outside."[3] As such, organizations must manage security based on strong policies. However, up-to-date policies are only one layer of defense. Individuals must be informed, educated, and equipped with the right sets of tools to effect positive protection of their information systems. Mapping policies to procedures and technologies provided by the necessary tools can establish a more secure infrastructure in which to operate and advance. As such a methodology will reveal, however, is the fact that security is not a product or set of products, but rather a process. Securing an enterprise is a multi-layer approach that demands persistence, balance, standards and commitment to be adequate, current and effective.

A firewall is an integral component to this defense mechanism and strategic process associated with a network security infrastructure. A firewall serves as a buffer or barrier between a trusted (and presumably secure) network and an untrusted (and, therefore, potentially insecure) network. The basic functions of a firewall include: packet filtering (set of rules to examine header of each packet encountered to determine whether packet should proceed or be stopped), stateful packet inspections (to track "state" of specific transmission to identify abnormal sequences which might represent a threat), application-level proxies (packet inspection at the application level through a "proxy" to determine whether the behavior of the packet is acceptable), and circuit-level proxies (SOCKS) "works at the session level, but like application-level proxies, SOCKS can also hide internal network addresses from outsiders because it sets up two distinct sessions – one to the remote server and another to the client. The SOCKS server, then, relays data between the two sessions. Since only the SOCKS server knows the precise correlation between the two, insiders are insulated from certain types of network-based attacks." Although a firewall limits exposure to certain types of attacks it, too, is an important but only single component of a security system. A firewall cannot protect against an authorized user's malicious behavior; protect against viruses, trojan horse programs, and new threats; protect against bad or nonexistent policies; and protect against human errors (through incorrect filter setup, etc.).[4]

Other methods to secure an inter-networked enterprise or to protect personal privacy require eliminating single points of failure to ensure confidentiality, integrity, and availability of data. Solutions that include personal firewalls (e.g. BlackICE Defender or ZoneAlarm) can prevent intruders from obtaining confidential credit card numbers, financial, medical, and other personal data. Users of the public Internet (or Intranets, Extranets, VPN's) must remain vigilant at all times and ensure that security mechanisms are in place to protect information that they provide online. Certain sensitive and personal information or photographs may be used for malicious social engineering goals to retrieve passwords and other data that can be identified (or inferred) as a consequence. Online users should guard against downloading any e-mail attachments that are not trusted or from trusted senders. Such attachments may contain harmful viruses and spyware (e.g. SpectorSoft, WhoWhatWhere). Individuals

© SANS Institute 2000 - 2005 Author retains full rights.

should establish "dummy" e-mail accounts (e.g. Hotmail, Yahoo, etc.) and use these e-mail addresses when completing online personal profiles, posting messages in newsgroups, and providing e-mail addresses to unknown/untrusted individuals. If this "dummy" e-mail account is compromised, the consequences may not be so severe as if the attack were against a primary e-mail account. Also, unwanted "cookies" should be disabled from your browser or rejected (through preference settings or via software like "Cookie Crusher") to prevent personal information and browsing activities from being collected and misused by external sources. Consider "opting out" of allowing external websites from sharing your personal data with third parties. This can be accomplished by reviewing a website's Privacy Statement and indicating your preferences accordingly. Also, sensitive data should be encrypted and digitally signed when transmitted via the Internet to prevent unauthorized access or disclosure of confidential information. Due to the fact that websites maintain a record of individual visits to the site and may obtain personal identification through such transactions, online users may benefit from using an anonymizer (www.anonymizer.com) to prevent the disclosure of private credentials. Another proactive measure is to clear your memory cache or "history" after surfing the Internet to hide the digital footprint (or record) of sites you have visited. This can be accomplished by deleting this information trail/log from your browser's preferences.[5]

Because electronic security is so vital to protect personal, corporate, government, and institutional assets, solutions are wide-ranging and ever-changing. Consequently, individuals must not be misinformed or rely on simple, "one-size-fits-all" safeguards. Common information security misconceptions[6] often include the notions that:

1) A firewall is sufficient to secure my network or website.
2) I can patch my OS (operating systems) and applications when I get around to it.
3) I don't have to worry about physical security; that's the building administrator's job.
4) I back-up data to tape or on the network so we're covered in the event of data loss.
5) Remote access is secure because I use a virtual private network (VPN) with user names and passwords [authentication mechanisms].

Because information security requires multi-layered solutions, the goal is to make your systems more difficult to penetrate and cause attackers to focus on easier targets. A comprehensive defense strategy should be based upon the value of assets that must be protected, the consequences of loss of confidentiality or operational capability, vulnerabilities that could be exploited to bring about the losses, existing threats that could exploit the vulnerabilities, the likelihood that a threat might occur, and the availability and appropriateness of options and resources to address risks and concerns.

To most effectively counter external threats, Carnegie Mellon University's Software Engineering Institute (Networked Systems Survivability [NSS] Program) has

© SANS Institute 2000 - 2005 Author retains full rights.

established the OCTAVE method that should be incorporated into an overall defensive security strategy and policy. The OCTAVE method comprises "three phases that provides a systematic, context-driven approach to managing information security risks, and enables an organization to assemble a comprehensive picture of their information security needs. Phase 1 identifies information assets and their values, as well as threats to those assets and the security requirements to protect them. Phase 2 examines the information assets of the organization in relation to the information infrastructure components to identify those components that are high priority. During this phase, the organization identifies the high-priority information infrastructure components, missing policies and practices, and vulnerabilities. Phase 3 builds upon the information captured during Phases 1 and 2. Risks are identified by analyzing the assets, threats, and vulnerabilities. Estimates of impact and probability of the risks are made, and the risks are then prioritized, ultimately resulting in the development of a protection strategy and a comprehensive, enterprise-wide plan for managing security risks."[7]

Armed with this comprehensive analysis, information management, and strategy development, the common security misconceptions can be methodically discounted and eliminated. In its place, some or all of the following processes should be considered and integrated into a proactive, defensive security and risk management program:

1) Develop and maintain comprehensive security policies, standards, procedures, guidelines documentation (e.g. remote access, e-mail, etc.).
2) Establish physical & environmental protection.[8]
3) Separation of duties.[9]
4) Internal and external vulnerability assessments (NetRecon, Nessus).
5) Host and network-based Intrusion Detection (HIDS/NIDS) of system and network components (Intruder Alert, NetProwler, ISS RealSecure, SecureNet, Snort/Acid, etc.).
6) Systematic log analysis (firewall, syslogs, etc.).
7) Regular auditing and policy adherence monitoring (Enterprise Security Manager, etc.).
8) PKI (Public Key Infrastructure) encryption, digital certificates/signatures.
9) Two- (or multi-) factor authentication (one time strong passwords, smart tokens, biometrics).
10) Harden operating systems (disable unnecessary services, user IDs, and privileges).
11) Install software updates and patches, as necessary.
12) Install updated anti-virus software.
13) Establish back-up and recovery procedures (develop security emergency response team and incident handling plan).
14) Perform regular checks for new security alerts and advisories

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

© SANS Institute 2000 - 2005 Author retains full rights.

(CERT/CC, SANS, etc.).[10]
15) Conduct ongoing security training and awareness programs (including ethics).[11]
16) Track current security legislation.
17) Remain vigilant to stay ahead of hacker exploits.

By taking a broad, comprehensive, and complete view of information security and protecting your assets from many fronts to guard against any type of attack, unintended malicious consequences will be significantly mitigated, if not eliminated entirely.

Also, leading the way to develop future security policies and regulations, President George W. Bush has recently proposed the establishment of a US Federal Cyber Security Board, proposed to begin operations on October 1, 2001. This board will be comprised of 21 senior officials from all major federal agencies (including the Departments of State, Defense, Justice, Energy, and Treasury, in addition to the National Security Agency, CIA and FBI), replacing the previous administration's plan where only 11 agencies were represented. This committee will be charged with establishing the necessary national safeguards to prevent a "Digital Pearl Harbor" by a terrorist/rogue nation attack which could have a devastating impact on information systems, electrical grids, and other critical infrastructure (defense facilities, financial institutions/ATM networks, air traffic control/transportation system, national power/communication system). However, exactly how the board will enforce standards is currently being debated vigorously. Some opponents of the new board argue against a "big brother" approach to protecting national information systems against foreign and domestic threats. Other critics oppose the abolishment of a single, high-profile security chief to be replaced by a bureaucratic board that will report to the National Security Advisor. However, the new plan will empower more agencies to participate in key decision making security matters that will be created through consensus.[12]

With ever-expanding international trade and data transfers taking place vis-à-vis complex global (including wireless) networks, the United States and our allies must protect our economic and government interests through strategic and aggressive means to prevent cataclysmic events from occurring. By implementing and enforcing strong, multi-layered security policies and processes, constructive progress can and will defeat global threats and malicious activities today and throughout time.

[T]he reason that it is so hard to secure a complex system like the Internet is, basically, because it's a complex system. Systems are hard to secure, and complex systems are that much more operose.[13] However, we must develop and deploy the right defenses now and in the future. For as Martin Luther King, Jr. once proclaimed, "we have come this place to remind ourselves of the fierce urgency of now." And by implementing proactive, comprehensive security processes, let us take what steps are necessary to prevent individual and organizational incidents that would result in comparative devastation as to that which was the fate of Mary, Queen of Scots centuries ago.

© SANS Institute 2000 - 2005 Author retains full rights.

And if we are to contribute to the world's future well-being according to the views and spirit of the great industrialist, Andrew Carnegie, the planet would survive and thrive in ways we cannot even begin to imagine. "No man becomes rich unless he [or she] enriches others. The average person puts only 25% of his [or her] energy and ability into his [or her] work. The world takes off its hat to those who put in more than 50% of their capacity, and stands on its head for those few and far between souls who devote 100%." We must give more!

## REFERENCES


1 Singh, Simon, "The Code Book – The Evolution of Secrecy from Mary, Queen of Scots to Quantum Cryptography", 1999.

2 Erbschloe, Michael, "Information Warfare: How to Survive Cyber Attacks", 2001, p. 287.

3 Computer Security Institute (CSI), "2001 Computer Crime and Security Survey", http://www.gocsi.com/prelea_000321.htm

4 Crume, Jeff, "Inside Internet Security: What Hackers Don't Want You to Know", 2000, pp. 72-82.

5 Cohen, Adam, "Internet Insecurity", Time Magazine, July 2, 2001, pp. 49-50.

6 Mourer, Darrin, "5 Common Information Security Misconceptions", Business Security Advisor, July/August 2001, pp. 30-31.

7 Allen, Julia, Alberts, Christopher, Behrens, Sandi, Laswell, Barbara, and Wilson, William, "Improving the Security of Networked Systems" (White Paper), Carnegie Mellon University – Software Engineering Institute, Networked Systems Survivability Program, http://www.stsc.hill.af.mil/crosstalk/2000/oct/allen.asp

8 Chirillo, John, "Hack Attacks Denied: A Complete Guide To Network Lockdown", 2001, pp. 352-353.

9 Anderson, Ross, "Security Engineering – A Guide to Building Dependable Distributed Systems", 2001, pp. 189-191.

10 Security Alerts & Advisories, http://www.cert.org, http://www.sans.org (http://www.incidents.org), http://www.infragard.net, http://www.nipc.gov/warnings/warnings.htm

11 Nichols, Randall K., Ryan, Daniel J., Ryan, Julie J.C.H., "Defending Your Digital


© SANS Institute 2000 - 2005 Author retains full rights.

Assets Against Hackers, Crackers, Spies & Thieves, 'Before the Attack: Protect and Detect'", 2000, Chapter 13, pp. 414-418.

12 http://www.cnn.com/2001/TECH/industry/07/18/technology.security.ap/index.html

13 Schneier, Bruce, "Secrets & Lies: Digital Security in a Networked World", 2000, p. 7.

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

Last Updated: May 28th, 2017

# Upcoming Training


| | | | |
|---|---|---|---|
| SANS Stockholm 2017 | Stockholm, Sweden | May 29, 2017 - Jun 03, 2017 | Live Event |
| SANS San Francisco Summer 2017 | San Francisco, CA | Jun 05, 2017 - Jun 10, 2017 | Live Event |
| SANS Houston 2017 | Houston, TX | Jun 05, 2017 - Jun 10, 2017 | Live Event |
| Security Operations Center Summit & Training | Washington, DC | Jun 05, 2017 - Jun 12, 2017 | Live Event |
| Community SANS Ottawa SEC401 | Ottawa, ON | Jun 05, 2017 - Jun 10, 2017 | Community SANS |
| SANS Charlotte 2017 | Charlotte, NC | Jun 12, 2017 - Jun 17, 2017 | Live Event |
| SANS Rocky Mountain 2017 - SEC401: Security Essentials Bootcamp Style | Denver, CO | Jun 12, 2017 - Jun 17, 2017 | vLive |
| Community SANS Portland SEC401 | Portland, OR | Jun 12, 2017 - Jun 17, 2017 | Community SANS |
| SANS Secure Europe 2017 | Amsterdam, Netherlands | Jun 12, 2017 - Jun 20, 2017 | Live Event |
| SANS Rocky Mountain 2017 | Denver, CO | Jun 12, 2017 - Jun 17, 2017 | Live Event |
| SANS Minneapolis 2017 | Minneapolis, MN | Jun 19, 2017 - Jun 24, 2017 | Live Event |
| SANS Columbia, MD 2017 | Columbia, MD | Jun 26, 2017 - Jul 01, 2017 | Live Event |
| SANS Cyber Defence Canberra 2017 | Canberra, Australia | Jun 26, 2017 - Jul 08, 2017 | Live Event |
| SANS Paris 2017 | Paris, France | Jun 26, 2017 - Jul 01, 2017 | Live Event |
| SANS London July 2017 | London, United Kingdom | Jul 03, 2017 - Jul 08, 2017 | Live Event |
| Cyber Defence Japan 2017 | Tokyo, Japan | Jul 05, 2017 - Jul 15, 2017 | Live Event |
| SANS Los Angeles - Long Beach 2017 | Long Beach, CA | Jul 10, 2017 - Jul 15, 2017 | Live Event |
| Community SANS Phoenix SEC401 | Phoenix, AZ | Jul 10, 2017 - Jul 15, 2017 | Community SANS |
| SANS Munich Summer 2017 | Munich, Germany | Jul 10, 2017 - Jul 15, 2017 | Live Event |
| SANS Cyber Defence Singapore 2017 | Singapore, Singapore | Jul 10, 2017 - Jul 15, 2017 | Live Event |
| Community SANS Minneapolis SEC401 | Minneapolis, MN | Jul 10, 2017 - Jul 15, 2017 | Community SANS |
| Mentor Session - SEC401 | Macon, GA | Jul 12, 2017 - Aug 23, 2017 | Mentor |
| Mentor Session - SEC401 | Ventura, CA | Jul 12, 2017 - Sep 13, 2017 | Mentor |
| Community SANS Atlanta SEC401 | Atlanta, GA | Jul 17, 2017 - Jul 22, 2017 | Community SANS |
| Community SANS Colorado Springs SEC401 | Colorado Springs, CO | Jul 17, 2017 - Jul 22, 2017 | Community SANS |
| SANSFIRE 2017 | Washington, DC | Jul 22, 2017 - Jul 29, 2017 | Live Event |
| Community SANS Charleston SEC401 | Charleston, SC | Jul 24, 2017 - Jul 29, 2017 | Community SANS |
| SANSFIRE 2017 - SEC401: Security Essentials Bootcamp Style | Washington, DC | Jul 24, 2017 - Jul 29, 2017 | vLive |
| Community SANS Fort Lauderdale SEC401 | Fort Lauderdale, FL | Jul 31, 2017 - Aug 05, 2017 | Community SANS |
| SANS San Antonio 2017 | San Antonio, TX | Aug 06, 2017 - Aug 11, 2017 | Live Event |
| SANS Boston 2017 | Boston, MA | Aug 07, 2017 - Aug 12, 2017 | Live Event |