

Hanford Security

Remote Marketing Research Report

Prepared by

Beth Klinski and Kristin Sawyer

Prepared for

Hanford Site and Dr. Pam Henderson, WSU

Executive Summary

Hanford began in the early 1940's as part of the war effort to develop nuclear materials. Currently, the Hanford site has a moderate security environment that was brought about as the Hanford mission changed its focus from that of producing nuclear material to one of environmental clean up. The Hanford Security Awareness program has always been an important part of security.

The purpose of this marketing study was to determine three key issues. The first issue being to determine the strengths and weakness of the current security education and awareness program from a communications stand point. Second, recommend how the security education and awareness program might be enhanced to broaden its appeal and to improve project Hanford employee participation and security education and awareness initiatives. Thirdly, to establish a baseline of information that will provide measurements and meaningful conclusion so that management can then target specific areas for program emphasis.

We, a group of Washington State University students, were asked by Mr. Chester Braswell of Protection Technology Hanford (PTH) to study the security awareness program and make improvements. This was done with for our consumer behavior course with Dr. Pam Henderson overseeing us.

We conducted primary and secondary research. We used several sources including in-depth employee interviews, email surveys, personal interviews with individuals in Arlington with similar functioning facilities, and similar high security interviews. We also looked at web sites from other functioning plants similar to Hanford.

Results from an email survey indicated that improving Hanford General Employee Training (HGET), email, management communications, site news paper (Hanford Reach) news articles, staff meetings and posters might be beneficial to the security program. However, throughout our research, we determined that interpersonal advertising is what will work best. Efforts to improve security awareness should be focused on meeting with employees and discussing issues first hand. We also found that having more staff meetings would encourage personal ownership among employees.

We also found the following ideas to be beneficial in improving security awareness:

- Use the Hanford Reach to promote security
- Have an end of the day checklist
- Use eye-catching posters to spread the word.
- Have a security awareness week

By following our recommendations we believe that security awareness at PTH can be greatly improved. The focus should be to encourage commitment to security

issues in all employees. It is also important to determine on a limited budget how to use your resources effectively.

Table of Contents

Introduction.....	4
Topics Addressed.....	5
Industry Interviews.....	5
High-security Industry.....	5
Email Survey at Hanford.....	5
In-depth Interviews.....	5
Methodology.....	6
Industry Interviews.....	6
High-security Industry.....	6
Email Survey at Hanford.....	6
In-depth Interviews.....	6
Results.....	6
Industry Interviews.....	9
High-security Industry.....	10
In-depth Interviews.....	12
Email Survey at Hanford.....	11
Recommendations.....	18
HGET.....	20
Email and Website.....	20
Interpersonal Communications.....	22
Mass Media.....	23
References.....	25
Appendix A-Content Analysis.....	20
Appendix B- Industry Interviews from SE-SIG.....	28
Appendix C- Industry Interviews.....	43
Appendix D- In-depth Employee Interviews.....	48
Appendix E- ORISE web site excerpt.....	70
Appendix F- LLNL web site excerpt.....	72
Appendix G- Pictures from SE SIG.....	74

INTRODUCTION

Since its inception in the early 1940's Hanford security awareness program was made an integral part of security. The primary goal of security awareness is the reduction of security incidents through an alert work force. This goal is met when employees take an active part in security, which in turn reduces both the security threat and the number of security incidents. Currently, the Hanford site has a moderate security environment that was brought about as the Hanford mission changed its focus from that of producing nuclear material to one of environmental clean up.

To date, the Hanford site requires that all 14,000 employees wear badges. There are security guards that patrol the site frequently. They are also at the gates, and randomly search people's vehicles, which are entering the site, for prohibited articles. It is also very important that all doors are locked, computers are turned off when not in use, and that all classified information is locked away.

Mr. Chester Brawsell, head of security education and awareness at Project Technology Hanford (PTH), has an impressive security program. Mr. Braswell has made mouse pads with security messages. He also has a "security pays in many ways recognition" program. This is where employees get great prizes like blankets and Mag Lites for doing a good deed, like reminding people to wear their badges. There is also an Intranet "push-pull" program that is doing very good. This is where someone clicks on an ad and then it takes him or her to another spot having to do with security. The Security "ED" character is new at Hanford. This is a security cartoon character that is published in the Hanford Reach. "ED" was introduced in January of 2000, and has had some responses from employees. Employees are encouraged to send in ideas for "ED's" next appearance. There are many other things that Hanford is doing to improve their security awareness program.

The purpose of this marketing study was to determine three key issues. The first issue being to determine the strengths and weakness of the current security education and awareness program from a communications stand point. Second, recommend how the security education and awareness program might be enhanced to broaden its appeal and to improve project Hanford employee participation and security education and awareness initiatives. Thirdly, to establish a baseline of information that will provide measurements and meaningful conclusion so that management can then target specific areas for program emphasis.

Working with Mr. Braswell, we were trying to improve security awareness at Hanford. We, a group of Washington State University students, conducted research and interviews to determine what needed improvement in the security awareness program. First of all, this included determining what helped people take personal

ownership for security. Also we researched techniques of how to keep security updated and effective. We also were researching how to enhance employee training by improving the training programs available. It is also important to determine, on a limited budget, how to use resources carefully and effectively.

Throughout this project we determined that it is important to encourage employees to take personal ownership for security. The focus should be to encourage commitment and not compliance by all employees. When there are personal ties to these security programs, the benefits will greatly improve security awareness at the Hanford site.

TOPICS ADDRESSED

Our research that we conducted included industry interviews of similar facilities, industry interviews with other high security facilities, an email survey for Hanford employees, and in-depth interviews of Hanford employees. For industry interviews with similar facilities, we focused on these issues:

- What precautions were taken at the end of a workday (i.e doors locked, computers logged off)
- How security awareness is promoted
- Determining what security approaches were most and least effective
- Determining the influence that employees had on developing security programs
- What the repercussions of not wearing a badge
- If there were plans for future promotion of security awareness

When conducting our high security industry interviews we focused on these issues:

- What the level of security was at the facility
- How security department promoted employee obligations
- What communications methods did they find most useful
- What sorts of rewards and punishments did they have for encouraging security compliance
- How do they encourage their managers and employees to take ownership for security to take personal ownership for security issues

When conducting our email survey to the Hanford employees we focused on these issues:

- Determining the managers and employees level of their “security conscious” attitudes
- Determining if the amount and quality of security information is adequate
- Determining the most effect way to promote/communicate security ads
- Focus on what encourages employees to be security conscious
- How can the security awareness department improve employee involvement in and personal ownership for security issues

When conducting our in-depth interviews we focused on these issues:

- The most important and effective ways to promote security awareness
- If employees knew how to acquire security information
- Determine if employees know the procedures to keep Hanford secure (i.e. lock doors, and log off computers)
- What the employee's personal opinions were on improving and promoting security awareness

METHODOLOGY

The similar industry interviews took place at the SE SIG conference in Arlington, Virginia. Six people from various DOE sites around the country were interviewed. The six participants included Larry Wilcher, from the DOE; Gary Chidester, from the DOE; John Soy, from Bonneville Power Administration; Christina Hartley, from Wackenhut Services; Trent Olaveson, from Sandia National Laboratories; and Tracey Lamee, from Sandia National Laboratories. Various lectures on security issues were attended to obtain information on security awareness. The interviews were conducted during the breaks between lectures at the conference. The length of the interviews lasted between ten and twenty minutes.

The in-depth interviews with the high security facilities were conducted over the phone with four industries. The first interview, conducted with Gerald, the general security manager at Hewlett Packard, took approximately twenty minutes. The second interview with Tim, the security manager at Wafertech, lasted approximately twenty minutes. The third interview with Glen, the security coordinator at Linear Technologies in Camas, Washington, lasted ten minutes. The fourth interview with Travis, at Chemica Inc. in Bend, OR, lasted approximately fifteen minutes.

For the email surveys sent to Hanford employees a final version of the questions was placed on the Hanford website, 945 employees were asked to respond to the survey. 372 employees responded, a response rate of almost 40%. This data was put into an excel program and later analyzed by placing the information into graphs.

The in-depth employee surveys took place on the telephone. Eleven people were interviewed from the Hanford Site. The employee surveys lasted between 10 and 20 minutes.

RESULTS

Industry Analysis

Important Security Behaviors

When attending the SE SIG conference in Arlington, besides attending the lectures, management interviews were conducted. Many of the interviewed managers had similar ideas. When the managers were asked what type of precautions were taken at the end of a workday they had similar answers. Gary Chidester said, "There's an end of day checklist. Make sure that all containers secured/double checked, computers are turned off, disks are accounted for, copier is turned off, and all doors are locked." Larry Wilcher had similar procedures to Gary's plan. Larry said it was important to, "Make sure that all assets are locked- Second double-check everything. Make sure that the alarms are set. Individuals are responsible to insure that what they handle is secure on their computer. Every night all the computers must be off, even during the day when they're not using it." Everyone interviewed seemed to have some kind of a checklist or routine that they used to secure their office at the end of the day.

Common Mass Media

When the managers were asked how they build security awareness at their site they answered with a variety of different ways. Gary Chidester thought that the best way to build security awareness was through, "Visual education methods, posters, newsletters, individual meetings, and monthly news articles." Tracey Lamee had a different view she thought the best way was to do it through, "annual training. We do special briefings. There are many announcements on the net. It's a small site; we touch everyone." Trent Olvason thought that the best way to build security awareness was to have, "Visual education methods, posters, newsletters, individual meetings, monthly news articles." The most common ways are by posters, monthly news articles, staff meetings and email announcements.

Most Effective

The managers were also asked which security approaches were most effective and least effective. The managers had a wide range of effective security approaches. An end of the day checklist is a great way of reminding employees of the duties that must be done before leaving their office for the night. Christina Hartley said, "We have a poster contest. I think that this is most effective. We have a reward for the winner each month. It's usually like some kind of gift certificate to a restaurant or a department store. The winning poster is posted throughout the site." Larry Wilcher also had ideas similar to Christina's. He felt that the, "Most effective are the audio/visual aids that are used. Such as posters and videos. Media aids that promote new security problems work well." Gary Chidester thought that, "Briefing and debriefings are most effective. One-on-one is very effective. This is not always possible, but is most effective." Tracey Lamee also thought that one-on-one is the most effective. She felt that the people retained information better this way. Trent Olvasen also thought that briefings were very effective. He said that it's the most important because "it's an individual department with 15-30 people. When they are small like this, and everyone knows each other, they feel more comfortable and ask more questions." John Soy had a slightly different idea of what an effective security

approaches are. He felt that the, “Most important is to make employee see why it’s important. They have to buy into it; they have to see how security would effect their time. They need to see how it protects you.” It seems very effective to have interpersonal means of addressing security issues. People learn from one on one meetings, trainings, etc. They enjoy being interactive and employees do recall information they have learned first hand better than from posters or email. Although posters and emails do not work wonders at informing employees about security issues, they are good means of reminders.

Least Effective

The majority of the people all felt that the least effective way was computer-based training. Larry Wilcher said that, “A study was done at the DOE and less than 5% of people retained the computer aid information.” Gary Chidester also thought computer training was very ineffective because, “There are never any interactions.” Tracey Lamee also had similar feelings. She felt they were least effective because, “People hardly pay attention to them.” In conclusion, all the managers interviewed discouraged computer- based training.

The majority of the interviewed managers said that they try to include employees in developing security guidelines and procedures. Many of the managers said that they were open to employee suggestions. Trent Olvasen said that, “They (employees) have taken all site regulations to the line- made changes and came up with the Safeguards and Security Guide from A-Z, a book of security procedures.” The interviewed managers felt that it is important to consider the employees feedback.

Enforcement

The security managers seemed to have different procedures if someone failed to wear a badge on site. John Soy said, “There isn’t really a penalty yet. The security guards check to see if people are wearing them. There is minimal classified information here.” On the other hand Christina Hartley said that, “The employee is taken off the site, if they don’t have a badge. YOU MUST HAVE A BADGE!” Larry Wilcher also had a procedure that his site followed, “First you will get warned if you don’t have a badge. It must be visible at all times. If it becomes a problem it’s reported to their supervisor. Then there are also infraction programs. Its kept on their record, and three infractions in twelve months can lead to suspension.” The majority of the managers had some kind of procedure, which usually lead to an infraction.

Security Awareness

Some of the managers had plans for promotion of security awareness. Christina Hartley said that, “We are going to start more self-assessments; everyone is required to participate in a yearly trade show, where ideas are exchanged.” Gary Chidester said that his site was, “starting to have security awareness meetings by

telephonic conferences. We have an annual security refresher. We are also having more briefing and debriefings.” Trent Olvasen said that he was starting to do the S.S.I.M.S. (safeguard security informant management systems) program. Larry Wilcher’s site “Was working on a new security awareness internet based project. Themes people like, for example: Alice in Wonderland. The ISM (integrated security management) is also implementing a new policy; if you didn’t do this, then what would you do?” There are many new security awareness ideas surfacing.

High Security Facilities Analysis

Effective Security Strategies

When studying similar industries such as Hewlett Packard, Linear Technologies, Wafertech and Chemica Inc., a few key issues kept coming up. First of all, the security departments promote employee obligations by encouraging employees to work as a team. If employees work together with the security guards the sites will be more secure. The staff needs to take security personally. The Hewlett Packard general security manager, Gerald, stressed the importance of making security a “team effort.” If employees feel like the security is a group effort, the individual will pay more attention to the negatives and positives of their security situation. Communication is also important. Along with being a team effort, employees like hearing news first hand. When implementing new ideas and rules, a meeting should be held. The focus should be on keeping employees feeling included in the process. If security is not discussed on a regular basis, it will be forgotten and not taken seriously, until a theft or problem occurs and it will be too late.

Most Effective

The most effective communication method by most facilities seems to be direct communication, i.e. phone calls and department meetings. However, it is understood that this is not always possible and in those cases, advertisements over the web site are effective. It is important to keep these updated to insure users they are getting the most recent information, or again, they will feel left out of the loop, and not feel the need to take security personally and seriously. This is when the system fails and we lose participation of the employees. Poster advertisements and frequently updated bulletin boards are good ways of reminding employees to keep security a priority, however, they are not proven very effective in educating or promoting security awareness. As Travis Bodeutsch, from Chemica Inc. put it, “If an email is sent to employees and then brought up and discussed at the company meeting, there is generally a high degree of responsiveness.” The emails, posters, and flyers on bulletin boards will always prove more effective, when they are discussed first hand with employees. Employees should be kept updated on the newest security information.

Enforcement

It was determined that all high security sites feel security guards are an important asset. Having uniformed and undercover guards patrol the sites makes employees more comfortable and helps prevent theft. Another important issue is having nametags or badges mandatory at all times by all employees.

Security guards and wearing badges walk hand in hand to make employees take personal ownership for security. If an employee sees a person wandering the facility without a badge, it is their responsibility to inquire about it. If the site rarely has theft issues, then to keep employees on their toes, there should be random badge checks where an undercover security officer walks with no badge with hopes that employees will stop him. To make employees more security conscious, offer them something from the following list, or similar to this, for taking the time to stop that officer.

- Free lunch ticket
- Sports tickets
- T-shirt
- Basketball/Volleyball
- Gift Certificate
- Starbucks gift certificate

It has also proven effective to have security guards do random vehicle checks. Guards at the gates can lower the chances of an unmarked vehicle getting through, and check to make sure that the vehicles don't have any restricted items in them.

In-Depth Interviews with Hanford Employees

When interviewing various non-management Hanford employees many trends were seen. The majority of the employees knew where to go for help when they had security issues. Some of the new Hanford employees were unsure about what the security department consisted of. One employee, who has worked at Hanford for ten months, was unaware that there even was a security awareness program; although he said he did know how to reach the Hanford Patrol. Many employees had mixed feelings about what was effective security awareness. Some felt that monthly presentation and safety meetings were very effective, while others felt that this was ineffective. The majority of the employees felt that security reminders via email was the most effective way to receive security notices. Even though this seems to be effective, it would probably get a higher response rate, if the issues were discussed at a meeting of some sort while question could be asked and answered. A simple email reminder alone may be too easily overlooked. Discussions would initiate recall of these issues, making them better understood and effective.

Finding Security Information

When the issue about knowing where to look or ask about security concerns came up, the majority of the interviewed employees all felt that the best way was to either look on the security website, or ask their supervisor. One employee said, "You can either call security or ask your manager. There are also security cars patrolling quite frequently. For the quickest access I would look on the security website." Other employees felt that the web site could be updated. Another Hanford employee felt

that, “an update of the web page would allow quicker access. An email address where you could ask a specific question and get a quick response would be very helpful.” Also, the community wide ‘security 911’ seems effective to most of the employees. The direct phone number to a security officer is a quick and effective way to get questions answered and issues taken care of.

Daily Duties

The majority of the employees said that making sure everyone had a badge on was one of the best ways to keep Hanford secure. Also keeping computers off when not in use was very important. An employee felt that, “You must always keep your eyes open. If you see someone with out his or her security badge on, report it to your supervisor immediately. Make sure that doors are always secure. When you leave your office make sure that your computer is off.”

Taking Personal Ownership

When the employees were asked what makes them take ownership for security there was a variety of answers. Some people felt that it was because of peer pressure and peer acceptance, like for example if an employee saw someone with out a badge they have to report it, even if it was a friend. However, this could also be a bad situation. Nobody wants to turn in a friend on a situation that will not harm anyone. It may be difficult to get an employee to turn in a friend, especially if they see no harm being done, by the employee (friend) not wearing a badge. One employee thought that, “It is kind of embedded in training. We are always being made aware of it... its kind of subliminal. They are natural everyday habits at work.” Most employees felt that questioning an unbadged wanderer was important. However, not every not always questions the wanderer. Many thought a reward system of some sort would be effective in enhancing the chances of employees confronting the unbadged person. It is also important to have undercover security officers wander the halls to survey who may need more training in stopping an unbadged individual. If nobody stops an unbadged person, the reason is most likely because they are not trained in the steps to take, or else they are not taking personal responsibility for security on the side. Personal ownership must be encouraged.

Receiving Security Reminders

There are many different ideas employees recommended to increase personal awareness of security amongst their co-workers. Some people felt that updating the security website more often would be helpful. People also felt that having more security posters around the site would be nice. One man felt that a Q & A section on the security website, where you could ask a question and get a reply. Then take the questions that have already been asked and post those answers on a message board. One employee said, “When people are caught violating the rules, we don’t hear about it. It would be nice if they could somehow start telling us when things happened where someone didn’t follow the rules.”

Employee Ideas

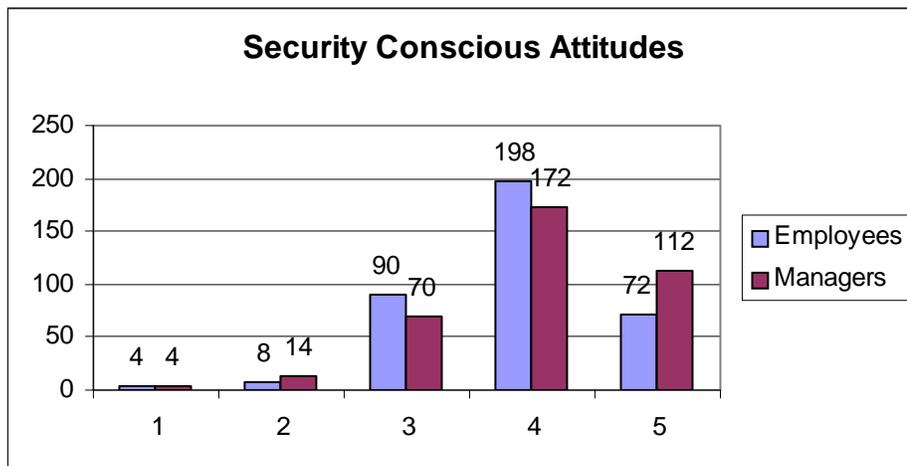
When the employees were asked about ways they could think of to increase ownership among co-workers they had many ideas to share. An employee thought that, “Email reminders would be a good way to increase personal responsibility. More posters posted around the building would be nice. The Hanford reach does a good job in promoting security, and it is read quite often. The cartoon they use is funny and it catches the eye, so to continue using that source would help also.” Another employee said, “It would be nice if security would give you free stuff-mouse pads, magnets, and calendars, things that you use every day. Advertisements... coffee mugs, and key rings would also be nice. The Hanford Reach does a good job. They have a cartoon that is very funny. I can’t think of programs that are more beneficial than they already have. You could talk about security issues in monthly meetings.” Promotional marketing items seem to be a way of advertisement that many employees like.

Email Survey of Hanford Employees

With almost a 40% response rate to the email survey that was sent to Hanford employees, a great deal of information and ideas were received.

Enhancing Manager/Employee “security consciousness”

The graph below illustrates the results from the question, “Employees/Managers that I’ve observed have a ‘security conscious’ attitude. 1=Not very, 5= Very conscious; 5 is ideal. The average rating for employees was 3.88 and the average rating for managers was 3.99.



After analyzing the data in an excel program, we determined that a lot of attention should be given to enhancing the “security conscious” attitude of both employees and managers. (See chart above.) Maybe the lack of team effort or unity, has contributed to this problem. This graph also shows that security managers are more security conscious, therefore it shows that managers have slightly greater ownership. This indicates that managers care more about security. Ideally the rating should be a five, but currently it was rated at a high three. Security issues are probably not discussed as much as they should be. To get managers and employees to contribute, security must be seen as an important issue and discussed regularly at meetings and training sessions. Employees should be asking more questions, and managers either answering them, or finding the answers. The most effective way to make this happen is to discuss them at group functions.

Who’s Most Responsible?

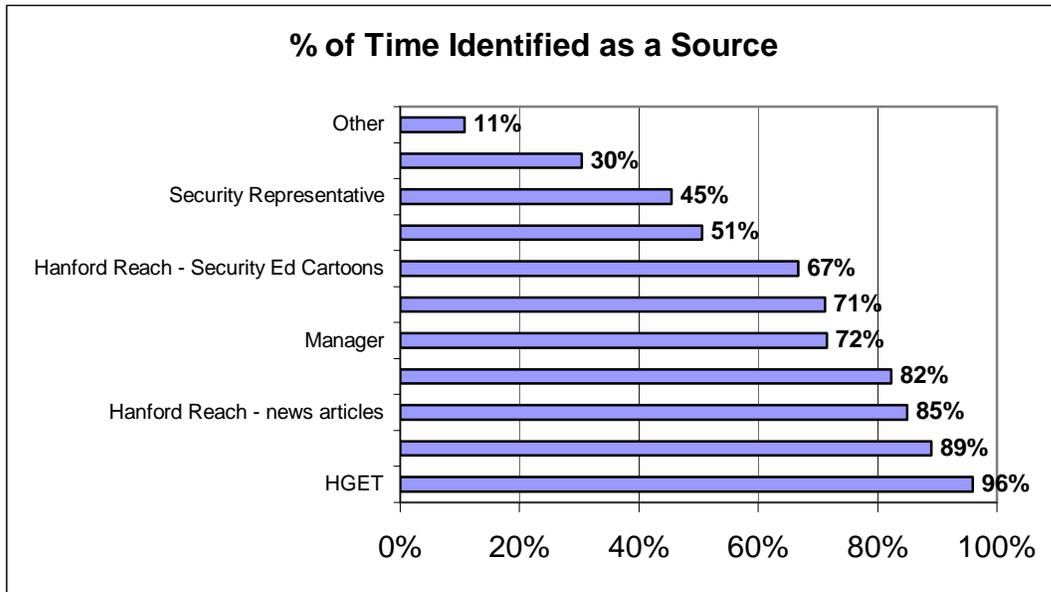
Employees were asked the question, “Who is most responsible for security in their work area?” The highest rated response was “Me” with an average of 4.21, on a scale from one to five. Second was manager with 3.55. The third was security with a 3.11 average. The fourth was the senior leader with a 2.7 average. The fifth was the security education office with a 2.32 average. From the data that was received, it is encouraging to note that on a scale of being most responsible for security in their work area, the majority of employees said that it is their responsibility to know security issues. About 275 of the 372 employees interviews said that it was their responsibility, above anyone else’s, to take security seriously. Second being their immediate supervisor/manager. It is good news that employees know that it is their responsibility, above anyone else’s, to find out about security issues. The next step is encouraging them to be active in this role. That is where discussing the issues in groups will be effective.

Are Amounts and Quality of Information Satisfactory?

Employees were asked the question, “Are the amount and quality of security information adequate?” On a scale of one to five, quality was rated 3.29, with one being low quality and five being high quality. The amount of security information was rated at an average of 3.54, with one being not enough information, and five being too much information. It appears that employees feel like they are receiving enough information, but that it could be of higher quality. Its possible that mass media doesn’t impact behavior. Using posters or promotional items may be something that is appealing to an employee, but it may not impact their behavior. Using interpersonal communication instead may improve the quality of information the employees receive because it more one-on-one. Maybe employees have become complacent with their position in security issues. Something needs to be done to jump start them and get them involved again with security awareness.

Communication Methods: How do Employees Receive Information?

It has been determined that employees receive their security information from the following sources. The survey question asked, “I have obtained or have seen security awareness information from this communication source. Check all that apply.”

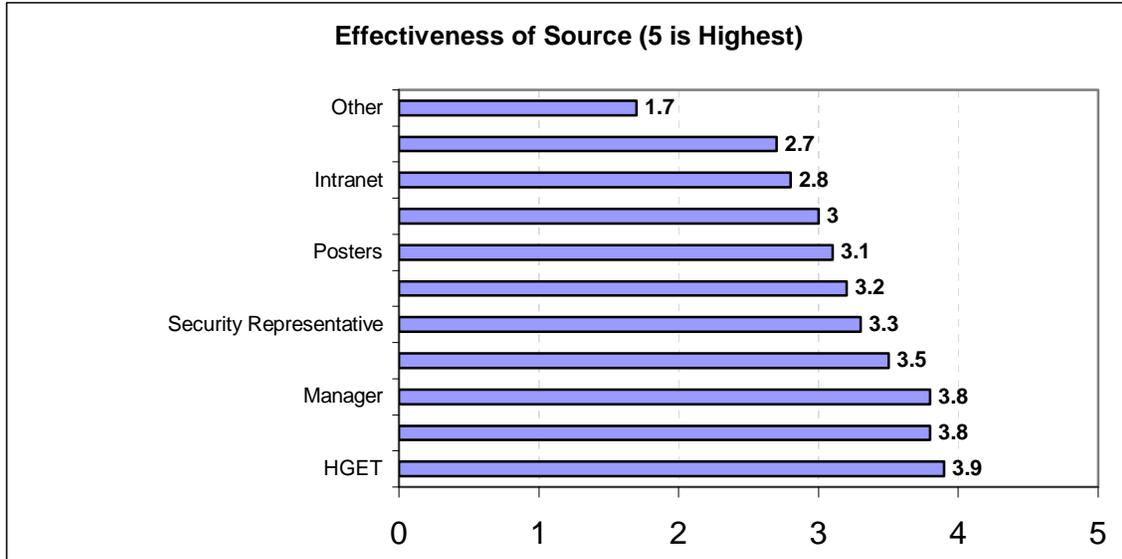


HGET, followed by Email, Hanford Reach-news articles, posters, management and Staff meetings were the top six on the list. Followed by Hanford Reach-Security Ed, intranet, security representatives, promotional items and other.

The first eight of these sources were used by over 50% of the respondents, indicating that the top 8 are remembered as promotional security awareness. However, it is important to point out that although a source may be seen, it does not necessarily mean it is effective. It is possible to see a poster, which may remind someone of the importance of security, however, it does not teach or educate on security issues. A security advertisement may be seen or experienced by an employee, but it does not mean that the source is effective.

Communication Methods: Most Effective Sources

On average, employees rated the following in order of most effective to least effective in advertising. The email question was stated, “How effective are these communication methods? 1 being not effective and 5 being very effective.”

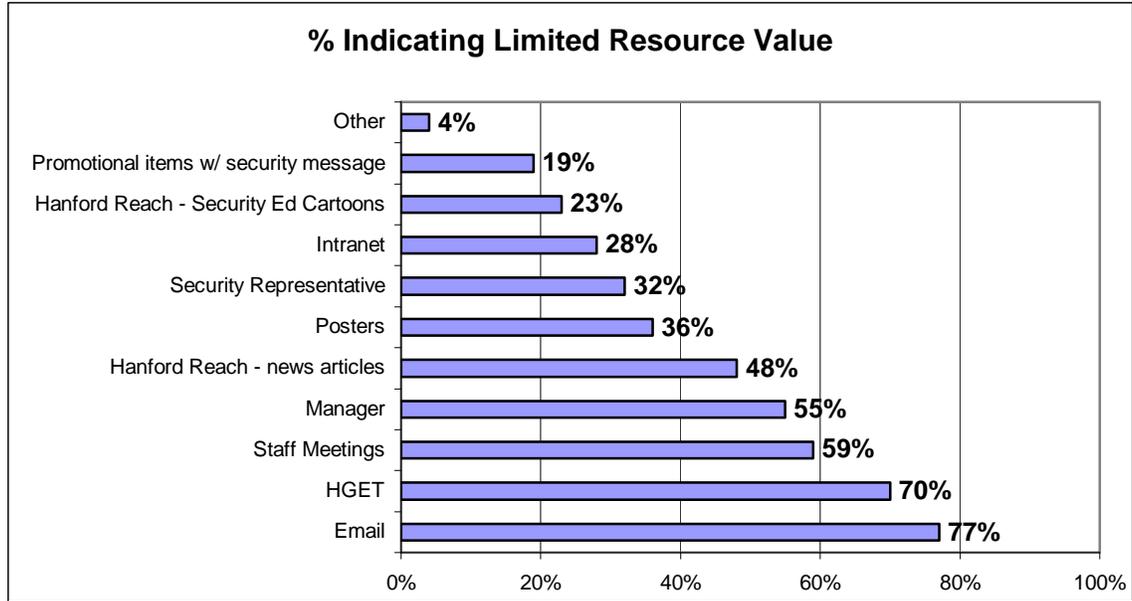


Top of the list was HGET, followed by Email, management, staff meetings, security representatives and Hanford Reach-news articles. Followed by Posters, Hanford Reach-security Ed, intranet, promotional items, and other.

In comparing the above two graphs, HGET and Email were rated the top two. Management moved up from being rated as fifth in the percentage of time used as a source to the third most effective source in the second graph above. Posters were rated fourth in the percentage of time used as a source, where it was rated seventh as an effective source. Posters, Hanford Reach and Security Ed moved down in rank. Even though these are well known, they may not necessarily be the most effective. This indicates that interpersonal methods are more effective than mass media. From these two graphs it appears interpersonal methods are viewed as very effective, but underused. Increasing interpersonal methods of communication will likely increase perceived quality, while not increasing perceptions that too much information is being provided. This addresses the concerns raised by the questions regarding the amount and quality of information provided.

Using Limited Resources

When employees were asked the question, “With limited resources, which of these communication methods would you use? Check all that apply,” the results were as follows.



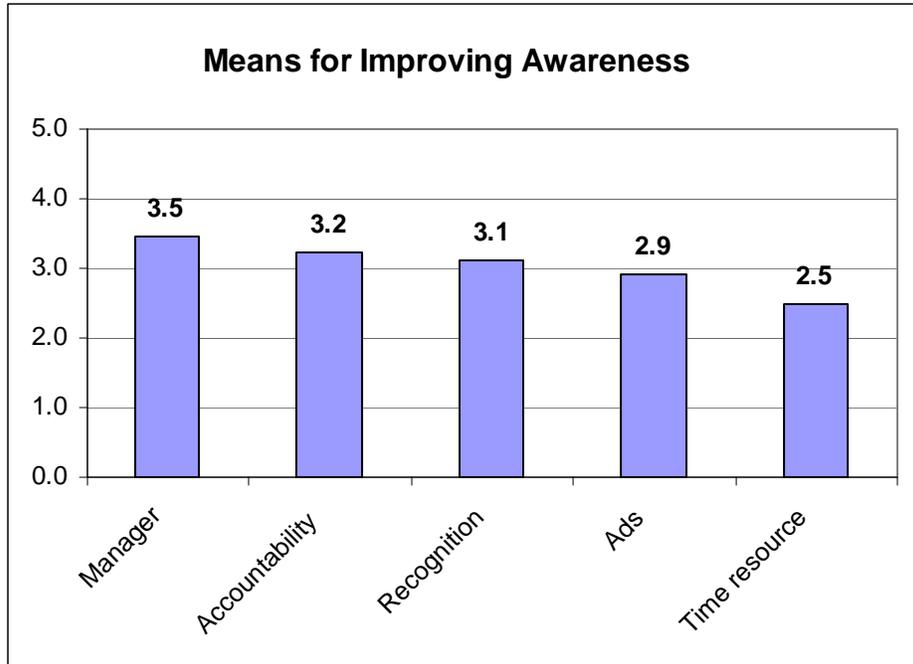
The top of the list was Email, followed by HGET, Staff Meetings, Management, Hanford Reach-news articles, and posters. The next five were Security Representative, Intranet, Hanford Reach-Security Ed, Promotional items with security message and other.

Of the communication methods above, six methods were consistently among the top of the list. They included HGET, Email, Management, Hanford Reach-news articles, Staff meetings and Posters. From the high number of employees that ranked these as influential, leads us to believe they must be kept up.

Interpersonal methods such as staff meetings and managers were rated high. Using these methods doesn't require a high budget. Security representatives were rated less, which doesn't mean that they are not effective, but that it is costly to have a security staff. Overall email was the highest, which means this should always be used and that employees see it as both effective, and cost effective. HGET was also rated as high, because it is a mandatory security educational requirement.

Employee Security Consciousness

The results from the email survey question, "In your opinion, what would improve Hanford employees security consciousness? Rank from one to five; one being least important and five being most important."

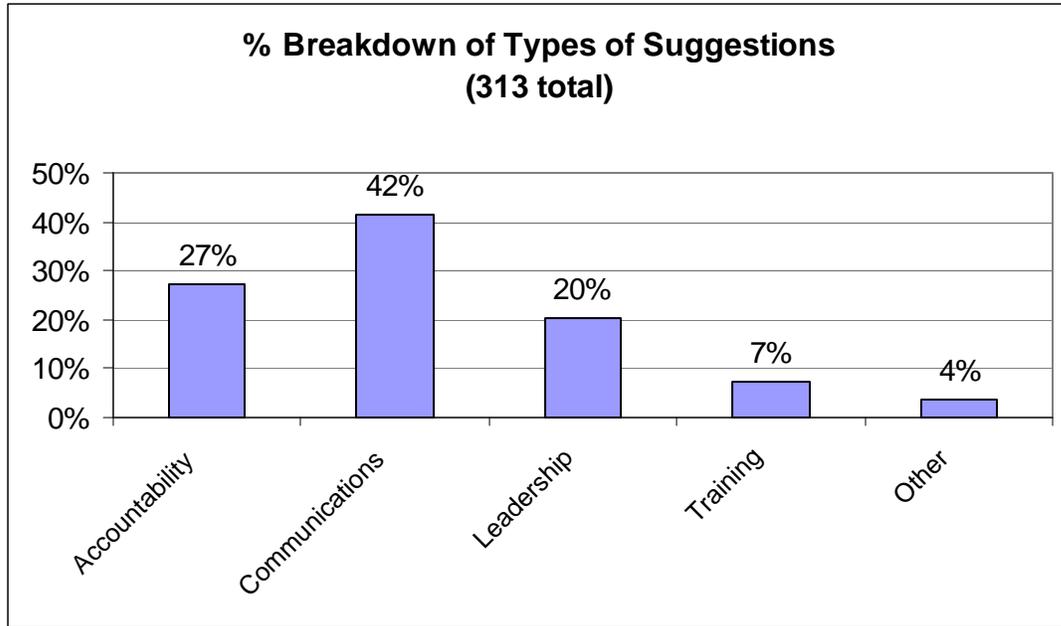


Management was rated high as well as accountability and recognition. This indicates that employees like interpersonal means of security education.

Management was rated most important in improving security awareness. Management involvement is an interpersonal, effective method of keeping security issues fresh in employees' minds. Accountability, meaning discussing and making known the issues that occur on site, was also rated highly. Employees enjoy hearing when something goes wrong, what the consequences were to the individual at fault, and how security will be improved because of it. Recognition, meaning rewards and benefits, is also an interpersonal method of improving awareness. Everyone can enjoy rewards for jobs well done. Movie tickets or a t-shirt are great rewards. Advertisements were rated low, as well as time resources.

Employee Ideas

When employees were asked the open ended question, "How can (or should) the security awareness department improve employee involvement in and personal ownership for security issues" the following chart displays the breakdown of the 313 total responses.



This chart supports the idea that interpersonal communication of security issues works better than individual education, such as computer-based education or email awareness.

Accountability involves that employees are held accountable for their actions while on site and the consequences of a bad decision or action may be made available to the public. Communications would include improving the methods of advertising security issues. Leadership includes management acting as role models. Training is programs such as HGET, and security meetings. A variety of comments fell under the category other.

Recommendations

The table below helps distinguish the differences in the four categories of data gathered. The four different methods of collecting data were the employees who were interviewed over the phone; the managers (experts) interviewed at the SE SIG, the email survey of employees, and the company/other high-security facilities. The table compared the similarities and differences of enforcement used at their facility, how ownership was increased, key behaviors that were used by employees to increase security, and what the most effective and least effective methods were for increasing security awareness.

	Employee	Manager (Experts) from SE-SIG	Email Survey	Company/Industry
Enforcement	Warning	Infraction	Accountability	Supervisor notification
Increasing Ownership	Peer pressure	Visuals, one-on-one	Communications; HGET, email	Work as a team
Key Behaviors	Lock doors, turn computers off	End of the day check list	Wear badge, computer security	Lock doors, turn computers off
Most Effective	Email, interpersonal	One-on-one	HGET, email, interpersonal	Bulletin boards
Least Effective	Yearly updates	Computer training	Promotional items	Promotional items

In comparing our results, there were many similarities and some that were a little conflicting. There were mixed results on what was the most effective. The employee interview and the survey both showed that email was most effective though. The survey and the company both agreed that promotional items were ineffective. There was a consensus on key behaviors. Three of the fields felt that lock doors, turn off computers, etc was most critical. All four fields also agreed that some type of warning had to be enforced for not wearing your badge. The survey basically complied with the other research methods. Having an email survey would be a good way to measure what needs to be changed or improved in the future. Comparing our results in a table also captures a big picture of what is being done and how other sites are doing things the same or differently. The table also complies with our recommendations, using one-on-one communication, having an end of the day checklist, using email more, etc. This also shows that personal communication is a better way to go, such as using one-on-one. Using mass media such as computer training was shown to be less effective.

When trying to improve security there are some important issues that need to be remembered. Jon C. Todd, Chief, Office of Defense Nuclear Security, had some very important issues that security personnel must consider:

- Security must make sense
 - Employees will implement if they know “why” requirements
 - Employees must be provided the opportunity for feedback
 - All employees impacted must have an opportunity to participate in security
 - Management must listen to feed back
-
- **WORK AS A TEAM**
 - No-one individual has all the answers

- Different sites have different views
- Want integrated approach to security
- Must get out of the “Us” vs. “Them”
- Accept responsibility and move on
- “Education of employee first”

All of these ideas that Jon Todd discussed are important to give thought to. These are the ideas that need to be implemented in order to have an efficient security team. These are common themes that managers need to be reminded of frequently, so they will apply them toward their employees. Discussing them at meetings, and even having posters could implement these suggestions.

Through the research for Hanford security awareness that we conducted, we concluded that it is important to include all employees when passing the word on new issues. It must be a group effort to get the best response by employees. If security management tries implementing a new rule, or a new reward system, or something of the like, it is important to discuss this first hand with all employees at the site. When employees begin feeling left out, they lose interest and personal ownership for security at the site goes down. It is important to instill in their minds the need for security. It should be in the back of their minds at all times that security is a top priority. This is recommended by managers at other high security facilities, as well as by managers at the SE SIG conference in Virginia. The following recommendations should help in determining how the security education and awareness program might be enhanced to broaden its appeal and to improve project Hanford employee participation and security education and awareness initiatives.

Based on what the table above showed was the most effective way to improve security awareness, and analyzing all of the data collected, we concluded with three major recommendations. The first being HGET, then email, and interpersonal communications.

HGET

HGET was ranked quite high in the email survey, although a study done by the DOE showed that less than five percent of people retained computer aid information. This is something that should continue being used, because employees felt it was effective, but shouldn't be depended upon, considering the results of the DOE survey.

Email and Website

Email was ranked as being very effective in the email survey, as well as in the phone interviews with employees. Email is also an inexpensive way to get the word out to everyone quickly. This is also something that the majority of employees check on a daily basis. According to the email survey done at Hanford, employees

realize that it is their responsibility, above anyone else's, to find out about security issues. It must be important then, to have resources available and easy to retrieve. Email and the Intranet are a good way to make them available. The key is to encourage them to be active in their role to find answers, and understanding the importance of security awareness.

- Send Security "ED" reminders via email. There were some conflicting results about Security "ED." The email survey showed that "ED" did not rate high in promoting security, while the phone interviewed employees thought "ED" rated high. Security "ED" could be a more effective way of promoting security if it was sent through emails, which proved to be an effective way of receiving security information. People seem to really like "ED". Having "ED" cartoons sent out via email might be a better communication method, versus the Hanford Reach.
- Send end of the day checklists via email. This is also a way to improve security awareness. It is important that everyone develops a routine at the end of the day. It could also consist of note pads with checklists already printed in them. Then all the employee would have to do at the end of the day would be to look at the checklist and mark off each task he or she does before going home for the day. Or if it was sent through email, or used as a site wide screen saver, all the employee would have to do would be to look at his or her computer screen.
- Use email to distribute daily security news. Some of the employees felt that they should know about when something security related has happened. Having stories of security events that took place that day would be interesting to the employee. An email could be sent out to employees using real life examples of security violations. For example, an email could be sent saying, "A Hanford employee forgot to take his bow and arrow out of the trunk from a hunting trip, and brought it on the site. During hunting season make sure all of your weapons stay at home." Or "An employee brought a propane tank on to the site today. Remember to leave your propane tanks in the back yard during barbeque season." Emailing these kinds of real life examples would be beneficial, and then if employees had any questions about it, it could be emailed to a security officer.
- Using email to distribute articles from the Hanford reach would also be very effective. There were conflicting results about the Hanford Reach. The Reach could be a way to promote security, but the email survey showed that it wasn't very effective. On the other hand, the phone interviews showed that it was effective and that people were reading it. The newspaper could be an effective way of passing the word on new implementations, because once a person hears the news, it will be spread by word-of-mouth, but according to the email survey, this paper isn't read by many people. If there were impacting articles taken from the Reach and emailed to employees the rate of reading may be higher, especially if they sound interesting, or are "late breaking news." Employees may be more curious about that and open the email, rather than pick up a copy of the paper.

- Continue sending out the advertisements on the Intranet and via email, but be sure they are updated and interesting. Old news is not news at all, and old news that continuously makes it on the website will make people give up using it as a source because they always find the same thing when they are searching for news. It is important to keep employees updated on the newest issues and rules of security, which could be sent via email. The bulletin boards where numbers, posters and ideas are posted should also be kept updated. Many employees use this source for information regarding security.
- The employees also liked the idea of sending and receiving emails. It would be nice if the website had a place to send and receive questions. The help area on the website could be labeled something such as “Safeguard & Security”.
- Have a well up-dated web site. Doing this is an excellent way to spread security information. People are sitting behind computers all day long. It is a quick reference for them to use if they have security questions. Many other security facilities use web sites. ORISE, Oak Ridge Institute for Science and Education, has a web site that has an area that focuses on employee health and safety. This includes areas that deal with the Center for Human Reliability Studies, such as work place violence prevention and personal security; environment, safety and health groups, and medical education and outreach programs (See Appendix E). The LLNL, Lawrence Livermore National Laboratories, website had a very updated security website. It had a page that had all the new security tools you could order like an Internet scanner and a safe patch. It also had a very informational section that had information about policies, procedures, new training programs, and who to contact about security. (See Appendix F). We also looked at the Pantex website, the Kansas City Plant web site, and the Bonneville Power Administration web site, but was unable to locate a section in their sites having to do with security.

Interpersonal Communications

Our results showed that interpersonal communication methods were very effective. Manager at the SE-SIG meeting ranked staff meeting and managers very high in the email survey, and also. Using small group or one-on-one communications makes the employee feel more important.

- Have weekly staff meetings. There are many ways to pass the news first hand. The most effective would be at weekly meetings. Make security awareness a priority at meetings. Discussing issues of importance that will encourage questions and discussions that will teach all employees and keep the issues fresh in their minds year round. When employees have a chance to reflect and give ideas at meetings such as these, they feel involved, included, and like important decision makers, creating personal ownership for these issues. As a result of these meetings, they will be more aware of the importance of security when they are back at their offices or cubicles. At these meetings, employees should be encouraged to ask questions, initiate discussions, and managers should be searching out answers if

they don't know them. The meetings should not be passive. They need to encourage interaction and interest in the issues.

- Have security management discuss the issues with department managers and then have those managers discuss the issues at weekly meetings with just their department. This may be an even more effective method of passing information because people in small departments will be more likely to ask questions, also, these questions could be better directed at serving their department effectively. Each department has specific needs, and these needs can be met better by addressing them at small meetings.
- Work one-on-one with employees. It is hard to do this with such a big company, but people will feel included if the security department can touch everyone. This could be having department managers have individual meetings with the employee to praise him/her and discuss new security issues. New employee orientation is a good time for this to can happen from the interview in Arlington.

Mass Media

There were many mass media ideas seen at the SE-SIG. Mass media ranked low on the email survey. Mass media was not very effective to Hanford employees. If Hanford did want to continue using mass media, some recommendations were concluded from our SE-SIG surveys.

- Poster contests are a good way to get employees involved, especially if there is some type of reward offered every month. Posters contests get employees to think about what security means to them and how they view and then they get to create it on paper.
- Hold a security awareness day. Doing this several times over the year could also be effective. The surveys conducted tended to show that more repetitive, frequent activities were effective, and less frequent, yearly activities were not very effective. Holding a security awareness day would only be effective if it was frequent, like once or twice a month. This could be formatted out where it could focus on a different department each time. The chosen department could plan an open house for the other employees, where they could receive funding for this through the security department. Then the security department wouldn't have to worry about planning it, because the chosen department would.
- Hanford could also produce a video about security awareness. It would be interesting if Hanford could produce a series of very short videos with really simple messages, which managers could use as a support item at their meetings, so Mr. Braswell wouldn't have to be everywhere at once. Hanford could maybe even get the DOE to share the cost of producing the videos. The video could demonstrate prohibited items. A video that is repetitive, shown in segments, and gives many examples of security do's and don'ts could be very effective. It would be fun

though to bring “ED” to life. Security “ED” is a character that many Hanford employees recognize as being security conscious.

- Use the bulletin boards in the buildings. Employee phone interviews show that this is very effective. People go there for answers and phone numbers for information on their questions. It is also inexpensive, and could be updated weekly. The bulletin boards could also be placed where employees like to hang out, like in their employee break room.
- Promotional items were not rated high in the email survey, but could be effective in specific circumstances. They could emphasize a specific thing, such as an end of the day checklist. It would be effective, if promotional items were to be used, to have them directly related to an employee as some kind of reward. Offer rewards for good behavior in security issues. If an employee stops an unbadged officer, give them a free lunch ticket or a mouse pad with an end of the day checklist on it. Word will pass like wild fire that an employee received this award, and it enhances the chance of others in the area to do the same behavior. And, it’s not necessary to always give rewards, but just enough to make it known to employees that often times, rewards are involved. It is human nature to go above and beyond the call of duty if rewards are involved.

These recommendations were developed based on collecting four fields of data, which included an email survey sent to Hanford employees, attending the SE-SIG in Arlington, conducting in-depth phone interviews with Hanford employees, and also conducting in-depth phone interviews with other similar high security facilities. The actual data collected appears in appendices. We encourage you to read those.

References

The majority of data came from interviews. The interviewed managers from similar industries were:

Larry Wilcher- U.S. DOE

Tracy Lamee - Sandia National Laboratories

Trent Olvaeson- Sandia National Laboratories

John Soy- Bonneville Power Administration

Christina Hartley- Wackenhut Services, Inc.

Gary Chidester- U.S. DOE

The interviewed managers from other high security industries were:

Glen- Linear Technologies

Tim- Wafertech

Travis- Chemica

Gerald- Hewlett Packard

The employee's interviewed in depth were:

Lynn Adams

Henry Booth

Daniel Coffeland

Gail Chaffee

Toni Lauricella

Bobby Baker

Steven Cantrell

Mryna Sills

Carol Meader

Bruce LaRue

We also got a large portion of data from the 375 employees who filled out our email survey.

Some of the information also came from other security web sites:

www.ornl.gov/orise.htm

http://www.llnl.gov/OCM/Computer_Security.html

Appendix A

Content Analysis

The purpose of the content analysis is to evaluate the messages used to communicate security awareness at Hanford. The review was information provided by Mr. Braswell and other security facilities around the U.S. This included recent samples of materials being used at Hanford such as, Security “ED” cartoons and DOE posters. The materials from sites around the U.S. were gathered at the SE SIG conference in Arlington, VA.

We, Washington State University students, analyzed the following items and reached a general consensus on our observations.

Communication Strengths:

Posters:

(these ideas were gathered in Arlington)

Security Posters are a good way to promote security. The majority of the posters observed in Arlington were eye catchers. One poster had a picture of a family with the caption “Security means protecting what matters most.” This poster has an emotional effect on the viewer. Another poster had big words that said, “Security.... Just DO It.” We felt that this wasn’t very original because it was imitating the Nike slogan. One poster had a leprechaun with a pot of gold that said, “Security depends on more than just luck.” This poster was very creative and colorful. There were many posters with cartoons on them, which seemed to be more of an eye catcher. Even though these posters are positive, it doesn’t mean that they are effective.

Security Posters are a good way to promote security. In the 70’s and 80’s security posters played a significant role in bringing security awareness to Hanford employees. There was not as much in the 90’s due to the lack of funding. The main purpose of the security posters is to promote strong security awareness at Hanford. The posters use cartoon characters to address security themes like, “Access control,” and “wear your badge.” We feel that the reason why they use these cartoons is because people are more likely to read them. Hanford has even used famous cartoons to promote security like Charlie Brown. There was also a DOE poster used at Hanford. It had a picture of a suitcase with a passport and the caption, “Include counterintelligence and security in your foreign travel plans.” We liked this idea, but the picture on the poster was really outdated. We didn’t even notice it at first, because it wasn’t very eye appealing, but it did have a good message.

Promotional items/gifts:

Mr. Braswell has a variety of promotional gifts. These range from fleece blankets to personal alarms. These gifts are very useful and beneficial. There were also many promotional items collected in Arlington from different sites. The Kansas City Plant had a large assortment of promotional items. They were all useful. KCP had flashlight key chains, pens, sewing kits, mouse pads, name badge necklaces, and even Shout wipes. These are items that employees could use every day. Mr. Braswell also gives mouse pads to employees. They were higher quality than the KCP mouse pads. Mr. Braswell uses a photograph of some people working at the tank farms at night. This shows how dedicated Hanford employees are and that they take pride in their work.

Rewards for security behaviors:

Mr. Braswell has also made it part of the security awareness program to give rewards for people when they show positive security behaviors. The gifts that employees receive are high quality, which include fleece blankets, personal alarms, leathermans, and Mag Lites. These gifts provide an incentive to display positive security behaviors.

Hanford Reach:

Another security promotion is Security "ED". Security "ED" is a funny cartoon that Hanford uses to remind people of security awareness. It uses themes like "don't forget to lock your doors" and remember to wear your badge at all times." Security "ED" is also published in the Hanford Reach, a local Tri-Cities newspaper.

Conclusions:

This content analysis concludes that positive messages are perceived when programs:

- Keep messages simple
- Use an incentive to promote good behaviors
- Send a message that workers will value

Most of the posters used (in Arlington) relied on a more intellectual approach, rather than one that used more of an emotional appeal. The content analysis did not review the articles used in the Reach, only the Security "ED" cartoons. By reviewing these materials we have a better understanding now of how promotional materials can initiate compliance and positive security behaviors.

Appendix B

INDUSTRY INTERVIEW WITH SIMILAR FACILITY

INDUSTRY EXPERT/CUSTOMER INTERVIEWEE INFORMATION		
Name:	Company:	Title:
Segment Designation:	Company Type:	
Address:	Telephone: (Email:
INTERVIEWER INFORMATION		
Interviewer:	Consent:	Interview Date/Duration:
INTERVIEW SUMMARY		
<p>Interviewee Issues:</p> <ul style="list-style-type: none"> • Note the general attitude of the employees toward security • Determine where the manager sees problems, and the employees • Determine what is effective in getting the security message across. • What are the consequences of a security failure? • What does the manager need to get employees to be more security minded? 		

INTERVIEW DETAILS	
Question 1:	Where are you from? What is your position? How many years have you been there?
Reply:	•
Question 2:	What precautions are taken at the end of the day? (Locked doors, computers logged off)
Reply:	•
Question 3:	How do you build security awareness? In other words how is it promoted?

Reply:	
Question 4:	What approaches are most effective? Why? Which are least effective? Why?
Reply:	<ul style="list-style-type: none">•
Question 5:	Have employees ever been involved in the process of developing security procedures and or guidelines?
Reply:	<ul style="list-style-type: none">•
Question 6:	I know that requiring badges to be worn is common practice at DOE facilities; is this correct? What are the consequences for failing to wear a badge? Is this a common problem?
Reply:	<ul style="list-style-type: none">•
Question 7:	Are there any plans for future promotion of security awareness (in-progress)? Is there anything that you'd like to try but haven't been able to this far?
Reply:	<ul style="list-style-type: none">•

INDUSTRY EXPERT/CUSTOMER INTERVIEWEE INFORMATION			
Name:	Gary Chidester	Company:	U.S. DOE Title: Office of C.I.
Segment Designation:	Management	Company Type:	Security Awareness
Address:		Telephone:	(202) 586-0254 Email: Gary.chidester@cn.doe.gov
INTERVIEWER INFORMATION			
Interviewer:	Beth Klinski	Consent:	Industry Interview Date/Duration: 4/09/01 15 minutes
INTERVIEW SUMMARY			
Interviewee Issues:			
<ul style="list-style-type: none"> • Note the general attitude of the employees toward security • Determine where the manager sees problems, and the employees • Determine what is effective in getting the security message across. • What are the consequences of a security failure? • What does the manager need to get employees to be more security minded? 			

INTERVIEW DETAILS	
Question 1:	Where are you from? What is your position? How many years have you been there?
Reply:	<ul style="list-style-type: none"> • Been a DOE federal employee since 1991. Work at the office of counterintelligence, main function is to protect of people programs. Counterintelligence and security are parallel with different responsibilities.
Question 2:	What precautions are taken at the end of the day? (Locked doors, computers logged off)
Reply:	<ul style="list-style-type: none"> • There's an end of day checklist. Make sure that all containers secured/ double checked, computers are turned off, disks are accounted for, copier is turned off, and all doors are locked.
Question 3:	How do you build security awareness? In other words how is it promoted?

Reply:	Visual education methods, posters, newsletters, individual meetings, monthly news articles.
Question 4:	What approaches are most effective? Why? Which are least effective? Why?
Reply:	<ul style="list-style-type: none"> Brief and debriefings are most effective. One on one most effective. This is not always possible, but is most effective. The least effective is the computer refresher courses, there is never any interactions this way. They also send you documents and expect you to sign them and send them back, there is also no interaction this way, and people don't always read the document.
Question 5:	Have employees ever been involved in the process of developing security procedures and or guidelines?
Reply:	<ul style="list-style-type: none"> We have asked employees to solicit input. We have poster contests, and reward the winner. We also have forms that you fill out when there are guest speakers with your input.
Question 6:	I know that requiring badges to be worn is common practice at DOE facilities; is this correct? What are the consequences for failing to wear a badge? Is this a common problem?
Reply:	<ul style="list-style-type: none"> Guards patrol frequently looking for people without their badges. They also touch, and feel the badge to make sure its not altered. Other employees also correct you if you don't have it on.
Question 7:	Are there any plans for future promotion of security awareness (in-progress)? Is there anything that you'd like to try but haven't been able to this far?
Reply:	<ul style="list-style-type: none"> We are also starting to have security awareness meetings by telephonic conferences. We have an annual security refresher. We are also having more briefing and debriefings.

INDUSTRY EXPERT/CUSTOMER INTERVIEWEE INFORMATION					
Name:	Tracey Lamee	Company:	Sandia Nat. Laboratories	Title:	Computer security operations
Segment Designation:	Management	Company Type:	Security Awareness		
Address:		Telephone:	(925) 294-2848	Email:	tnlamee@sandia.gov
INTERVIEWER INFORMATION					
Interviewer:	Beth Klinski	Consent:	Industry	Interview Date/Duration:	4/09/01 15 minutes
INTERVIEW SUMMARY					
Interviewee Issues:					
<ul style="list-style-type: none"> • Note the general attitude of the employees toward security • Determine where the manager sees problems, and the employees • Determine what is effective in getting the security message across. • What are the consequences of a security failure? • What does the manager need to get employees to be more security minded? 					

INTERVIEW DETAILS	
Question 1:	Where are you from? What is your position? How many years have you been there?
Reply:	<ul style="list-style-type: none"> • Sandia National Laboratories in Livermore, CA. I work for computer security operations dept. I have worked here for 19 ½ years. I protect national interest.
Question 2:	What precautions are taken at the end of the day? (Locked doors, computers logged off)
Reply:	<ul style="list-style-type: none"> • we practice double check checking. (making sure we did everything twice like turn off all machines, make sure doors are locked, and safes are secure)
Question 3:	How do you build security awareness? In other words how is it promoted?
Reply:	We have annual training. We do special briefings. There are many announcements on the net. It's a small site, we touch everyone.
Question 4:	What approaches are most effective? Why? Which are least effective? Why?
Reply:	<ul style="list-style-type: none"> • One on one is the most effective. People retain information better. • Computer based programs are least effective, people hardly pay attention to them.
Question 5:	Have employees ever been involved in the process of developing security procedures and or guidelines?
Reply:	<ul style="list-style-type: none"> • We have not yet formally, but people feel comfortable enough to say if they feel a procedure should be changed.
Question 6:	I know that requiring badges to be worn is common practice at DOE facilities; is this correct? What are the consequences for failing to wear a badge? Is this a common problem?
Reply:	<ul style="list-style-type: none"> • People are denied access. If it's a continuing problem, action is taken with their supervisor. If its really a problem, they have to leave their badge at the gate at the end of the day.
Question 7:	Are there any plans for future promotion of security awareness (in-progress)? Is there anything that you'd like to try but haven't been able to this far?
Reply:	<ul style="list-style-type: none"> • There isn't really any plans in progress, our security program is doing just fine for now.

INDUSTRY EXPERT/CUSTOMER INTERVIEWEE INFORMATION					
Name:	Trent Olaveson	Company:	Sandia Nat. Laboratories	Title:	
Segment Designation:	Management	Company Type:	Security Awareness		
Address:		Telephone:	(925) 294-3238	Email:	tbolave@sandia.gov
INTERVIEWER INFORMATION					
Interviewer:	Beth Klinski	Consent:	Industry	Interview Date/Duration:	4/09/01 15 minutes
INTERVIEW SUMMARY					
<p>Interviewee Issues:</p> <ul style="list-style-type: none"> • Note the general attitude of the employees toward security • Determine where the manager sees problems, and the employees • Determine what is effective in getting the security message across. • What are the consequences of a security failure? • What does the manager need to get employees to be more security minded? 					

INTERVIEW DETAILS	
Question 1:	Where are you from? What is your position? How many years have you been there?
Reply:	<ul style="list-style-type: none"> • Sandia National Laboratories in Livermore, CA. I have been there for 10 years. I am a security specialist. I protect information that could impact national security if lost.
Question 2:	What precautions are taken at the end of the day? (Locked doors, computers logged off)
Reply:	<ul style="list-style-type: none"> • Do a daily routine. Make sure that all lockers, monitors, are secured. There is a protective force, lock down, with an alarm.
Question 3:	How do you build security awareness? In other words how is it promoted?
Reply:	Online web, newsletter, site, newsletter, briefings, guest speakers, new security info displays.
Question 4:	What approaches are most effective? Why? Which are least effective? Why?
Reply:	<ul style="list-style-type: none"> • Most effective is the department briefings because it's an individual department with 15-30 people. When there small like this, and everyone knows each other, they feel more comfortable and ask more questions. • Least effective is the O Nine training, it's a program that's on the computer and there's too many requirements.
Question 5:	Have employees ever been involved in the process of developing security procedures and or guidelines?
Reply:	<ul style="list-style-type: none"> • Yes they have taken all site regulations to the line- made changes and came up with the Safeguards and Security Guide from A-Z, a book of security procedures.
Question 6:	I know that requiring badges to be worn is common practice at DOE facilities; is this correct? What are the consequences for failing to wear a badge? Is this a common problem?
Reply:	<ul style="list-style-type: none"> • Yes, you are denied access; if a badged person tries to take a non-badged person somewhere they can get an infraction.
Question 7:	Are there any plans for future promotion of security awareness (in-progress)? Is there anything that you'd like to try but haven't been able to this far?
Reply:	<ul style="list-style-type: none"> • Yes we are starting the S.S.I.M.S. (safeguard security informant management systems) program. It is better classified.

INDUSTRY EXPERT/CUSTOMER INTERVIEWEE INFORMATION					
Name:	Christina Hartley	Company:	Wackenhut Services, Inc.	Title:	Security specialist
Segment Designation:	Management	Company Type:	Security Awareness		
Address:		Telephone:	(803) 725-1711	Email:	Tina.Hartley@srs.gov
INTERVIEWER INFORMATION					
Interviewer:	Beth Klinski	Consent:	Industry	Interview Date/Duration:	4/10/01 15 minutes
INTERVIEW SUMMARY					
Interviewee Issues:					
<ul style="list-style-type: none"> • Note the general attitude of the employees toward security • Determine where the manager sees problems, and the employees • Determine what is effective in getting the security message across. • What are the consequences of a security failure? • What does the manager need to get employees to be more security minded? 					

INTERVIEW DETAILS	
Question 1:	Where are you from? What is your position? How many years have you been there?
Reply:	<ul style="list-style-type: none"> I have been with Wackenhut for 14 years. I am a security specialist. Security is very important I focus on it a lot, we are minimal classification though.
Question 2:	What precautions are taken at the end of the day? (Locked doors, computers logged off)
Reply:	<ul style="list-style-type: none"> We are in a property protection area. We are at a site where you can have authorized personal only. We make sure that all doors are locked, all the files are locked away. We have a Sifer locked door.
Question 3:	How do you build security awareness? In other words how is it promoted?
Reply:	We have weekly trainings on security. We also have annual and quarterly newsletters.
Question 4:	What approaches are most effective? Why? Which are least effective? Why?
Reply:	<ul style="list-style-type: none"> We have a poster contest. I think that this is most effective. We have a reward for the winner each month. It's usually like some kind of gift certificate to a restaurant or a department store. The winning poster is posted throughout the site. Computer based trainings are least effective.
Question 5:	Have employees ever been involved in the process of developing security procedures and or guidelines?
Reply:	<ul style="list-style-type: none"> We ask employees for their input and suggestions. We have a drop box for that.
Question 6:	I know that requiring badges to be worn is common practice at DOE facilities; is this correct? What are the consequences for failing to wear a badge? Is this a common problem?
Reply:	<ul style="list-style-type: none"> The employee is taken off the site, if they don't have a badge. YOU MUST HAVE A BADGE!
Question 7:	Are there any plans for future promotion of security awareness (in-progress)? Is there anything that you'd like to try but haven't been able to this far?
Reply:	<ul style="list-style-type: none"> We are going to start more self-assessments; everyone is required to participate in a yearly trade show. Where ideas are exchanged.

INDUSTRY EXPERT/CUSTOMER INTERVIEWEE INFORMATION			
Name:	John Soy	Company:	Bonneville Power Administration
		Title:	Personal security specialist
Segment Designation:	Management	Company Type:	Security Awareness
Address:		Telephone:	(503) 230-5098
		Email:	jjsoy@bpa.gov
INTERVIEWER INFORMATION			
Interviewer:	Beth Klinski	Consent:	Industry
		Interview Date/Duration:	4/09/01 15 minutes
INTERVIEW SUMMARY			
Interviewee Issues:			
<ul style="list-style-type: none"> • Note the general attitude of the employees toward security • Determine where the manager sees problems, and the employees • Determine what is effective in getting the security message across. • What are the consequences of a security failure? • What does the manager need to get employees to be more security minded? 			

INTERVIEW DETAILS	
Question 1:	Where are you from? What is your position? How many years have you been there?
Reply:	<ul style="list-style-type: none"> I have been at Bonneville for one year and four months. I am a personal security specialist. I look after people.
Question 2:	What precautions are taken at the end of the day? (Locked doors, computers logged off)
Reply:	<ul style="list-style-type: none"> Make sure that all doors are locked. Make sure that the vault is locked. Have to have a key to get to my part of building, a janitor can only come in with clearance.
Question 3:	How do you build security awareness? In other words how is it promoted?
Reply:	I'm just starting to brief with employees when they are new, as part of orientation.
Question 4:	What approaches are most effective? Why? Which are least effective? Why?
Reply:	<ul style="list-style-type: none"> Most important is to make employee see why it's important. They have to buy into it, they have to see how security would effect their time. They need to see how it protects you. A less effective way is that it runs like a bureaucracy. It can be boring because of the redundancy of the same stuff over and over again.
Question 5:	Have employees ever been involved in the process of developing security procedures and or guidelines?
Reply:	<ul style="list-style-type: none"> They need to be. There's not really any program for that yet. There needs to ownership taken.
Question 6:	I know that requiring badges to be worn is common practice at DOE facilities; is this correct? What are the consequences for failing to wear a badge? Is this a common problem?
Reply:	<ul style="list-style-type: none"> There isn't really a penalty yet. The security guards check to see if people are wearing them. There is minimal classified information here.
Question 7:	Are there any plans for future promotion of security awareness (in-progress)? Is there anything that you'd like to try but haven't been able to this far?
Reply:	<ul style="list-style-type: none"> I know that its important to update things, but more important things keep happening that has to be dealt with.

--	--

INDUSTRY EXPERT/CUSTOMER INTERVIEWEE INFORMATION			
Name:	Larry Wilcher	Company:	U.S. DOE
Title: Senior security executive			
Segment Designation:	Management	Company Type:	Security Awareness
Address:	Telephone: (301) 903-2528		Email: Larry.wilcher@hq.doe.gov
INTERVIEWER INFORMATION			
Interviewer:	Beth Klinski	Consent:	Industry
Interview Date/Duration:		4/09/01 15 minutes	
INTERVIEW SUMMARY			
<p>Interviewee Issues:</p> <ul style="list-style-type: none"> • Note the general attitude of the employees toward security • Determine where the manager sees problems, and the employees • Determine what is effective in getting the security message across. • What are the consequences of a security failure? • What does the manager need to get employees to be more security minded? 			

INTERVIEW DETAILS	
Question 1:	Where are you from? What is your position? How many years have you been there?
Reply:	<ul style="list-style-type: none"> • U.S. Department of Energy. Larry has been with the DOE since 1987. 30 yrs. Of governmental and military experience. At the DOE he's served as the program manager for OPSEC and technical security programs. He was promoted to Senior Executive Service as the director, Field Operations Division in 2000.
Question 2:	What precautions are taken at the end of the day? (Locked doors, computers logged off)
Reply:	<ul style="list-style-type: none"> • Make sure that all assets are locked- Second double-check everything. Make sure that the alarms are set. Individuals are responsible to insure that what they handle is secure on their computer. Every night all the computers must be off, even during the day when they're not using it.
Question 3:	How do you build security awareness? In other words how is it promoted?
Reply:	There is a major poster campaign. They have posters everywhere. There are also screen savers. There is an education promotional professional program that teaches security awareness.
Question 4:	What approaches are most effective? Why? Which are least effective? Why?
Reply:	<ul style="list-style-type: none"> • The least effective approaches are the annual security meetings. It is a burden, especially computer aid training. A study was done at the DOE and less than 5% of people retained the computer aid information. • Most effective are the audio/visual aids that are used. Such as posters and videos. Media aids that promote new security problems work well.
Question 5:	Have employees ever been involved in the process of developing security procedures and or guidelines?
Reply:	<ul style="list-style-type: none"> • We are a very secure area. A few composed plant workers have recommended how the plant can operate better. We also have scientists who want to publish their work, and there are things that can't be published. It is important to tell them why certain things can be published.
Question 6:	I know that requiring badges to be worn is common practice at DOE facilities; is this correct? What are the consequences for failing to wear a badge? Is this a common problem?
Reply:	<ul style="list-style-type: none"> • First you will get warned if you don't have a badge. It must be visible at all times. If it becomes a problem it's reported to their supervisor. Then there are also infraction programs. It's kept on their record, and three infractions in twelve months can lead to suspension.
Question	Are there any plans for future promotion of security awareness (in-progress)? Is there

7:	anything that you'd like to try but haven't been able to this far?
Reply:	<ul style="list-style-type: none">• They are working on a new security awareness internet based project. Themes people like, for example: Alice in Wonderland. The ISM (integrated security management) is also implementing a new policy; if you didn't do this, then what would you do?

APPENDIX C

INDUSTRY INTERVIEW QUESTIONS

INTERVIEWED by: Kristin Sawyer

- 1. What is your position at _____ company?**

- 2. Why does your company have security? Do you have classified information? Toxic materials?**

- 3. What precautions do you take at your business when leaving for the day? I.e. lock doors? Log off computers?**

- 4. How does your company promote security awareness?**

- 5. Are there advertising approaches that don't work?**

- 6. What security advertising approaches do work well?**

- 7. Do you wear badges or nametags at your site?**

- 8. Are there security guards present on the site, and what do they look for?**

**INDUSTRY INTERVIEW QUESTIONS:
INTERVIEWED by Kristin Sawyer**

1. **What is your position at ____ company?**
HP-General Security manager. Gerald
2. **Why does your company have security? Do you have classified information? Toxic materials?**
Main concern: Theft. Also classified information.
3. **What precautions do you take at your business when leaving for the day? I.e. lock doors? Log off computers?**
Those, plus locking cubicle offices.
4. **How does your company promote security awareness?**
The web site promotes awareness, posters.
5. **Are there advertising approaches that don't work?**
Don't be too harsh or point fingers at employees. Make the effort a team effort. Progress will occur if it's a team effort.
6. **What security advertising approaches do work well?**
Rewards. Randomness. Under cover security guards roaming with no name tags-see if anyone catches them. Reward a person who catches them.
7. **Do you wear badges or nametags at your site?**
Photo ID's are worn.
8. **Are there security guards present on the site, and what do they look for?**
They search for anything out of the ordinary-what doesn't appear normal. They search the buildings for people who seem to be confused. Sometimes they are uniformed and sometimes they aren't.

Comments: They have a site-wide 911, and he suggests giving rewards such as free lunch tickets for catching an unbadged employee, or an unmarked security guard.

**INDUSTRY INTERVIEW QUESTIONS:
INTERVIEWED by: Kristin Sawyer**

1. **What is your position at _____ company?**
Applications engineer at Chemica Technologies, Inc.
2. **Why does your company have security? Do you have classified information? Toxic materials?**
Confidential documents and also toxic materials. Also have expensive equipment and samples to protect. In addition, there are substances regulated by the Drug Enforcement Agency.
3. **What precautions do you take at your business when leaving for the day? I.e. lock doors? Log off computers?**
All exterior doors are shut and locked and the security system is enabled. All secure filing cabinets and chemical storage cabinets are locked.
4. **How does your company promote security awareness?**
Not much is done to promote security. Employees are informed of the basic security measures when they are hired. If issues arise they are brought up at the weekly company meeting.
5. **Are there advertising approaches that don't work?**
Information that is just posted on the bulletin board is often overlooked.
6. **What security advertising approaches do work well?**
If an e-mail is sent to employees and then it is brought up and discussed at the company meeting, there is generally a high degree of responsiveness.
7. **Do you wear badges or nametags at your site?**
No, it is a small company and everyone is familiar with other employees.
8. **Are there security guards present on the site, and what do they look for?**
No, there are no security guards.

INDUSTRY INTERVIEW QUESTIONS**INTERVIEWED by: Kristin Sawyer**

- 1. What is your position at _____ company?**
Glen, security coordinator at Linear Technologies.
- 2. Why does your company have security? Do you have classified information? Toxic materials?**
Life safety systems and classified information
- 3. What precautions do you take at your business when leaving for the day? I.e. lock doors? Log off computers?**
Not a high security environment, but no big need for it. There is 24 hour security, and it is important to pass on activity that has occurred throughout the day to the new shift members.
- 4. How does your company promote security awareness?**
Training, updates as needed. 24 hour training for new people.
- 5. Are there advertising approaches that don't work?**
No-everything is worthwhile.
- 6. What security advertising approaches do work well?**
Job fairs, newspaper, posters, website ads
- 7. Do you wear badges or nametags at your site?**
Badges and nametags are worn
- 8. Are there security guards present on the site, and what do they look for?**
There are security guards who lock up after various shifts. NOT a big deal if doors left unlocked-security will take care of it. Rewards are a good way of keeping security around, but there is no need at Linear Technologies.

INDUSTRY INTERVIEW QUESTIONS**INTERVIEWED by: Kristin Sawyer**

- 1. What is your position at _____ company?**
Tim, Security manager at Wafertech in Camas, WA.
- 2. Why does your company have security? Do you have classified information? Toxic materials?**
Both need security at the site.
- 3. What precautions do you take at your business when leaving for the day? I.e. lock doors? Log off computers?**
Automatic shut down of computers after 10 minutes if not used.
Lock doors and safes. Lock file cabinets etc.
- 4. How does your company promote security awareness?**
Full day of security training during new employee training week.
Sessions offered throughout the year for everyone.
- 5. Are there advertising approaches that don't work?**
Posters are not so useful.
- 6. What security advertising approaches do work well?**
Emails and website advertisements are effective. There is a lot of one-on-one training during the initial hiring of employees-good environment to learn in.
- 7. Do you wear badges or nametags at your site?**
Badges are worn
- 8. Are there security guards present on the site, and what do they look for?**
There are security guards. They look for parking stickers in vehicles 2 times/week. There are also undercover security men search for these things, along with unbadged people and anything out of the ordinary.

APPENDIX D

In-depth Employee Interviews:

INDUSTRY EXPERT/CUSTOMER INTERVIEWEE INFORMATION		
Name:	Company:	Title:
Segment Designation:	Company Type:	
Address:	Telephone:	Email:
INTERVIEWER INFORMATION		
Interviewer:	Consent:	Interview Date/Duration:
INTERVIEW SUMMARY		
Interviewee Issues: <ul style="list-style-type: none"> • Note the general attitude of the employees toward security • Determine where the manager sees problems, and the employees • Determine what is effective in getting the security message across. • What are the consequences of a security failure? • What does the manager need to get employees to be more security minded? 		

INTERVIEW DETAILS	
Question 1:	How many years have you worked for Hanford?
Reply:	
Question 2:	What security awareness have you seen that is most effective or least effective? Do you have a preference for how you receive security information and reminders?
Reply:	
Question 3:	If you have questions about security issues, do you know how to get the answers? What could the security awareness group do to allow quicker access to the information you need?
Reply:	
Question 4:	What types of activities are you expected to do on a regular basis to keep Hanford secure? I.e. lock doors, turn off computers.
Reply:	
Question 5:	What causes people to take personal responsibility or ownership for security?
Reply:	
Question 6:	What kinds of programs or materials would you recommend to increase personal awareness of security amongst your co-workers?
Reply:	
Question 7:	What kinds of programs or materials would you recommend to increase personal responsibility or ownership for security amongst your co-workers?

INDUSTRY EXPERT/CUSTOMER INTERVIEWEE INFORMATION					
Name:	Bobby Baker	Company:	Hanford	Title:	Safety Rep. Solid waste /occupational safe engineer
Segment Designation:	Non-Management	Company Type:	Security Awareness		
Address:	Hanford	Telephone:	376-8774	Email:	R_B_Robert_Baker@RL.gov
INTERVIEWER INFORMATION					
Interviewer:	Beth Klinski	Consent:	Acknowledged	Interview Date/Duration:	3/30/01 20 minutes
INTERVIEW SUMMARY					
Interviewee Issues:					
<ul style="list-style-type: none"> • Note the general attitude of the employees toward security • Determine where the manager sees problems, and the employees • Determine what is effective in getting the security message across. • What are the consequences of a security failure? • What does the manager need to get employees to be more security minded? 					

INTERVIEW DETAILS	
Question 1:	How many years have you worked for Hanford?
Reply:	<ul style="list-style-type: none"> Have worked for Hanford for 17 years. Safety engineer at Giaff Construction Co. for 5 years prior to working for Hanford.
Question 2:	What security awareness have you seen that is most effective or least effective? Do you have a preference for how you receive security information and reminders?
Reply:	<ul style="list-style-type: none"> I think the most effective is when the requirements are reiterated frequently. I think the least is the annual staff meetings.
Question 3:	If you have questions about security issues, do you know how to get the answers? What could the security awareness group do to allow quicker access to the information you need?
Reply:	First you would contact your manager, if you couldn't find the answer there, you could call security directly and ask one of them. I wasn't aware that there was a security awareness group. I think incorporating security into the general employee training is very effective.
Question 4:	What types of activities are you expected to do on a regular basis to keep Hanford secure? I.e. lock doors, turn off computers.
Reply:	<ul style="list-style-type: none"> It is important to maintain your computers frequently and change your password often also for protection. It is very important to be on the alert for people who are unbadged, and you must confront them, you can't let them walk by and not say anything.
Question 5:	What causes people to take personal responsibility or ownership for security?
Reply:	<ul style="list-style-type: none"> You must have it. This is a difficult question. At Hanford you are indoctrinated with security awareness from the time you are hired. Security is key around here.
Question 6:	What kinds of programs or materials would you recommend to increase personal awareness of security amongst your co-workers?
Reply:	<ul style="list-style-type: none"> There are materials already here and available for use. Refresher training electronic mail. Articles in the Hanford Reach, everyone reads the reach.
Question 7:	What kinds of programs or materials would you recommend to increase personal responsibility or ownership for security amongst your co-workers?
Reply:	<ul style="list-style-type: none"> Complacency attitude- missions changed dramatically from when the site was producing. During that time awareness was quite high- people do become complacent over a period of time. There used to be more patrolling of the site, and also helicopters, they have done away with this.

INDUSTRY EXPERT/CUSTOMER INTERVIEWEE INFORMATION					
Name:	Daniel Coffland	Company:	Hanford	Title:	Heavy equipment operator
Segment Designation:	Non-management	Company Type:	Security Awareness		
Address:	Hanford	Telephone:	376-8473	Email:	D_L_Coffland@RL.gov
INTERVIEWER INFORMATION					
Interviewer:	Beth Klinski	Consent:	Acknowledged	Interview Date/Duration:	3/30/01-20 minutes
INTERVIEW SUMMARY					
Interviewee Issues:					
<ul style="list-style-type: none"> • Note the general attitude of the employees toward security • Determine where the manager sees problems, and the employees • Determine what is effective in getting the security message across. • What are the consequences of a security failure? • What does the manager need to get employees to be more security minded? 					

INTERVIEW DETAILS	
Question 1:	How many years have you worked for Hanford?
Reply:	<ul style="list-style-type: none"> I have worked at Hanford for 10 months. I am also a Pasco Police Reserve Officer. I have been an officer for the last six years.
Question 2:	What security awareness have you seen that is most effective or least effective? Do you have a preference for how you receive security information and reminders?
Reply:	<ul style="list-style-type: none"> I think that education meetings are the most effective; they tell you what to look for, what to do when you see a situation and how to report it. I feel that there is not enough patrol around during the day, they are either at the barricade or at their office, and I never really see them around. They need to patrol the area more.
Question 3:	If you have questions about security issues, do you know how to get the answers? What could the security awareness group do to allow quicker access to the information you need?
Reply:	<p>First I would go to the manager, second I would call the Hanford patrol. Or I would look on the security website where I can email the security dept. with a question concerning security.</p>
Question 4:	What types of activities are you expected to do on a regular basis to keep Hanford secure? I.e. lock doors, turn off computers.
Reply:	<ul style="list-style-type: none"> I would make sure people were wearing their badges, and if they weren't I would question them. I also make sure doors and car doors are locked, and make sure that computers are turned off.
Question 5:	What causes people to take personal responsibility or ownership for security?
Reply:	<ul style="list-style-type: none"> We are a five star status company. We need to be proud of who work for. If we report a certain situation we should get rewards for it.
Question 6:	What kinds of programs or materials would you recommend to increase personal awareness of security amongst your co-workers?
Reply:	<ul style="list-style-type: none"> That is a tough question, I can't think of anything at the moment.
Question 7:	What kinds of programs or materials would you recommend to increase personal responsibility or ownership for security amongst your co-workers?

Reply:	<ul style="list-style-type: none"> I cant think of anything at the moment. I haven't been there very long so Im not very aware of the other programs that are available.
--------	---

INDUSTRY EXPERT/CUSTOMER INTERVIEWEE INFORMATION			
Name:	Bruce LaRue	Company:	Hanford
		Title:	Scientist 1
Segment Designation:	Non-management	Company Type:	Security Awareness
Address:	MO279/A135/200W	Telephone:	373-2311
		Email:	Bruce_W_LaRue@rl.gov
INTERVIEWER INFORMATION			
Interviewer:	Beth Klinski	Consent:	Acknowledged
		Interview Date/Duration:	03/08/01 10 minutes
INTERVIEW SUMMARY			
<p>Interviewee Issues:</p> <ul style="list-style-type: none"> Note the general attitude of the employees toward security Determine where the manager sees problems, and the employees Determine what is effective in getting the security message across. What are the consequences of a security failure? What does the manager need to get employees to be more security minded? 			

INTERVIEW DETAILS	
Question 1:	How many years have you worked for Hanford?
Reply:	<ul style="list-style-type: none"> I have worked at Hanford for one year.
Question 2:	What security awareness have you seen that is most effective or least effective? Do you have a preference for how you receive security information and reminders?
Reply:	<ul style="list-style-type: none"> Lacking in information. Cant find very much information when you look on the security website. Bruce likes to go backpacking. He doesn't know how much a problem it would be to bring his equipment on site, like propane gas, Swiss army knife, or an axe. He feels that there needs to be more detail on prohibited items. He feels that there needs to be more accessible modification on prohibited articles like camping equipment.
Question 3:	If you have questions about security issues, do you know how to get the answers? What could the security awareness group do to allow quicker access to the information you need?
Reply:	<ul style="list-style-type: none"> Bruce looks on the security website He feels that an update of the web page would allow quicker access. An email address where you could ask a specific question and get a quick response would be very helpful.
Question 4:	What types of activities are you expected to do on a regular basis to keep Hanford secure? I.e. lock doors, turn off computers.
Reply:	<ul style="list-style-type: none"> Keep your eyes open. If you see someone with out their security badge on, report to supervisor immediately. Make sure that doors are always secure. When you leave your office make sure that your computer is off.
Question 5:	What causes people to take personal responsibility or ownership for security?
Reply:	<ul style="list-style-type: none"> People do need to be careful. There is a lot of peer pressure and peer acceptance. If someone is not wearing his or her badge then, you have to report it. Even if its one of your friends.
Question 6:	What kinds of programs or materials would you recommend to increase personal awareness of security amongst your co-workers?
Reply:	<ul style="list-style-type: none"> The security website could have more information. Reminders posted around site would also help. An email Q & A address would also be nice.

Question 7:	What kinds of programs or materials would you recommend to increase personal responsibility or ownership for security amongst your co-workers?
Reply:	<ul style="list-style-type: none"> Email reminders would be a good way to increase personal responsibility. More posters posted around the building would be nice. The Hanford reach does a good job in promoting security, and it is read quite often. The cartoon they use is funny and it catches the eye, so to continue doing that would help also.

INDUSTRY EXPERT/CUSTOMER INTERVIEWEE INFORMATION					
Name:	Gail Chaffee	Company:	Hanford	Title:	Specialty engineer
Segment Designation:	Non-management	Company Type:	Security Awareness		
Address:	MO401/29/100K	Telephone:	372-1411	Email:	Gail_A_Chaffee@rl.gov
INTERVIEWER INFORMATION					
Interviewer:	Beth Klinski	Consent:	Acknowledged	Interview Date/Duration:	03/09/01 10 minutes
INTERVIEW SUMMARY					
Interviewee Issues:					
<ul style="list-style-type: none"> Note the general attitude of the employees toward security Determine where the manager sees problems, and the employees Determine what is effective in getting the security message across. What are the consequences of a security failure? What does the manager need to get employees to be more security minded? 					

INTERVIEW DETAILS	
Question 1:	How many years have you worked for Hanford?
Reply:	<ul style="list-style-type: none"> I have worked at Hanford for 10 years
Question 2:	What security awareness have you seen that is most effective or least effective? Do you have a preference for how you receive security information and reminders?
Reply:	<ul style="list-style-type: none"> I feel that the monthly safety presentations are very effective, since we all go to them. There are also many patrol vehicles, which I feel increases safety. I work at the K Base and security walks through the building quite frequently. There are also spot checks when you enter or leave the site. You also must wear your badge at all times. I don't have a preference on how I receive security info... I guess an email would be a good way.
Question 3:	If you have questions about security issues, do you know how to get the answers? What could the security awareness group do to allow quicker access to the information you need?
Reply:	<ul style="list-style-type: none"> Call Security. Have security person assigned to project that you have a question about answer it for you. The Intranet has great security messages (banner ads) that continually change. I definitely would not want to hear it over a loud speaker.
Question 4:	What types of activities are you expected to do on a regular basis to keep Hanford secure? I.e lock doors, turn off computers.
Reply:	<ul style="list-style-type: none"> It's about attitude, challenge people with out badge... if they don't tell your supervisor. Report if there's a suspicious brief case by a door, and no one's by it. If there's ever any suspicious nature, call security or management. I don't lock my office door, but there are auto locks on my building door, and you need to know the code to get in. If I'm working late hours, it's my responsibility to make sure the door I'm using stays locked. I always turn off my computer. There are multitudes of requirements convened in one.
Question 5:	What causes people to take personal responsibility or ownership for security?
Reply:	<ul style="list-style-type: none"> It is kind of embedded in training. We are always being made aware of it... its kind of subliminal. They are natural everyday habits at work.
Question 6:	What kinds of programs or materials would you recommend to increase personal awareness of security amongst your co-workers?

Reply:	<ul style="list-style-type: none"> To do a good job... People who work downtown have a different awareness. The downtown people deal with people off the streets. I work in the area of Hanford that is 30 miles from town, there are always security people patrolling. You must show your badge. The people downtown are more susceptible. I don't interact with general public.
Question 7:	What kinds of programs or materials would you recommend to increase personal responsibility or ownership for security amongst your co-workers?
Reply:	<ul style="list-style-type: none"> It would be nice if security would give you stuff like mouse pads, magnets, and calendars, things that you use every day. Advertisements... coffee mugs, and key rings would also be nice. The Hanford Reach does a good job. They have a cartoon that is very funny. I can't think of programs that are more beneficial than they already have. You could talk about security issues in monthly meetings.

INDUSTRY EXPERT/CUSTOMER INTERVIEWEE INFORMATION			
Name:	Toni Lauricella	Company:	Hanford Title: Tank coordinator
Segment Designation:	Non-management	Company Type:	Security Awareness
Address:	2750E/A207/200E	Telephone:	373-6343 Email: Toni_L_Lauricella@rl.gov
INTERVIEWER INFORMATION			
Interviewer:	Beth Klinski	Consent:	Acknowledged Interview Date/Duration: 03/08/01 15 minutes
INTERVIEW SUMMARY			
<p>Interviewee Issues:</p> <ul style="list-style-type: none"> Note the general attitude of the employees toward security Determine where the manager sees problems, and the employees Determine what is effective in getting the security message across. What are the consequences of a security failure? What does the manager need to get employees to be more security minded? 			

INTERVIEW DETAILS	
Question 1:	How many years have you worked for Hanford?
Reply:	<ul style="list-style-type: none"> • One year. Most of the employees have worked here longer than me.
Question 2:	What security awareness have you seen that is most effective or least effective? Do you have a preference for how you receive security information and reminders?
Reply:	<ul style="list-style-type: none"> • I feel that people awareness is most effective. I can't really think of anything that I have seen that is ineffective. I would definitely say that computer email is the best way to receive security information and reminders. People will definitely see it there... they sit in front of a computer all day.
Question 3:	If you have questions about security issues, do you know how to get the answers? What could the security awareness group do to allow quicker access to the information you need?
Reply:	<ul style="list-style-type: none"> • Yes... you can either call security or ask your manager. There are also security cars patrolling quite frequently. For the quickest access I would look on the security website.
Question 4:	What types of activities are you expected to do on a regular basis to keep Hanford secure? I.e lock doors, turn off computers.
Reply:	<ul style="list-style-type: none"> • I work in an area where information is not classified. The best thing to do is be aware of the rules and regulations and make sure to follow them, and if you see someone not following them, tell your supervisor or contact security.
Question 5:	What causes people to take personal responsibility or ownership for security?
Reply:	<ul style="list-style-type: none"> • I feel that it's a personal integrity thing. People realize that it's necessary to do a job. It also people not feeling above...like it's major thing. Ex: "I don't need to do that kind of thing."
Question 6:	What kinds of programs or materials would you recommend to increase personal awareness of security amongst your co-workers?
Reply:	<ul style="list-style-type: none"> • When people are caught violating the rules, we don't hear about it. It would be nice if they could somehow start telling us when things happened where someone didn't follow the rules.

Question 7:	What kinds of programs or materials would you recommend to increase personal responsibility or ownership for security amongst your co-workers?
Reply:	<ul style="list-style-type: none"> • That would be hard since I think it's a personal integrity problem. I'm not sure how you could change that in someone. I think just to have a strong management is the best thing. People feel peer pressure too. I'm not sure how you could change that either.

INDUSTRY EXPERT/CUSTOMER INTERVIEWEE INFORMATION			
Name:	Henry Booth	Company:	Hanford Security Title: Scientist 1
Segment Designation:	Non-management	Company Type:	Security Awareness
Address:	2750E /D164 /200E	Telephone:	373-3523 Email: Henry W Booth@rl.gov
INTERVIEWER INFORMATION			
Interviewer	Beth Klinski	Consent-	Acknowledged Interview date 3/08/01
INTERVIEW SUMMARY			
Interviewee Issues:			
<ul style="list-style-type: none"> • Note the general attitude of the employees toward security • Determine where the manager sees problems, and the employees • Determine what is effective in getting the security message across. • What are the consequences of a security failure? • What does the manager need to get employees to be more security minded? 			

INTERVIEW DETAILS	
Question 1:	How many years have you worked for Hanford Security?
Reply:	<ul style="list-style-type: none"> • Aggregate time 16 yrs. • Current position 5 yrs.
Question 2:	Have you ever had a security clearance?
Reply:	<ul style="list-style-type: none"> • Had the Q clearance, but doesn't have that now.
Question 3:	How do you feel about the changes that have occurred over the years regarding security and Hanford's change to environmental clean up?
Reply:	<ul style="list-style-type: none"> • Clearances are adequate for whats going on now, less access control.
Question 4:	Based on your experiences at Hanford's, what security training have you had that has proven effective?
Reply:	<ul style="list-style-type: none"> • Staff meetings are most effective. Security is usually always on the agenda at staff meetings.
Question 5:	What security materials have you seen which are most effective or least effective?
Reply:	<ul style="list-style-type: none"> • Doesn't notice posters. Gets security awareness from other employees, management chain, and staff meetings.
Question 6:	If you have a questions about security, do you know whom to contact? Who is that person(s)?
Reply:	<ul style="list-style-type: none"> • First step is to ask other employee. • Second step is to ask manager. • If there is a major problem, call 911 immediately.
Question 7:	What types of activities are you expected to do on a regular basis to keep Hanford safe? I.e. lock doors, turn off computers.
Reply:	<ul style="list-style-type: none"> • Lock doors. <p>Turn off computers. Change passwords on computers regularly. General walk through of area to be sure everything is secure before leaving.</p>

INDUSTRY EXPERT/CUSTOMER INTERVIEWEE INFORMATION					
Name:	Steven Cantrell	Company:	Hanford's Security	Title:	NHC
Segment Designation:	Industry Expert/Customer	Company Type:	Security Awareness		
Address:		Telephone:	509 376 6439	Email:	Steven_C_Cantrell@rl.gov
INTERVIEWER INFORMATION					
Interviewer:	Kristin Sawyer	Consent:	Acknowledged	Interview Date/Duration:	March 9, 2001 10 minutes
INTERVIEW SUMMARY					
<p>Interviewee Issues:</p> <ul style="list-style-type: none"> • Note the general attitude of the employees toward security • Determine where the manager sees problems, and the employees • Determine what is effective in getting the security message across. • What are the consequences of a security failure? • What does the manager need to get employees to be more security minded? 					

INTERVIEW DETAILS	
Question 1:	How many years have you worked for Hanford's Security?
Reply:	<ul style="list-style-type: none"> • Bulleated response. On and off since 1976
Question 2:	What security awareness have you seen that is most effective or least effective? Do you have a preference for how you receive security information and reminders?
Reply:	<ul style="list-style-type: none"> • Response The posters and the information posted on the bulletin boards is most helpful. It's important to know your coworkers-recognize them. The yearly updates are highly effective.
Question 3:	If you have questions about security issues, do you know how to get the answers? What could the security awareness group do to allow quicker access to the information you need?
Reply:	<ul style="list-style-type: none"> • Response Either contact a manager or use the emergency phone list posted by every phone. Steven is not in a highly sensitive area. The bulletin board is great.
Question 4:	What types of activities are you expected to do on a regular basis to keep Hanford's secure? le lock doors, turn off computers.
Reply:	<ul style="list-style-type: none"> • Bulleated response. Lock door, many just have cubicles. He also has to lock the fire-proof vault.
Question 5:	What causes people to take personal responsibility or ownership for security?
Reply:	<ul style="list-style-type: none"> • Bulleated list of responses and reactions Personal morals and upbringing. Either you'll care or you won't.
Question 6:	What kinds of programs or materials would you recommend to increase personal awareness of security amongst your co-workers?

Reply:	<ul style="list-style-type: none"> • Bulleled response <p>The random checks catch you off-guard and are good reminders. Reminders sent in the mail are ineffective because it's too easy to toss them. The monthly security meetings are very effective also.</p>
--------	---

INDUSTRY EXPERT/CUSTOMER INTERVIEWEE INFORMATION			
Name:	David Nichols	Company:	Hanford's Security
		Title:	
Segment	Industry	Company	
Designation:	Expert/Customer	Type:	Security Awareness
Address:	825jadwin	Telephone:	509 376 4351
		Email:	David_H_Nichols@rl.gov
INTERVIEWER INFORMATION			
Interviewer:	Kristin Sawyer	Consent:	Acknowledged
		Interview Date/Duration:	April 10, 2001 10 minutes
INTERVIEW SUMMARY			
<p>Interviewee Issues:</p> <ul style="list-style-type: none"> • Note the general attitude of the employees toward security • Determine where the manager sees problems, and the employees • Determine what is effective in getting the security message across. • What are the consequences of a security failure? • What does the manager need to get employees to be more security minded? 			

INTERVIEW DETAILS	
Question 1:	How many years have you worked for Hanford's Security?
Reply:	<ul style="list-style-type: none"> • Bulleated response. 19 years in same area.
Question 2:	What security awareness have you seen that is most effective or least effective? Do you have a preference for how you receive security information and reminders?
Reply:	<ul style="list-style-type: none"> • Response The Hget training on the website needs to be improved, but it would be very effective. Gets most information here, but the training from this is too quick and too much is easily overlooked.
Question 3:	If you have questions about security issues, do you know how to get the answers? What could the security awareness group do to allow quicker access to the information you need?
Reply:	<ul style="list-style-type: none"> • Response Yes...security phone number is handy. Bulletin board is also effective, however, there isn't enough security information on it.
Question 4:	What types of activities are you expected to do on a regular basis to keep Hanford's secure? Ie lock doors, turn off computers.
Reply:	<ul style="list-style-type: none"> • Bulleated response. Log off computers and lock door when leaving at night.
Question 5:	What causes people to take personal responsibility or ownership for security?
Reply:	<ul style="list-style-type: none"> • Bulleated list of responses and reactions Didn't want to comment.
Question 6:	What kinds of programs or materials would you recommend to increase personal awareness of security amongst your co-workers?
Reply:	<ul style="list-style-type: none"> • Bulleated response Better Hget training on the web. It should be more challenging.

INDUSTRY EXPERT/CUSTOMER INTERVIEWEE INFORMATION					
Name:	Myrna Sills	Company:	Hanford's Security	Title:	Building Administrator
Segment Designation:	Industry Expert/Customer	Company Type:	Security Awareness		
Address:		Telephone:	509 372 0687	Email:	Myrna_L_Sills@rl.gov
INTERVIEWER INFORMATION					
Interviewer:	Kristin Sawyer	Consent:	Acknowledged	Interview Date/Duration:	March 9, 2001 15 minutes
INTERVIEW SUMMARY					
Interviewee Issues:					
<ul style="list-style-type: none"> • Note the general attitude of the employees toward security • Determine where the manager sees problems, and the employees • Determine what is effective in getting the security message across. • What are the consequences of a security failure? • What does the manager need to get employees to be more security minded? 					

INTERVIEW DETAILS	
Question 1:	How many years have you worked for Hanford's Security?
Reply:	<ul style="list-style-type: none"> • Bulleled response. 10 years
Question 2:	What security awareness have you seen that is most effective or least effective? Do you have a preference for how you receive security information and reminders?
Reply:	<ul style="list-style-type: none"> • Response Random vehicle checks that have been taken away due to budgetary reasons were very effective. Mailing flyers isn't effective. The cartoons in the Reach, news briefs are good and random badging tests are as well.
Question 3:	If you have questions about security issues, do you know how to get the answers? What could the security awareness group do to allow quicker access to the information you need?
Reply:	<ul style="list-style-type: none"> • Response The bulletin boards are updated and informative. The Hanford's today webpage is also informative. She felt she had quick access to the information
Question 4:	What types of activities are you expected to do on a regular basis to keep Hanford's secure? Ie lock doors, turn off computers.
Reply:	<ul style="list-style-type: none"> • Bulleled response. Log off computers, keys are locked up in file cabinets, patrol people test doors.
Question 5:	What causes people to take personal responsibility or ownership for security?
Reply:	<ul style="list-style-type: none"> • Bulleled list of responses and reactions Pride in their work, and we all pay taxes for this facility
Question 6:	What kinds of programs or materials would you recommend to increase personal awareness of security amongst your co-workers?
Reply:	<ul style="list-style-type: none"> • Bulleled response Fluor Hanford Today and the bulletin board are already implemented. It would be helpful to continue the random checks...random vehicle inspections, random badgeless people, etc. Randomness is key!!

INDUSTRY EXPERT/CUSTOMER INTERVIEWEE INFORMATION					
Name:	Carol Meader	Company:	Hanford's Security	Title:	
Segment Designation:	Industry Expert/Customer	Company Type:	Security Awareness		
Address:		Telephone:	509367 2224	Email:	Carol_A_Meader@rl.gov
INTERVIEWER INFORMATION					
Interviewer:	Kristin Sawyer	Consent:	Acknowledged	Interview Date/Duration:	March 9, 2001 10 minutes
INTERVIEW SUMMARY					
<p>Interviewee Issues:</p> <ul style="list-style-type: none"> • Note the general attitude of the employees toward security • Determine where the manager sees problems, and the employees • Determine what is effective in getting the security message across. • What are the consequences of a security failure? • What does the manager need to get employees to be more security minded? 					

INTERVIEW DETAILS	
Question 1:	How many years have you worked for Hanford's Security?
Reply:	<ul style="list-style-type: none"> • Bulleled response. Almost 10 years
Question 2:	What security awareness have you seen that is most effective or least effective? Do you have a preference for how you receive security information and reminders?
Reply:	<ul style="list-style-type: none"> • Response Posters, emails are good
Question 3:	If you have questions about security issues, do you know how to get the answers? What could the security awareness group do to allow quicker access to the information you need?
Reply:	<ul style="list-style-type: none"> • Response Bulletin board is good...already has quick access
Question 4:	What types of activities are you expected to do on a regular basis to keep Hanford's secure? le lock doors, turn off computers.
Reply:	<ul style="list-style-type: none"> • Bulleled response. Lock doors, log off computers, put keys away
Question 5:	What causes people to take personal responsibility or ownership for security?
Reply:	<ul style="list-style-type: none"> • Bulleled list of responses and reactions Replace what is lost or damaged on their own.
Question 6:	What kinds of programs or materials would you recommend to increase personal awareness of security amongst your co-workers?
Reply:	<ul style="list-style-type: none"> • Bulleled response Watch each other, know who your coworkers are. Emails are helpful. Random checks are good.

Appendix E

ORISE website excerpt

About the Environment, Safety, and Health Group

An organization that achieves safe, hazard-free working conditions can expect healthy, productive employees and a thriving, vibrant environment for its community.

The Environment, Safety and Health (ESH) Group at the [Oak Ridge Institute for Science and Education](#) (ORISE) assists a wide variety of government and corporate clients in attaining optimum environmental and health standards by creating specialized [training](#) and [technical](#) resources and programs.

With experience in energy management, environmental health, environmental law, health physics, [radiation protection](#), [industrial hygiene](#), [occupational safety](#), and [risk management](#), the ESH group represents a wealth of expertise in environmental, safety, and health disciplines.

ORISE's ESH Group brings extensive training capabilities to its clients and is highly qualified to fulfill your organization's environmental, safety, and health training requirements through the following:



Large-scale, multidisciplinary training programs



Comprehensive training services



Use of instructional systems design modules



Military training



Program management and assessment



Human resources



Advanced training technologies



Performance support systems



[Distance learning](#) and Web-based training

Should your requirements call for expertise that is unavailable in-house at ORISE, the ESH Group will contract with specialists outside the organization. Through [Oak Ridge Associated Universities](#) (ORAU), we are affiliated with a number of universities across the United States. Additionally, ORISE has over 15 years of experience in managing the [Training Resources and Data Exchange](#) (TRADE) a network of more than 2,000 individuals from 65 organizations.

For more information, contact Peggy Smith at smithp@orau.gov.

[SEARCH](#) || [ABOUT ESH](#) || [MISSION & VISION](#) || [CAPABILITIES](#) || [PROJECTS](#) || [TRAINING](#)
[TECHNICAL SUPPORT](#) || [CLIENTS](#) || [PUBLICATIONS](#) || [FOR MORE INFORMATION](#) || [ESH HOME](#)

[ORAU Home Page](#) || [ORISE Home Page](#)

LLNL website excerpt



Guide to Key Lab Policies Related to Prime Contract Requirements

<h2>Computer Security</h2>				
<u>Contract References</u>	Contact Organization	Directorate Point of Contact	Policies, Procedures, and Guides	<u>Training Available</u>
Clause I.049 Appendix F Appendix G	<u>Computer Security Organization (CSO)</u> (<u>External Web Site</u>)	<u>Organizational Information System Security Officers (OISSOs)</u>	<u>LLNL Computer Use Policy and Security Rules</u> <u>LLNL Computer Security Policies/Guidelines</u> <u>Safeguards & Security Program Guide</u> <u>Annual Security Refresher Briefing</u>	Computer Security Courses, CS Series

[Go to DOE Information Security Home Page](#)
[Go to DOE Computer Incident Advisory Capability Home Page](#)

[Go to Other Contract Requirement Areas](#)

[Home](#) | [Contract 48](#) | [Appendix G](#) | [Lab Policies](#) | [Appendix F](#) | [FAQs](#) | [Bookmarks](#) | [Go To](#) | [E:MC2](#) | [Usage Notes](#) | [What's New](#) | [Comments](#)

Last updated on March 13, 2001 by Ann Willoughby
 If you have technical questions about this page, contact:
 Ann Willoughby -- willoughby1@llnl.gov

and [LLNL Disclaimers](#)

UCRL-AR-121904

This page is located at http://www.llnl.gov/OCM/Computer_Security.html

APPENDIX G

Pictures from SE-SIG



Figure 1- BWXT PANTEX- Security Display



Figure 2- KANSAS CITY PLANT- Security Display



Figure 3- KANSAS CITY PLANT- Security Display



Figure 4- POSTERS from SE-SIG



Figure 5- Beth, Alison and Sophia at SE-SIG



Figure 6- Beth interviewing Gary Chidester