Facilitator Notes

Introduction

Over the past 10 years, personnel working in the Department of the Navy have become more and more dependent on the use of Information Systems and Information Technology to do their jobs. The new, networked environment we live in today has created many new changes in the way we work, communicate, interact with others, and generally view the world. This new environment has also given rise to ethical issues that challenge our traditional value system and ethical norms. These ethical issues are a result of our use of Information Technology - an instrument creating new human action and making it possible for humans to behave in ways they could not without technology.

The Navy and Marine Corps have experienced an increased number of incidents of unethical behavior by personnel using government computers and networks. The cause of these incidents is not the result of a deterioration of our Honor Code -- but in fact, linked to the nature of Information Technology itself. Factors contributing to these behaviors include the limited enforcement of existing policy and regulation, the "policy vacuums" that are created by the expansion of Information Technology, and the individual users perception of the technology, it's capabilities, and it's uses.

The purpose of this training is to provide Department of the Navy personnel with a training tool that furthers their understanding of the ethical responsibilities that are required when using Information Technology and to provide a broad knowledge base that facilitates better decision making when facing ethical dilemmas.

The military Honor Code mandates that military personnel be held to a higher standard of behavior than what is typically expected of our civilian counterparts. In today’s military, personnel have more autonomy and are required to exercise personal judgment and decision-making more than ever before. Choices about personal behavior, specifically, making decisions that are ethical and beneficial to the service member and his organization, become more pronounced in cyberspace. The process of effective decision-making is at the heart of this training. Simply pointing to a list of rules in a frame on a wall doesn’t provide an individual with the tools to react to situations he or she finds in daily life. There is an enormous amount of information available to Navy and Marine Corps personnel concerning ethics and ethics awareness in the Department of Defense. The goal of this training is to condense available information and combine it with scenario-based dilemmas to provide a concise and informative tool to better prepare the users of this material with the knowledge to deal with the ethical dilemmas that can be faced while using Information Systems and Information Technology.
Objectives
Identify for the user what Information Technology and Information Technology Ethics are and how the study of ethics relates to Information Technology.

Explain how and why Information Technology gives rise to ethical dilemmas that other technologies don't.

Provide framework for Information Technology users with tools that will assist them in their decision-making when faced with Information Technology ethical dilemmas.

Make users aware of the ethics policies of DoD and better understand their application.

Training Format

This subject matter lends itself more toward group discussion than individual reading and rote memorization. Therefore, this training is designed to allow for small discussion group interaction concerning Information Technology and its ethical use.

The Scenarios portion of the CD contains over 20 scenarios addressing various ethical dilemmas for presentation and discussion, each ending with discussion points and a reference to the appropriate regulation or instruction best suited for guiding that decision.

What is IT Ethics: Theoretical Background

IT ethics is rooted in the conventional study of ethics. In order to better understand ethics in the realm of computer technology, a brief discussion of some popular ethics models should be addressed.

The Golden Rule

Whether elicited from Confucius, Aristotle, or the Bible, the principle of treating others the way you want to be treated often reveals to the decision
maker what the right thing to do is. This “golden rule” establishes a baseline for behavior by requiring a person to be concerned with the well being of others while acting for his own benefit. The decision makers use of this rule requires that he place himself in the shoes of someone who might be in a position to act in a way that could affect him, creating an introspective look at the decision making process and requiring specific thought application to the issue.

**Utilitarianism**

Utilitarianism is a consequence-based theory, stating that the only real factor a person should consider when making a decision is the consequence of the action and how many people would the action positively affect. The right (or good) choice is the one that provides the best outcome for the most people. At the basic level, this theory has an end toward the perfect solution, but human nature makes it difficult to determine what the right thing for all is. It becomes very easy for consequence-based decisions to become situational, with the decision maker rationalizing his actions for a self-serving purpose.

**Pluralism**

This theory is based on the concept of doing ones duty. Pluralism holds that decisions should be made out of a sense of duty to do the right thing. According to this theory, as rational beings, humans are able to resist impulse and do the right thing absolutely, regardless of the consequences. The concept of duty within the theory is that of doing the right thing, with the right attitude, for the right reason. Proponents of this theory espouse that the duty to do the “right” thing is absolute, without exception, regardless of circumstance. This is where the opponents of this theory take issue. Nothing can be considered absolute in the arena of personal human interaction because of the innumerable variables involved. Rational people exercising good judgment should be able to tell when exceptions can be made.
Now that we have looked at some theory, let’s see how ethics and technology are tied together.

**Ethics and Technology**

Consider the illustration below

In general, the law delineates what is legal and illegal in everyone’s eyes. On the question of law, there is no gray area, only a single line, to be crossed or to be observed. When the discussion turns to ethical behavior however, the line becomes fuzzy, or wider, with no single authority demanding observation of a particular barrier upon which not to cross. The shaded area is the one of concern for our discussion. This illustration is not in anyway limited to the IT world, but clearly the actions taken behind a computer or inside a network are applicable.

Keeping in mind the models just introduced, what are the issues that tie ethics and technology together and how has the emergence of technology created new ethical dilemmas?
Consider the following table.

<table>
<thead>
<tr>
<th>General Terminology</th>
<th>IT Terminology</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cheating</td>
<td>Copying</td>
</tr>
<tr>
<td>Plagiarizing</td>
<td>Copying, Internet search</td>
</tr>
<tr>
<td>Stealing</td>
<td>Copying, burning (as in copyrighted CD’s)</td>
</tr>
<tr>
<td>Trespassing</td>
<td>Enumeration</td>
</tr>
<tr>
<td>Spying</td>
<td>Monitoring, sniffing, surveillance</td>
</tr>
<tr>
<td>Misappropriation</td>
<td>Misuse, unauthorized use</td>
</tr>
</tbody>
</table>

In general, the actions on the left carry more negative connotation than those on the right. The increased use of IT has been the driving force behind the evolution of terminologies, each change lessening the negative connotation or degree to which the precedent term is received. The change in connotation is not hard to discern when viewed side-by-side. This may help us understand why there is a disconnect between how people perceive the real world and the world on the other side of the computer screen.

How does all of this apply to the military environment? Let’s take a military perspective from three different angles: First, from a technical viewpoint, next, from an organizational perspective, and finally, a personal viewpoint.

**Technical Viewpoint**

When dealing with IT and the virtual Internet environment, traditional ethical concepts apply, only now they require a bit of translation. In general, users have not viewed the world of computers as “the real world.” Hackers, “script kiddies,” and computer professionals have developed technical expertise, which enables them to commit cyber crimes or do serious damage to systems. It
has been commonplace in current news to hear about these people getting caught in cyber crimes and when questioned about the crime, the typical response from the perpetrators is they didn’t think they were doing anything wrong. This view of the IT world is being carried by many of the young men and women that are joining our armed forces. Changing these views through training and awareness is key to building a force that is not only IT savvy, but is aware that ethical conduct transfers into the realm of IT usage. As technology continues to develop, becoming more and more complex, it will be necessary for everyone to be as educated as possible when it comes to IT, in order to make a better decision when faced with an ethical dilemma.

**Organizational Viewpoint**

Military organizations are characterized by a distinctive culture, more than most other organizations. This culture, by design, permeates areas of personal as well as professional life. There has always been a subjugation of rights by those in the military. One’s expectation of privacy, and personal rights are not equal to those outside the military. The right to privacy is an instance that can be directly related to the IT world. Deployed sailors and Marines live in open barracks and share close quarters on ship. In these instances, there is no expectation of privacy. This reduction in privacy is a situation that no civilian would readily volunteer himself to be a part of. The right to privacy has expanded some with the advent of apartment-style barracks, but personnel are still subject to unannounced inspections and regulations that govern on-based residency. This privacy issue correlates directly to the IT privacy issue. All DoD computer systems are subject to monitoring, regardless of who is using the system. This type of universal monitoring isn’t commonplace outside the military organization.

**Regulations and Enforcement**

As it has done many times over when dealing with new issues that appear to be straightforward, the Department of the Navy applies its ideological
prudence by creating policy and regulation to address new circumstances. These new policies are typically based on previous paradigms, which may or may not fit the situation. Although every effort is taken to prevent gaps, the fact remains that computers and information technology create ethical issues that result in policy vacuums that cannot be addressed in a timely manner. The specific regulations and policies that are issued starting at the highest command, and then subsequently followed by each subordinate command, identify the “official” and “authorized” use of IT assets. These regulation and policies are a good first step, but fall short of addressing or resolving the problems that occur when personnel are faced with decisions that require ethical prudence.

The letter of the law so to speak is found in DoD Instruction 5500.7-R, which is the Joint Ethics Regulation. Chapter 2 of this Instruction deals with the Standards of Ethical Conduct. Section 2-301 is the appropriate section of the Manual dealing with this subject. You may view the entire document at http://www.defenselink.mil/dodgc/defense_ethics/ethics_regulation/.

The following is text directly from the Instruction:

2-301. Use of Federal Government Resources.

a. Communication Systems. See GSA regulation 41 C.F.R. Subpart 201-21.6 (reference (h)) on use of Federal Government telephone systems. Federal Government communication systems and equipment (including Government owned telephones, facsimile machines, electronic mail, internet systems, and commercial systems when use is paid for by the Federal Government) shall be for official use and authorized purposes only.

(1) Official use includes emergency communications and communications that the DoD Component determines are necessary in the interest of the Federal Government. Official use may include, when approved by theater commanders in the interest of morale and welfare, communications by military members and other DoD employees who are deployed for extended periods away from home on official DoD business.

(2) Authorized purposes include brief communications made by DoD employees while they are traveling on Government business to notify family members of official transportation or schedule changes. They also include personal communications from the DoD employee's usual work place that are most reasonably made while at the work place (such as checking in with spouse or minor children; scheduling doctor and auto or home repair appointments; brief internet searches; e-mailing
directions to visiting relatives) when the Agency Designee permits categories of communications, determining that such communications:

(a) Do not adversely affect the performance of official duties by the DoD employee or the DoD employee's organization;

(b) Are of reasonable duration and frequency, and whenever possible, made during the DoD employee's personal time such as after duty hours or lunch periods;

(c) Serve a legitimate public interest (such as keeping DoD employees at their desks rather than requiring the use of commercial systems; educating the DoD employee on the use of the communications system; improving the morale of DoD employees stationed for extended periods away from home; enhancing the professional skills of the DoD employee; job-searching in response to Federal Government downsizing);

(d) Do not put Federal Government communications systems to uses that would reflect adversely on DoD or the DoD Component (such as uses involving pornography; chain letters; unofficial advertising, soliciting or selling except on authorized bulletin boards established for such use; violations of statute or regulation; inappropriately handled classified information; and other uses that are incompatible with public service); and

(e) Do not overburden the communication system (such as may be the case with broadcasts and group mailings), create no significant additional cost to DoD or the DoD Component, and in the case of long distance communications, charges are:

1. Charged to the DoD employee's home telephone number or other non-Federal Government number (third number call);

2. Made to a toll-free number;

3. Reversed to the called party if a non-Federal Government number (collect call);

4. Charged to a personal telephone credit card; or

5. Otherwise reimbursed to DoD or the DoD Component in accordance with established collection procedures;

(3) In accordance with applicable laws and regulations, use of Federal Government communications systems may be monitored. See DoD Directives 4640.1 (reference (i)) and 4640.6 (reference (j)). DoD employees shall use Federal Government communications systems with the understanding that such use serves as consent to monitoring of any type of use, including incidental and personal uses, whether authorized or unauthorized. In addition, use of such systems is not anonymous. For example, for each use of the Internet over Federal Government
systems, the name and computer address of the DoD employee user is recorded by the Government and also by the locations searched.

(4) Most Federal Government communications systems are not secure. DoD employees shall not transmit classified information over any communication system unless it is transmitted using approved security procedures and practices (e.g., encryption, secure networks, secure workstations). In addition, DoD employees shall not release access information, such as passwords, to anyone unless specifically authorized to do so by the Agency Designee. See DoD Directives 5200.28 (reference (k)) and C-5200.5 (reference (l)). DoD employees should exercise extreme care when transmitting any sensitive information, or other valued data. Information transmitted over an open network (such as through unsecure e-mail, the internet, or telephone) may be accessible to anyone else on the network. Information transmitted through the Internet or by e-mail, for example, is accessible to anyone in the chain of delivery. Internet information and e-mail messages may be re-sent to others by anyone in the chain.

b. Other Federal Government Resources. Other than the use of Federal Government communications systems authorized in accordance with subsection 2-301.a. of this Regulation, above; the use of Federal Government resources as logistical support to non-Federal entity events in accordance with subsection 3-211 of this Regulation, below; and the use of Federal Government time authorized in accordance with subsection 3-300 of this Regulation, below; Federal Government resources, including personnel, equipment, and property, shall be used by DoD employees for official purposes only, except as follows:

(1) Agency Designees may permit their DoD employees to make limited personal use of Federal Government resources other than personnel, such as typewriters, calculators, libraries, and other similar resources and facilities, if the Agency Designee determines the following:

(a) The use does not adversely affect the performance of official duties by the DoD employee or the DoD employee's organization;
(b) The use is of reasonable duration and frequency, and made only during the DoD employee’s personal time such after duty hours or lunch periods;
(c) The use serves a legitimate public interest (such as supporting local charities or volunteer services to the community; enhancing the professional skills of the DoD employee; job-searching in response to Federal Government downsizing);
(d) The use does not put Federal Government resources to uses that would reflect adversely on DoD or the DoD Component (such as involving commercial activities; unofficial advertising, soliciting or selling; violation of statute or regulation; and other uses that are incompatible with public service); and
(e) The use creates no significant additional cost to DoD or the DoD Component.
Personal Viewpoint

Ethical issues cannot be resolved until a full understanding of what technology is, how it should be used, and what kind of ethical dilemmas IT creates are addressed.

The idea of doing one’s duty, serving one’s country, of honor, courage, and commitment create the backdrop upon which all service members must make decisions.

One issue is that no matter how well a service member tunes into the “military way of life,” there will always be the desire to put one’s own well being first, regardless of how it will affect others.

Another issue revolves around the complicated makeup of our organization, in that active duty military, civil service and contract personnel have different perspectives of the organization and each apply the value system they hold accordingly. For instance, the civil servant’s viewpoint may not be one of duty to country but to execution of a job description. Training programs, education and awareness, strict enforcement of existing policy and leadership are all pieces of the solution to the unethical behavior we see occurring almost daily. Part of the issue we arrive at is that leadership’s role in the decision making process is one of mentor and teacher, by instruction and by example, enabling each person to realize that the best decision for the individual is the decision that is best for all.

Core Values

No ethical discussion in a military context would be complete without discussing Core Values. Our core values of Honor, Courage, and Commitment apply to all aspects of life. Whether in uniform or out, on or off duty, in formation or in cyberspace, the general characteristics that are espoused during entry level training into the military should carry over in the IT world. Individual values and beliefs are ingrained, starting from childhood, shaping the way we view the world,
how we perceive right and wrong, and creating the convictions that motivate our actions. Values such as trust, responsibility, respect, judgment, and honesty are foundations we rely on in building our convictions and guidelines we use to govern our actions. When applied to the computer environment, there should be no difference in their application.

Discussion on Decision Making

The process of sound decision-making is a learned skill, taking years to develop. This section provides the basic elements and definitions of decision-making that will be useful to the users of this training.

A “decision” is defined as a conscious choice made among available alternatives. “Decision-Making” is the process by which an individual identifies problems, opportunities and outcomes as a result of the alternatives derived from the decision that will be made. There are several factors that influence an individual decision-maker’s ability to make decisions, such as values, personality, and the propensity for risk and potential for dissonance.

Values are guidelines a person uses when confronted with a situation in which a choice must be made. These values are acquired early in life and are a basic part of a person’s personality.

Personality is the psychological force or make-up of a person that derive from a person’s belief, attitude, needs, and external physical and environmental forces that are called upon to influence a give decision.

Risk can be characterized in terms of gains or losses, in which the decision-makers’ perception of the final outcome is influenced by what they perceive the outcome might be.

Dissonance is internal conflict created by holding beliefs and attitudes that conflict with each other at the same time.
A decision maker will unconsciously use these factors to influence a decision. Decisions are further broken down into two categories: Programmed and non-programmed decisions.

Programmed decisions are a consequence of past situations that have occurred where a decision maker is able to apply “rule sets” from previous situations that enable that decision maker to choose an alternative that best suits his or her need or desired outcome.

Non-programmed decisions are just the opposite, where the situation that has occurred is new and the decision maker does not have the past situational expertise and must rely on other “rule sets” or experiences in choosing the right alternative for the given situation.

With guidance from existing policy, regulation, Core Values and the Military Honor Code, it is hard to believe that Department of the Navy personnel – when using Information Technology – could make an “unethical” decision, that is, choose an alternative that does not fit our ethical standard. Yet some people choose to take the “risk” and go counter to our ethical standard, while others just are not aware that their decisions concerning the use of Information Technology is inappropriate or unauthorized.

The small percentage of Department of the Navy personnel that choose to blatantly defy existing policy, regulation and the core values in place will continue to do so no matter what. The other percentage of personnel can apply these basic decision making steps that will ensure that the best possible outcome can be achieved:

---

**Step 1.** Are you aware of any rule, regulation, statute, policy or directive that would otherwise alter your decision?

**Step 2.** Are you aware of all the possible outcomes or impacts of the decision that will be made?

**Step 3.** Is the result of your decision an outcome that is counter to the known core values – Honor, Courage and Commitment? Or counter to the Department of the Navy Honor Code?

**Step 4.** Would you do the resulting action in front of your Commanding Officer, Command Senior Enlisted or supervisor?

By applying these steps the decision maker will be able to choose an alternative that will result in the best possible outcome.
Behaviors

As defined by the DoD instruction, official use, authorized use, and unauthorized use are the only three types of actions that can be taken with a DoD computer or network. From these usage definitions, a list of activities was created to expand them into specific illustrations of each action. Many of these actions can be further tuned into specific examples to fit various types and sizes of commands. Feel free to modify these actions as you see fit. The actions are not listed in any order.

- Originating/Forwarding Chain email
- Forwarding Joke emails
- Chat room use
- Playing Games
- Personal Email Subscriptions
- Downloading Freeware
- Downloading MP3's
- Downloading Porn
- Paying personal bills online
- Personal Online Shopping
- On-line Gambling
- Conducting Personal Stock Trades
- Use for Personal Business
- Hate Mail
- Threatening Email
- Sending Class Info on Unclass System
- Unauthorized Access of another account
- Email Monitoring
- Internet Access Monitoring
- Mirroring Email Accounts
- Creating Dummy Accounts
- Password Theft
- Identity Theft
- Hacking (all types)
The scenarios are designed to facilitate discussion of ethical dilemmas faced by the characters.

Password Theft Scenario Unauthorized Access

Issues: Appropriate Use; Security; Privacy

Corporal Jones watched as Corporal Edwards logged in with his user name and network password. He never intended to memorize the password, but how hard is it to forget “asdf7890”? At the time he thought that Corporal Edwards' password was too easy for someone to steal, but he didn’t mention it, and didn’t think anything about it after that.

Three months later, Corporal Jones was rushing to finish a project for Captain Gonzales, when he realized that most of the data he needed to complete the project was on Corporal Edwards’s computer. Corporal Edwards wasn’t coming back from his OCONUS TAD trip until next week. Just as he is about to tell the Captain he could not finish the job, he realized that he could get into Corporal Edwards’ computer files because he remembered Corporal Edwards’ password.

DECISION POINT

1. Does Corporal Jones log into the network using Corporal Edwards' password, retrieve the files he needs and log out?
2. Does Corporal Jones tell Captain Gonzales that he cannot finish until Corporal Edwards' return?

Discussion Points/Things to consider:

Should Corporal Jones violate network policy and Corporal Edwards’ trust by using his password to get the information he needs to complete the project? It would ensure that he gets the job done in time. No one would ever know about using the password.

Wouldn’t it be a violation of Corporal Edwards’ privacy? If Corporal Jones uses the password, should he tell Corporal Edwards to change his password when he gets back? Should he have told Corporal Edwards that he saw the password in the beginning?

Typical network policy dictates that no one will use someone else's network account, as well as warning users to protect their passwords and make them difficult for anyone to remember.
Would using Corporal Edwards’ password be something that the Staff Sergeant would approve of? Would the Captain approve?
Password Theft Scenario:  Part 2  Unauthorized Access

Issues:  Appropriate Use; Security; Privacy; Leadership

Corporal Jones explains to Captain Gonzales that he cannot finish the project until Corporal Edwards’ return. Captain Gonzales wants to have the finished project to the C.O. by the end of the week, and he let’s Corporal Jones know that somehow it needs to be done. Corporal Jones then tells the Captain about his knowledge of Corporal Edwards’ password, and he could get the files easily, but that he just didn’t feel right doing that.

DECISION POINT:

1. Does Captain Gonzales direct Corporal Jones to use Corporal Edwards’ password to ONLY get the information he needs to finish the project, and then log out?
2. Does Captain Gonzales wait until Corporal Edwards comes back on Monday to get the finished project?

Discussion Points/Things to consider:

As a leader, Captain Gonzales has a dilemma here. He knows that Corporal Jones didn’t “feel right” about using Corporal Edwards’ password. He also would like to get this project finished and on the C.O.’s desk by Friday.

Should he tell Corporal Jones to do whatever is needed, and he’ll let Corporal Edwards know what they did when he returns? Is the project so critical as to warrant violating network policy in order to finish it?

What is Corporal Jones’ perception of his leadership if he goes against what Corporal Jones thinks is the right thing to do?
SSgt Harris is the System Administrator for the command. He is very technically competent, more so than his fellow system administrators on the base. He has taken courses on his off-duty time to learn as much as he can about networks and the particular operating system he is in charge of. He enjoys his work immensely, calling the network “his network” most of the time. His feeling of personal ownership of the network is almost beyond what would be considered normal.

SSgt Harris was nominated for Staff Non-Commissioned Officer of the Year for Marine Corps Logistics Base Albany. It has been a month since the interviews with the nominees. SSgt Harris knows that along with the award comes one week of special liberty, which he would like to take in Texas with his wife and son. He has an idea that the C.O. already knows who the winner is, but is waiting until the next battalion formation to announce the winner.

It would make his travel plans much easier if he could book his travel in advance, and waiting another 10 days for the announcement could increase his cost of travel.

**DECISION POINT:**

1. SSgt Harris considers mirroring the C.O.’s email account to try and find out if he won the SNCO of the Year award. He would only do it to find that out, and then delete the mirrored account. No one would ever know he did it.

**Discussion Points/Things to consider:**

SSgt Harris knows that he could accomplish this without anyone knowing what he did. Does this make it the right thing to do? The benefit of mirroring the C.O.’s account equates to a savings of possibly hundreds of dollars in plane tickets.

Mirroring of emails accounts is typically done as a backup to actual accounts for redundancy purposes. Nothing SSgt Harris is contemplating is illegal.
Chief Davis just bought a new MP3 player to replace his broken CD player. After a few nights at home on the Internet, he realizes that downloading MP3’s on his 56k modem takes all night. He knows that the network connection at work is a T1, and is fast enough to download MP3s quickly and easily, especially after working hours.

DECISION POINT

1. Does Chief Harris download MP3’s in the background of his desktop while working?
2. Does Chief Harris return after working hours and downloads MP3’s while finishing up paperwork?

Discussion Points/Things to consider:

Chief Harris can get faster downloads at work, but is that an authorized use of the network? Consider this: What if all owners of MP3 players within the command downloaded MP3’s while at work? This would degrade the performance of the entire network due to the amount of bandwidth being utilized by the MP3 traffic. This in turn restricts the amount of data being carried by the network.

What if he comes in after work? No one is using the network then.

Chief Harris can rationalize that MP3’s for his player are good for morale.

As with anything downloaded from the Internet, MP3s’ can contain viruses, which can be harmful to the network.
On-line Gambling Scenario

Issues: Appropriate Use

During the lunch portion of the training schedule, Gunnery Sergeant Walker clicks through the web pages of USAToday.com for the latest line on Monday Night Football. He has to get the bet in before the start of the game, and he won’t get home until it’s too late to call it in. He knows of various on-line sports books where he can bet on-line. He has used some of them before; they save time and are very convenient.

DECISION POINT

1. Does Gunny Walker log in and lay his bet on-line to save time and make sure he gets the best line available.

Discussion Points/Things to consider:

Is this something that is considered authorized use of the network? Gunnery Sergeant Walker is an authorized user, but does that give him the authorization to place bets online during lunch?

How is this different than typical Internet searches?

Should the Gunny be authorized to read the sports section of the USAToday.com website during working hours?
On-line Stock Trading Scenario

Appropriate Use

Issues: Appropriate Use

While eating breakfast at his desk at 0630, Major Easton reads the Wall Street Journal on-line, waiting for the rest of his staff to arrive at work. He reads an article concerning a company in which he owns stock, reporting their negotiations with DoD in finalizing one of the largest contracts of the year. The news and stock ticker that runs along the bottom of his computer screen is near real-time, and shows no significant increase in the stock price yet today.

He has been planning to increase his number of shares in this company, and now seems like a great opportunity before the stock price goes up. He has an on-line trading account, but he’s never used it at work. Waiting until the end of the day could cost him a lot of money.

DECISION POINT

1. Does Major Easton log into his trading account using the computer at his desk and purchase more shares of the company at the opening price?

Discussion Points/Things to consider:

This is clearly personal business, but why shouldn’t the Major be able to take advantage of workplace technology to invest his savings? Retirement planning and counseling is something the Marine Corps does for everyone getting out of the Marine Corps. Isn’t this a form of retirement planning?

Should the Major have a news and stock ticker on his screen? If everyone had one, the bandwidth that would be taken up would hamper the performance of the network.
Personal On-line Shopping

Issues: Appropriate Use

Lieutenant Anderson sees the Operational Tempo over the last month as somewhat incredible. He never realized that the Battalion would stay so busy during the six months prior to deployment. He feels like he hardly sees his house. Out the door before daylight, home after dark, up until midnight planning for the next day. And that’s when he’s not out in the field for a week straight.

He didn’t have time to get his sister a birthday card last week, his brother’s wedding anniversary is coming up, and Mother’s Day is next week. Who has time to shop with another battalion exercise starting Sunday night for 10 days in preparation to deploy in three weeks?

When he was at the Infantry Officer’s Course he at least had time to jump on-line and shop for things he needed after the training day was done.

DECISION POINT

1. Does Lieutenant Anderson use the office computer and purchase gifts for his sister, brother, and mother during lunch?

Discussion Points/Things to consider:

The Marine Corps’s Operational Tempo has continued to increase over the past few years. Even before then, it was not uncommon for infantry units to work from sunup to sundown for weeks in preparation for deployment. Is it too much to ask to allow users to do some shopping online to save some time?

What harm could come to the network from doing a little shopping online now and then?
Email Monitoring Scenario               Organizational Ethics

Issues: Privacy; Email use

Sergeant Johnson reported to the Sergeant Major as directed by his Platoon Commander. He had no idea why the SgtMaj wanted to see him. When he arrived, the SgtMaj asked Sergeant Johnson to look at some paperwork he had in front of him. Sergeant Johnson took the papers, and as he read, he realized that he was reading emails that he had sent to other Marines in various commands across the base, concerning their activities on liberty the weekend before. Although the emails did not contain any information concerning any illegal activities, they weren’t the type of emails that Sergeant Johnson wanted anyone else to see.

The SgtMaj informed him that although no action was going to be taken against him for the email content, he was to be aware that all email traffic is monitored on the network.

Sergeant Johnson left the SgtMaj’s office feeling as if his privacy had been violated.

DECISION POINT:

1. The decision in this case was that of the C.O. The C.O. had already authorized active monitoring of command email accounts as part of a command-wide drug investigation. The Officers and SNCOs of the command were fully aware of the stepped up monitoring.

Discussion Points/Things to consider:

Is there any expectation of privacy when using a government computer system?
Every government computer has a warning screen that appears prior to log in that states:

“All information, including personal information, placed on or sent over this system may be monitored. Use of this DoD computer system, authorized or unauthorized, constitutes consent to monitoring of this system.”

Most users only read the first few lines of this warning, if at all.

Is the C.O. decision to monitor emails to hunt for drug users appropriate? What about the privacy considerations of the users?
Chat Room Scenario

Issues: Appropriate Use

PFC Stevens hasn’t made many friends since he came to the company. After injuring his ankle on the range, he’s been pushing paper for the First Sergeant for a month. His lunchtime regimen has been limited to sitting in the office on phone watch.

PFC Stevens has many high school friends back home who love to log into their favorite chat room and chat for hours. How much more boring could his current duties be?

DECISION POINT:

1. Does PFC Stevens log into the chat room to talk to his high school buddies over lunch?

Discussion Points/Things to consider:

It certainly would be a morale booster if he went into the chat room and conversed with his buddies awhile. But is this proper use?

How is this different from calling home on the company office phone?

If it were a chat room full of Marines talking about issues dealing with Marine life, would it be more acceptable?
Game Playing Scenario

Issues: Authorized Use; Security

The network administrators had deleted all the games that came with the Windows Operating System. Lance Corporal Smith knew they had not blocked all the online game sites, because the command allowed a few of the computers to be used to play Marine DOOM on the network to hone tactical decision making skills.

DECISION POINT:

1. Does Lance Corporal Smith utilize this information and return after work and play online games rather than sit in his barracks room watching TV all night?

Discussion Points/Things to consider:

After hours there is no one on the network, and he is not disturbing anyone.

If the command allows Marine DOOM to be played, what’s wrong with a little Quake or Dungeon Master?
Identity Theft Scenario

Malicious Intent

Issues: Privacy;

As the System Administrator, it wouldn’t be hard for Chief Baker to create another account to look like Lieutenant Commander Springer’s. Getting Lieutenant Commander Springer’s Social Security Number from an old roster in the admin office would be relatively simple as well. With these two items, Chief Baker could apply for credit cards in LCDR Springer’s name and buy items online easily. The way online shopping is, the only thing you need is a number and an address, and LCDR Springer’s old address would do, now that he was leaving to go to Japan this month. He wouldn’t know anything about this on his credit rating for months.

DECISION POINT

1. Does the Chief use his skill as the System Administrator to commit a cyber crime?

Discussion Points/Things to consider:

As unlikely as it would appear, this sort of thing happens in the Department of the Navy. What is the thought process behind the Chief’s actions if he does what he’s contemplating? Does he not think he can get caught? Does his security in the online environment make him feel like he can steal without being found out?

Would the Chief likely steal money from a wallet left out in the gym locker room?

Some people will commit illegal acts more readily if they feel they are shielded by the computer network they are utilizing to perpetrate the crime.

Others are just criminally inclined whatever the method.
Sending comical emails Scenario

Appropriate Use

Issues: Network Usage; Unauthorized Use

The website www.annonomail.net is an anonymous emailer which allows people to send emails to friends, family, and co-workers anonymously. Sergeant Tracy has just been the recipient of an amusing and confusing email, until his buddy let him in on the joke. He thinks it would be funny to send out a few emails to his friends for laughs.

Decision Point:

1. Does Sgt. Tracy use a government computer to send humorous emails to his friends?

Discussion Points/Things to consider:

How is this any different from sending harassing or threatening emails? This obviously isn’t government business, but neither was emailing all his buddies about going to the movies Friday night. Is there any difference?
Threatening Email Scenario Unauthorized Use/Malicious

Issue: Security; Inappropriate Use; Abuse of Responsibility

Petty Officer Postorino is the email administrator and considered to be one of the Command computer experts. Because he knew he was a valued asset in his Command, he often reported for duty late. After several warnings about his tardiness, the Command Leading Chief put PO Postorino on report. He decides to get revenge by sending the Leading Chief an anonymous “threatening email” warning the Leading Chief to watch out – someone is going to get you!!!

Issue: Inappropriate Use; Abuse of Responsibility

Decision Point:

Does PO Postorino abuse his responsibility and authority as the email administrator by sending the Chief a threatening email? What are the significant ramifications of his actions?

Discussion Points/Things to consider:

He could send the anonymous threatening email to shake up his Leading Chief without the email being track to him. Because he is the Command email administrator, he could easily erase the logs that would implicate him as the culprit of the threatening email.
Lcpl Ford, HM3 Gaines, Cpl Clifton and Sgt Barrington were all going to end their obligated active service around the same time. They all decided to take various computer classes to better prepare themselves for transition into civilian life when their military obligation ended. About two months prior to their release from active duty, Sgt Barrington comes up with a wiz-bang idea. He convinces the other three guys to load Trojan Viruses onto the command computers so after they get off of active duty, they could get into a backdoor and conduct a distributed network attack to hack into other networks.

Decision Point:

Do these guys tamper with the Command computers to build a backdoor that will enable them to use the network once they are off of active duty?

Discussion Points/Things to consider:

Their intent is obviously malicious – why wouldn’t one of them step up to say what they were attempting to do is wrong. There also appears to be a little peer pressure – like the old saying goes – “birds of a feather flock together.”
Unauthorized Downloads Scenario

Issue: Inappropriate Use

YNC Sonia Adams has a flex working schedule and works from 2200 until 0800 Monday through Thursday, which frees up time so she can attend college during normal working hours. One evening YNC Adams received an email from a friend that informed her of some really neat pornographic web sites. In the email, YNC Adams friend told her that the pornographic sites were a new kind that could not be detected by the command network monitors. YNC Adams knows that the network is being monitored, but thinks to herself -- “what the heck – I’m here alone and they probably won’t catch me anyway, plus these are the new undetectable pornographic web sites.”

Decision Point:

Should YNC Adam access the pornographic web sites to download pornographic material on her government system?

Discussion Points/Things to consider:

Accessing pornographic material is absolutely unauthorized on government systems, but what if YNC Adams decides to download the pornographic material at home then share it with her colleagues at work?
Downloading Freeware Scenario  Unauthorized Use

Issue: Security; Network bandwidth

LT Reinkemeyer is an avid computer user and loves computer games. He loved gaming so much that he installed DSL at home to speed up his access to the Internet. Aware of the command policy and regulations about downloading application to his government PC, LT Reinkemeyer copied his favorite games that he downloaded from home on the Internet to a CD to take on deployment. Once underway LT Reinkemeyer realized that he forgot his CD with all the neat games at home. He is underway on a carrier, so he knows his ship has super-duper high-speed satellite connectivity and he decides to download the freeware to his government PC on ship.

Decision Point:

Fully aware of the command policy the good LT needs his fix. Should he download the freeware from the Internet?

Discussion Points/Things to consider:

The freeware the LT downloaded could contain Trojan viruses, and downloading huge games on the ships network increases bandwidth usage tremendously, which will degrade the speed of the ship’s network.
Personal Email Subscriptions Scenario  Unauthorized Use

Issue: Inappropriate Use; Network bandwidth

CDR Makarski is the Command Executive Officer of the USS Kearsarge. In his spare time he loves to hunt and fish, and has several magazine subscriptions for various outdoorsman type magazines. Knowing that while underway his subscriptions are always 2-3 weeks late, he contemplates signing up to receive his subscriptions electronically. CDR Makarski doesn’t own a personal computer at home, so he never has done this in the past.

Decision Point:

Does the CDR subscribe to his magazines on-line to get them on time while deployed?

Discussion Points/Things to consider:

Isn’t this just like getting any other email from home?

This is a morale booster that he considers extending to the rest of the crew.

How does this affect the bandwidth usage on the ship?
On-line Bill-pay Scenario  Unauthorized Use

Issue:  Inappropriate Use; Security; Network bandwidth

Seaman Recruit Michaels is a hard charging up and coming Seaman Apprentice that is so squared away he completed all of his personal qualifications through Petty Officer First Class in his first year of active duty. While getting cash out of the ATM, SR Adams notices an advertisement from his bank about paying bills online. Being the squared away sailor that he is, SR Adams thinks that paying bills online is a terrific idea, particularly once underway, but he does not have a PC since he lives in the barracks. Surely using one of the command’s computers would be alright.

Decision Point:

Does SR Adams decide to use one of the Command PC’s to pay his bills online?

Discussion Point:

What are the ramifications of this decision? What SR Adams is doing appears to be harmless – especially since he has no other means of using a computer to pay his bills.
As he walks through the building during lunch, Captain Anderson notices that many people who eat lunch at their desk are surfing the Internet as they eat. Everything from local news and weather to sports and crossword puzzles on their desktops. When he gets back to his office, he calls LCDR Byrd and asks him to come up to his office to answer a few questions concerning Internet use. Specifically, he wants to know what the command is doing in terms of limiting website access to questionable sites, and whether or not the system logs Internet traffic within the building. If so, the Captain would like to view today’s log.

Decision Point:

The decision has previously been made by the System Administrator to configure the system to log all Internet traffic within the command. The answers he will give the Captain should satisfy his access concerns. He prints out the log for the CO to read.

Discussion Points/Things to consider:

Should the CO be reviewing ALL Internet access? Or should he just be alerted to illegal or unauthorized traffic?

Aren’t their privacy laws that prevent this type of “Big Brother” behavior?
PDA Use Scenario

Issues: Inappropriate Use

Staff Sergeant Hopkins had received his new PDA from the Supply warehouse last month as part of the Regimental Commander’s initiative to aid small unit leaders in their training efforts. It was very convenient to have the battalion training schedule for the next 6 months at his fingertips rather than carrying around paper copies that needed to be revised every week. If there were any changes to the schedule, he would update his file with the “sync’ function in the PDA.

He has all this functionality at his fingertips, and wants to use it for his personal calendar and contacts as well as those for work.

DECISION POINT:

Should Staff Sergeant Hopkins use his government issued PDA for his own personal items? Does it really make sense to have 2 PDA’s, one for work related items and one for personal usage?

Discussion Points/Things to consider:

He has been told not to use his office computer for personal business. How is this different?