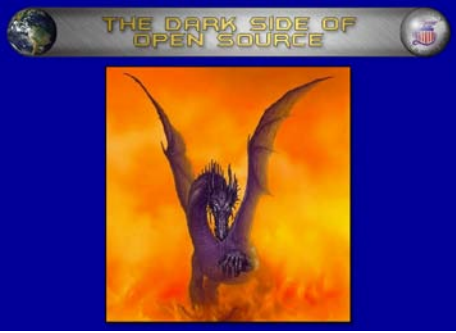
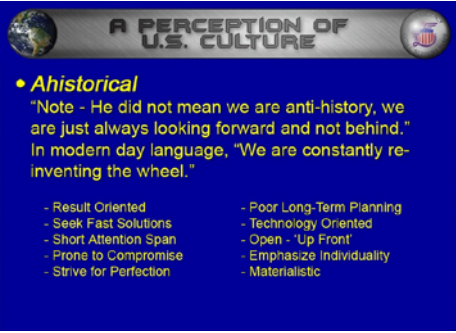
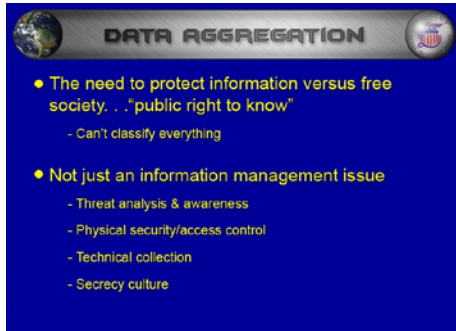


## LESSON PLAN: THE DARK SIDE OF OPEN SOURCE

<p><b>Slide #1:</b></p>  <p>Teaching Points:</p> <ol style="list-style-type: none"> <li>1. Public domain &amp; the "So what?" question</li> </ol>	<p>The question of how much information to release in the public domain comes down to two things: asking the “so what” question and understanding what “public domain” really is. Answering the “so what” question informs you of anyone out there who would/could use that information against you. Defining “public domain” helps you understand that anything released on the Web or via the media is potentially available to anyone who’s interested. If you realize that there are people who want your information because they want to hurt you, and that everything they need to know can be compiled if you release it, then deciding what to protect becomes a bit easier.</p>												
<p><b>Slide #2:</b></p>  <p>Teaching Points:</p> <ol style="list-style-type: none"> <li>1. Describe foreign views of Americans</li> </ol>	<p>A foreigner visited the US and while here, he made several observations about Americans, and published his observations the next year. He observed that Americans are a-historical, that is, we are always looking forward, never behind. He also ascribed the following characteristics to American culture:</p> <table border="0" style="width: 100%;"> <tr> <td>Results oriented</td> <td>Short attention span</td> </tr> <tr> <td>Open -- ‘Up Front’</td> <td>Poor long-term planning</td> </tr> <tr> <td>Prone to compromise</td> <td>Materialistic</td> </tr> <tr> <td>Emphasize individuality</td> <td>Seek fast solutions</td> </tr> <tr> <td>Strive for perfection</td> <td></td> </tr> <tr> <td>Technology oriented</td> <td></td> </tr> </table>	Results oriented	Short attention span	Open -- ‘Up Front’	Poor long-term planning	Prone to compromise	Materialistic	Emphasize individuality	Seek fast solutions	Strive for perfection		Technology oriented	
Results oriented	Short attention span												
Open -- ‘Up Front’	Poor long-term planning												
Prone to compromise	Materialistic												
Emphasize individuality	Seek fast solutions												
Strive for perfection													
Technology oriented													
<p><b>Slide#3:</b></p>  <p>Teaching Points:</p> <ol style="list-style-type: none"> <li>1. Describe foreign views of Americans</li> </ol>	<p>He also said we have a tendency to see others as being like us, as having our value system – a certain kind of arrogance that prevents us from recognizing differences in other societies. Would it surprise you to know the visitor was Alexis de Tocqueville, the French aristocrat, and he visited the U.S. in 1831? The same nature that drives Americans to seek solutions, move out, get things done drives us to share information, because information is central to those objectives. Also, we’ve infrequently experienced the dangers of sharing too much information, so we don’t recognize when to stop. We always give more than is necessary.</p>												

**Slide #4:**



- The need to protect information versus free society. . . "public right to know"
  - Can't classify everything
- Not just an information management issue
  - Threat analysis & awareness
  - Physical security/access control
  - Technical collection
  - Secrecy culture

Teaching Points:

1. Protection versus "Need-to-know"
2. When does information need protection?
3. Factors leading to release of information
4. Define "Lack of Awareness"
- 5.

The issue of aggregation of information -- that phenomenon where collectors and analysts take lots of pieces of information and mold them into useful intelligence -- is a difficult one in a free society. The culture and the laws of the United States compel us to balance the need to protect information with the public right to know. We can't, and shouldn't, classify everything that could potentially hurt us. It is not just an information management issue.

Information has no value in itself -- it has value in context. It requires protection only if it can be used against us, whether alone or in concert with other information. It is a matter of how an adversary could manipulate the pieces of information available in the public domain. The failure to recognize the threats and the intelligence value of any information is a lack of awareness, and inevitably leads to poor judgment on release of information. We must control access and limit the distribution of information to those who need to know. It is a matter of understanding the technical means by which an adversary can collect information, and the free availability of technology to help in that collection. At the same time, we must allow enough information to be released to the public to avoid the evolution of a secrecy culture, which would be counter to the nature of American democracy.

**Slide #5:**



- 100,000-people organization
- Part of mission classified
- Task: Communications
- Database
  - All unclassified information
  - Track parts & status
  - Track maintenance
  - Worldwide distribution
  - Chat room

Teaching Points:

1. Example of poor information release practices

As an example, you work for a worldwide organization of 100,000 people, and part of your mission is classified. Some people in the organization put their lives on the line doing their jobs, and if classified information were compromised, people could die. You are a communications operations manager, and one of your main problems is keeping track of pieces and parts -- what's operating and what isn't -- and how soon it will be fixed. You decide to develop a database that will provide you that information. You distribute the software to all of your co-workers, and use the Internet as the backbone for accessing and updating the database. Each individual piece of information that goes into the database is unclassified, so the database is unclassified.

Over time, your database works so well that others in the organization recognize its utility, and begin to use it to track other types of equipment. You add a chat room feature where maintenance personnel can talk about sharing resources and how to fix various items in our inventory. No single discussion is classified, as everyone knows it is for unclassified use only. Eventually, anyone who accesses the database can aggregate enough information to keep tabs on our operations and to predict our plans.

**Slide #6:**



Teaching Points:

- 1. Example (continued)

Turns out, there is a previously unknown group of nationalists unhappy with the U.S. presence in their country, and they have decided to adopt terrorist tactics to advance their cause.

They are funded by an international terrorist organization that has also provided them with training on terrorist tactics and ideology. They have access to, and are adept at exploiting, communications intelligence – specifically eavesdropping on telephones and faxes. They are experts in using open source to support their operations, and have moderately capable hackers to assist them in targeting open web sites, databases, and networks.

**Slide #7:**



Teaching Points:

- 1. Example (continued)

The terrorists break into our database. They acquire information to identify our resources and team members, and to identify their location and the dates of their next mission.

**Slide #8:**

**EXAMPLE**

Results

- Four of our team killed
  - unarmed
  - unaware of threat
  - unaware of vulnerability
- \$1.2 million equipment lost
- Program goals failed

The slide features a blue background with a globe icon on the left and a US flag icon on the right. It includes two small images: an American flag and a scene of a fire or explosion.

Teaching Points:

1. Example: Conclusion – Mission failure

The results are unthinkable. You lose an entire crew of people who were going to fix a broken communications tower in a remote part of the world to hostile action, and also, all their gear and equipment is lost. Four dead, three injured, \$1.2 million in state-of-the-art equipment lost or destroyed. The team was unarmed because no one thought there was a threat. All the information the terrorists got from the database was unclassified, but in retrospect, it is very vulnerable to aggregation and exploitation by your adversary. Therefore, your program has failed.

**Slide#9:**

**AGGREGATION**

- Classification rules recognize aggregation of unclassified information as potentially classified
- Freedom of Information Act recognizes aggregation: "Mosaic Theory"
- No good solution: "Electronic age"
- Basic OPSEC principle

The slide features a blue background with a globe icon on the left and a US flag icon on the right.

Teaching Points:

1. Unclassified information aggregation
2. Freedom of Information Act (FOIA)
3. Aggregation problems in automated age

Traditional classification rules recognize the potential for unclassified information to be aggregated into an overall classified product, but the solution for this situation is, for the most part, impractical in an automated age. The Freedom of Information Act (FOIA) recognizes aggregation as a "mosaic theory" problem, but this can only be applied as an exemption to release if the aggregation occurs as the result of a single request. Information obtained via the FOIA over multiple requests cannot be recovered. Neither classification management guidelines nor the FOIA offer a solution in the electronic information age. However, Operations Security (OPSEC) may be able to help.

**Slide #10:**

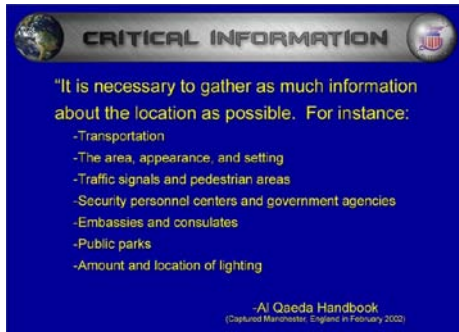


Teaching Points:

1. List ways OPSEC can help

The OPSEC process offers a model by which information can be released to the public domain while protecting those bits that could be damaging. The process offers an approach to identifying what information is critical to maintaining a necessary level of protection, to keep that which an adversary desires and requires out of the public domain. OPSEC also helps sort out who is the adversary, what vulnerabilities he could exploit, what levels of risk those vulnerabilities represent, and what to do about it.

### Slide #11:



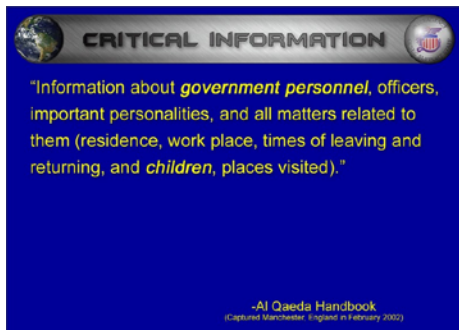
#### Teaching Points:

1. List a way to determine critical info
2. The Al Qaeda handbook
3. List open source items Al Qaeda terrorists are interested in

One way to identify what we should protect is to listen when our adversaries tell us what they need to know. In 2002, British authorities captured a handbook on how to conduct terrorist operations. The handbook points out that about 80% of the information needed to conduct terrorist operations can be obtained from open sources. It goes on to say that “it is necessary to gather as much information about the location as possible. For instance:

- Transportation
- The area, appearance, and setting
- Traffic signals and pedestrian areas
- Security personnel centers and agencies
- Embassies and consulates
- Public parks
- Amount and location of "lighting"

### Slide #12:

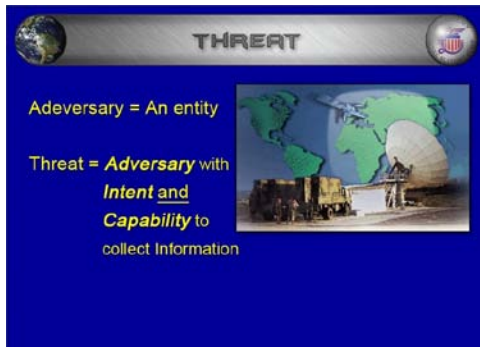


#### Teaching Points:

1. List more items of interest to terrorists

The handbook goes on to specify “information about government persons, officers, important personalities, and all matters related to them (residence, work place, times of leaving and returning, places visited, and children).” Now, when your adversary tells you what he needs to know, why would you not listen? Why would you not protect that information? A terrorist can visually collect much of what is on this list, but when they are doing surveillance, they are vulnerable. They must come out in the open, and we have a chance to catch them. It is much harder to know they are there if we publish everything they need in the media.

### Slide #13:



#### Teaching Points:

1. Define "threat"

What is the threat? While adversaries are the actual individuals and organizations out there, the threat is actually a measurement. Threat is a measure of how motivated and capable an adversary is to gain your critical information. The more motivated or better equipped an adversary is, the higher his threat rating.

**Slide #14:**



Teaching Points:

1. Define an adversary
2. List types of adversaries

Who is the adversary? Adversaries don't have to be terrorists. They can be criminals, drug trafficking groups, militia, extremists, cults, foreign intelligence operatives, or business competitors.

**Slide#15:**



Teaching Points:

1. Items that adversaries target

However, they all tend to target the same things: you and your family, your friends and coworkers, your company, your programs, your livelihood, and your country.

**Slide #16:**



Teaching Points:

1. List objectives for adversaries

Adversaries have multiple objectives. It may be intelligence collection to gain information superiority – knowledge is power, especially in business and politics. It may also be to deny service, to disrupt operations, or contaminate your database. It might be to gain notoriety, or to gain criminal advantage. It might be to terrorize the American population and cause irreparable harm to our economy and our culture.

**Slide #17:**

**TODAY'S CHALLENGES**

- 80-90% of all intelligence collected is unclassified; anything we freely provide will be exploited
- Unclassified systems to record, save and process information = compromise
- Technical security only as good as the next smart adversary
- Unclassified does not mean Unimportant

Teaching Points:

1. List modern vulnerability challenges
2. Problems in technical security
3. Unclassified doesn't mean "Unimportant"

The challenges and vulnerabilities today are many. We use mostly unclassified systems to record, save and process information, systems that are all too vulnerable to compromise and exploitation. The technical security we depend upon is only as good as the time it takes a smart adversary to find a way around it. Most of all, the challenge is to help our people recognize that “unclassified” is not synonymous with “unimportant.”

**Slide #18:**

**TODAY'S CHALLENGES**

YOU ARE HERE

Teaching Points:

1. List modern vulnerability challenges
2. Problems in technical security

The web is not the only open source available, but it is the easiest to use, the most accessible, and the least risky. However,

**Slide #19:**

**TODAY'S CHALLENGES**

Guess What?  
Your Information Is Still Out There!

Mr. Peabody, Sherman, and the Service VMAC Machine

© Jay Ward Productions

If the Web was around 500 years ago, the statement "the world is flat" would still be circulating on the net!

Teaching Points:

1. Web publishing is permanent

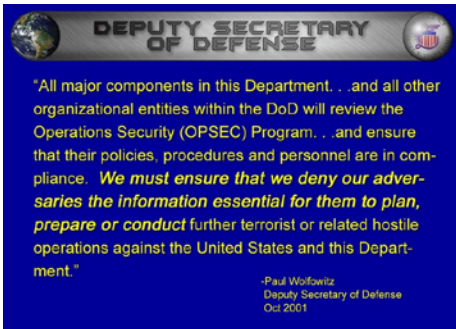
Once information is released it is gone for good. Finding information on the web requires only persistence. Once a piece of information is released to the public domain, it is waiting for someone to find it. You can't get it back. You can't tell everyone with a copy to destroy it. Archive programs absorb information several times a day. If no one found it today, they will tomorrow. If the Web was around 500 years ago, you'd still find studies proving why the world is flat!





information to allow a criminal to take advantage of your empty house, or your children's routines. Restrict release of detailed maps, instructions, procedures, and policies. Protect the identities and personal information of staff and leadership, and anyone else who might be targeted by terrorists. Don't share internal processes and security procedures or shortfalls. Don't discuss limitations. Always think like the bad guy, and before you release information assure yourself that you would be comfortable if Al Qaeda got the information you are releasing.

**Slide #23:**



Once it's been released, it's gone. Most of the information used by terrorists and other international thugs is information we gave away, not something they stole or obtained by stealth. Little pieces are important, because together they tell your story.

**Teaching Points:**

- 1. Watch what information you release

**Slide #24a:**



**Slide #24b:**



**End of Slideshow**