

Rating 1-3	Rating 4-5	Rating 6-7	Rating 8-10				
Threat	Color Code	2004 Rating	2006 Rating	2008 Rating	Detection Difficulty	Current Existence	Current Usage
Worm/Virus		9	7	6	3	9	8
Phishing/Whaling		1	4	5	5	7	6
Social Networking		-	2	6	9	9	8
Inappropriate Posting		8	6	4	7	5	5
Inappropriate Forwarding		5	6	8	7	6	7
Social Engineering		7	7	7	3	4	6
External Hacker		9	7	8	8	8	5
Tailgating		8	7	7	3	4	6
Account Sharing		8	6	5	8	7	6
Credential Documentation		7	6	6	7	6	7
Unauthorized Software		6	7	9	5	6	9
Defeating Protections		5	5	6	5	3	4
Unreliable De-Provisioning		8	7	6	7	4	4
Untrained / Disgruntled Personnel		9	9	9	9	2	2
Vulnerability	Color Code	2004 Rating	2006 Rating	2008 Rating	Remediation Difficulty	Current Existence	Current Exploitation
Security Un-Awareness		8	7	6	5	5	9
Security Training		8	7	6	5	5	7
Incomplete Security Policies		7	6	5	6	5	9
Undefined Security Procedures		9	7	5	8	6	6
Insecure Configuration		9	7	6	6	6	8
Insecure Applications		3	5	8	9	10	5
Un-applied Updates		9	7	6	7	6	6
Untrained / Disgruntled Personnel		8	7	6	8	2	6
Incomplete Logging		4	6	9	7	9	7
Ineffective Monitoring		8	8	8	8	8	7
Ineffective Auditing		5	7	9	8	8	7



Threat Definitions

Logic Bomb	A logic bomb is a piece of code intentionally inserted into a software system that will set off a malicious function when specified conditions are met. For example, a programmer may hide a piece of code that starts deleting files (such as the salary database), should they ever leave the company.
Computer Virus	Malicious software that attaches itself to other software. For example, a patched software application in which the patch's algorithm is designed to implement the same patch on other applications, thereby replicating itself.
Rabbit	This is a form of computer virus or worm that replicates without bound, thus exhausting available computing resources, but it does not spread to other systems.
Bacterium	A form of computer virus designed to attach itself to the OS in particular (rather than any application in general) and exhaust computer resources, especially CPU cycles.
Spoofing	In the context of network security, a spoofing attack is a situation in which one person or program successfully masquerades as another by falsifying data and thereby gaining an illegitimate advantage
Sequential Scanning	In the sequential scan, worms in an infected host will select randomly an IP address in an effort to identify system vulnerabilities.
Dictionary Scanning	This type of attack exploits a buffer overflow vulnerability in targeted client software through injection of malicious content from a custom-built hostile service
Digital Snooping	This is the electronic monitoring of digital networks to uncover passwords or other data. It has grown with the rapid adoption of wireless lans.
Spamming (DoS, DDoS)	This is the intentional overloading a system with incoming messages or other traffic to cause system crashes.
Tunneling	This refers to any digital attack that attempts to get "under" a security system by accessing very low level system functions (e.g., device drivers, OS kernels).
Scavenging	This is associated with automated scanning of large quantities of unprotected data (discarded media or online "finger" type commands) to obtain clues as to how to achieve access.
Counterfeit Equipment	Counterfeit hardware refers to an imitation that is made usually with the intent to deceptively represent its content or origins and with unknown integrity.
Counterfeit Software	Counterfeit software refers to an imitation that is made usually with the intent to deceptively represent its content or origins and with unknown integrity.
Software Malfunction	This refers to software behavior that is in conflict with intended function or operation that pose a security risk.



Threat Definitions, continued

BotNets	BotNet is a collection of software robots, or bots, that run autonomously and automatically. The term is often associated with malicious software, but it can also refer to the network of computers using distributed computing software.
Trap Door/Back Door	Software left available after code delivery for the purpose of future access.
TEDs/EPFCs/EMP (non-Nuclear)	These devices generate electromagnetic radiation from an explosion or an intensely fluctuating magnetic field caused by Compton-recoil electrons and photoelectrons from photons scattered in the materials of the electronic or explosive device or in a surrounding medium.
Insider Threat	An insider threat comes from an individual with malicious intent. Typically, it is an employee or officer of a business, institution, or agency. The term can also apply to an outside person who poses as an employee or officer by obtaining false credentials.
Trojan Horse	A Trojan horse, also known as a trojan, is malware that appears to perform a desirable function but in fact performs undisclosed malicious functions. Therefore, a computer worm or virus may be a Trojan horse.

The Threats We Face

Virus / Worm	A virus is malicious software that attaches itself to other software. Viruses are typically delivered through email or instant messaging attachments and downloaded files. A worm is similar to a virus but also attempts to infect other computers as well. Never open an email attachment unless it is from a known, trusted source.
Phishing / Whaling	Phishing is the act of sending an email designed to look like it has come from a trusted organization. Typical phishing emails ask the user to access a malicious website that purports to provide account verification or other services. Always use "out of band" communication methods (phone, fax, postal mail) to validate the source of any such emails.
Social Networking	Social networking sites provide an excellent opportunity for someone with malicious intent to perform extensive research about both personal and professional aspects of their users. This information can be very powerful when combined with Social Engineering techniques.
Inappropriate Posting	Never post job, job function, process, financial, or information technology details about you, other employees, or our organization on the Internet.
Inappropriate Forwarding	Never forward emails containing any job, job function, process, financial, or information technology details about you, other employees, or our organization on the Internet.



The Threats We Face, continued

Social Engineering	Social engineering is the process of defeating technical security measures by deceiving employees to reveal information including: username, account name, password, application names, server names, facility names, employee names, reporting relationships, technologies, procedure details, etc. Sophisticated social engineers never gather more than one piece of information from any one individual until finally building a highly plausible, detailed, and compelling story. Never provide this information over the phone unless the identity of the caller is known for certain.
External Hacker	External hackers typically consist of either "Script-kiddies" or elites. For an organization that has good security awareness, good security controls, and a good security program script-kiddies are an annoyance that must be addressed and elites will validate just how good the overall security is. For organizations that don't have awareness, controls, or a program in place script-kiddies can be a significant risk.
Tailgating	Always be aware of individuals that may be trying to access restricted areas in your facility by "hanging out" around entrances / exits and following you into the facility. This especially trouble-some in facilities that have external designated smoking areas.
Account Sharing	For some applications a common account may be required, however in the absence of this requirement, employees should never ad-hoc share accounts amongst themselves. This defeats the ability to properly audit activity that has occurred.
Credential Documentation	Never write down username, account, or password information.
Unauthorized Software	The proliferation on the world-wide-web of websites using "plug-ins" to deliver applications or content has de-sensitized employees to the extreme danger involved in installing ANY unauthorized, unapproved software on company owned computers.
Defeating Protections	Employees that have been given power user or administrator access to the computers they use can in some cases disable protections that are supposed to be in place including anti-virus and firewalls. This is typically done in an attempt to make the machine run faster.
Unreliable De-Provisioning	Leaving authorizations and account credentials in effect after an employee has quit, been terminated or changing job duties.
Untrained / Disgruntled Personnel	Employees constitute the largest threat to any companies information security. They have the required access and may be performing duties for which they have not been properly trained, or may act out in an attempt to address a perceived wrong.

