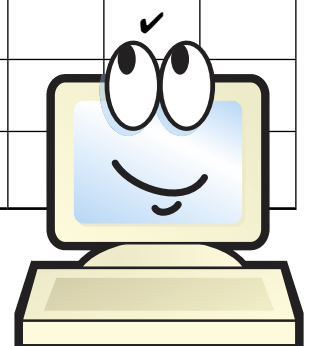




Security Awareness Program Metrics Internal User Behaviors <i>Examples to be tailored should be based on goals and then questions.</i>	G • B • U*	Survey	Observation	Help Desk Incid. Rpts	Manual Tests or Audits	Software (Automated)
% of users recognizing a security event scenario	G	✓				
% of users susceptible to social engineering (compare mid-week at mid-day to Friday afternoon)	B				✓	
% of users revealing their password when tested	B				✓	
% of users activating a "test virus"	B				✓	
% of security incidents having human behavior as a major factor / involving behaviors covered in awareness materials	BU			✓		
Storage of unauthorized file content on desktop or network resources, such as audio, video, or other multimedia files	B					✓
Number of attempts to access inappropriate/blocked Web sites	B					✓
Non-public information found in dumpsters outside of facilities	B		✓			
% of systems having unapproved software installed	BU				✓	✓
% of systems having unapproved hardware installed	B				✓	✓
% of e-mails (random sample) with inappropriate content	B				✓	
% of passwords visible or in common locations (e.g., under lamp)	B		✓			
% of PCs logged on and unattended	B		✓			
% of laptops, portable devices/media, sensitive data unsecured	B		✓			
% of laptops, portable devices/media stolen (office/travel)	B			✓		
Number of attempts to use unauthorized resources, e.g., VPN	B					✓
% of e-mails sent via Internet containing non-public/sensitive data that are not encrypted	B					
% of users wearing badges with picture facing out	G		✓			
% of monitors positioned to be easily seen from hallways, doors, or windows (especially on the ground floor)	B		✓			



continued on page 2

continued from page 1

Security Awareness Program Metrics Internal User Behaviors <i>Examples to be tailored should be based on goals and then questions.</i>	G • B • U*	Survey	Observation	Help Desk Incid. Rpts	Manual Tests or Audits	Software (Automated)
% of users who challenge unknown visitor with no access badge	G		✓	✓		
% of users who open a test e-mail with a questionable subject	B				✓	✓
% of users activating a "test virus"	B				✓	✓
% of users who click a link in a test e-mail (instead of typing the URL into their browsers)	B				✓	✓
% of users responding to a test e-mail via an "unsubscribe" link	B				✓	✓
% of crackable user passwords	B				✓	✓
% of user systems having spyware or malware installed	B				✓	✓
Number of incidents of unauthorized use of administrator privileges	U			✓	✓	
% of users sending Internet e-mail to multiple recipients who do not use the BCC field	B				✓	
% who have actively acknowledged policies / security responsibilities	G					✓
Number of major findings from internal & external security audits	B				✓	
% viewing optional security materials in online courses	G					✓
% participating in contests, suggestion programs, bonus questions	G					✓

* **G • B • U** = Good, Bad, or Ugly

G: Good behavior complies with the 'letter of the law' or better, the 'spirit of the law,' e.g., not releasing non-public information inappropriately, discovering and reporting a security vulnerability.

B: Bad behavior includes **naive mistakes** or **dangerous tinkering** – e.g., sharing a password, deploying a wireless network gateway that allows non-company personnel to use the company's network, setting up a packet spoofing application to test one's programming ability; or setting up a network monitoring scanner on one's PC.

U: Ugly behavior consists of **detrimental misuse** or **intentional destruction** – e.g., someone builds a special script that disabled other users' terminal sessions, forges e-mail header information to make it look like someone else sent a message, uses a file decryption program to discover the contents of a file containing trade secrets, or intentionally introduces a Trojan horse program into the network.

(Behavior categories inspired by "Analysis of End User Security Behaviors" – by Jeffrey M. Stanton, Kathryn R. Stam, Paul Mastrangelo, and Jeffrey Jolton, July 12, 2004.)



Security Awareness Program Metrics
End User Knowledge and Perceptions of IT Security
(Could be tailored for use as a Baseline Survey)



% of users who know where to find policies and standards
% who have read specific policies
% who believe that better security will improve the organization's ability to perform its mission – or will result in a competitive advantage
% who believe that reducing spam starts with better security practices (e.g., the more secure the computing environment, the more difficult it is for an unauthorized person to send spam)
% who believe security policies do not significantly interfere with their ability to get the job done
% who believe that security policies are enforced
% who know, or know of, an individual who has been disciplined for a security breach
% who have seen a password visible in their office or work area (e.g., in the last 6 months)
% who have been asked to share their passwords with a coworker
% who have been asked to do so by their supervisor
% who can correctly identify specific items covered in awareness materials
% who know their security officer by name
% who know how to contact their security officer (or the Incident Response Team / Help Desk)
% who know how to recognize an anomalous event
% who know when to contact the Help Desk versus the Incident Response Team
% who have asked for help with security (for work systems / for home systems)

continued on page 4

continued from page 3

Security Awareness Program Metrics End User Knowledge and Perceptions of IT Security <i>(Could be tailored for use as a Baseline Survey)</i>
% of users, managers, or technologists, who believe that security requirements do not apply to them / their business function
% who know if their computer use is monitored / how it is monitored
% of who use thumb drives or removable media
% who have remote access
% who avoid use of personal e-mail accounts at work
% who use company or government e-mail for personal use
% who believe that the acceptable use policy is enforced
% who believe that management is committed to security
% who believe that management sets a good example regarding security behaviors
% who believe that repeated bad security behaviors are punished
% who believe that ugly security behaviors are punished
% who believe that good security behaviors are rewarded