

SAMPLE Information Security Awareness and Training Program Assessment Report

Prepared By:

Eclipsecurity, LLC

**Contact Eclipsecurity at:
info@eclipsec.com
(312) 373.9382
www.eclipsec.com**

Contents

| | |
|--|----|
| Introduction..... | 1 |
| ISATP Approach and Scope | 1 |
| Pilot ISATP Analytics..... | 1 |
| Analysis of ISATP Pre-Assessment Questionnaire Responses | 2 |
| Analysis of Responses to True-False Questions..... | 2 |
| Analysis of Short Answer Responses | 10 |
| Finance..... | 10 |
| OD..... | 12 |
| Analysis of ISATP Presentation Evaluations | 14 |
| Analysis of Short Answer Responses | 14 |
| Analysis of Received Responses to 10-Point Rated Questions | 14 |
| Analysis of ISATP Presentation Survey..... | 15 |
| Analysis of Short Answer Responses | 15 |
| Eclipsesecurity Lessons Learned | 16 |

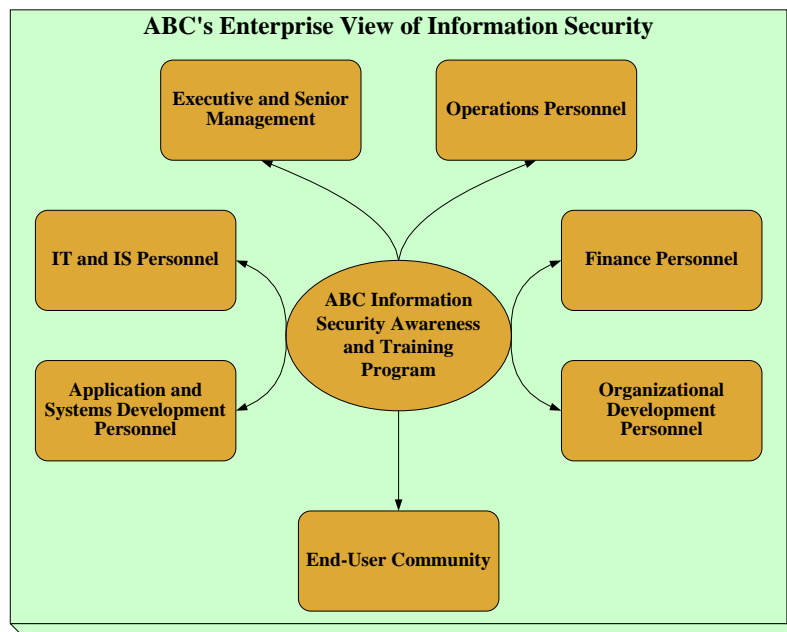
Introduction

Company “ABC” (ABC) engaged Eclipsesecurity, LLC (Eclipsesecurity) to develop and deliver an information security awareness and training program (ISATP). The primary business objective of the ISATP is to help ABC reduce occurrences of security-related incidents. Such incidents may include:

- Inappropriate and harmful disclosure of confidential financial or personal information;
- Unknowingly disclosing personal information to unauthorized parties in result of their malicious social engineering tactics;
- Enabling access to critical information systems due to personnel storing usernames and passwords in insecure locations (e.g., in unlocked desk drawers and on exposed post-it notes);
- Enabling access to critical information systems due to personnel leaving workstations exposed while attending internal meetings or visiting the washroom; and
- Physical access to resources allowing access to unauthorized information.

ISATP Approach and Scope

Distinct information security awareness and training sessions will ultimately be developed and specifically tailored for several audiences. To gain assurance of the effectiveness of the ISATP, ABC had requested that a pilot be performed. The pilot ISATP consisted of developing and providing sessions on behalf of two audiences; Finance and Organizational Development (OD) personnel. In light of the successful completion of the pilot ISATP, a consistent theme will be maintained to ultimately impart ABC’s enterprise view of information security among all audiences, as illustrated below.



Pilot ISATP Analytics

The emphasis of this report is to provide an analysis of the responses received to the following:

1. ISATP Pre-Assessment Questionnaire: The objective of this questionnaire is to understand the level of awareness participating OD and Finance personnel have with respect to the security

- ramifications associated with their daily business activities and overall professional business practices.
2. ISATP Presentation Evaluation: The objective of this evaluation form is to understand aspects of the pilot ISATP sessions that were effective, and aspects of the sessions that should be improved upon / enhanced.
 3. ISATP Presentation Survey: The objective of this survey is to address aspects of ABC's business operations that are of particular interest to ABC Information Security.

Analysis of ISATP Pre-Assessment Questionnaire Responses

The ISATP Pre-Assessment Questionnaire (PAQ) consists of two sections. The first section is comprised of twenty (20) true/false questions. The second section consists of seven (7) short-answer questions. As indicated in the Introduction of this ISATP Assessment Report, the primary objective of the PAQ was to understand the level of awareness participating OD and Finance personnel have with respect to the security ramifications associated with their daily business activities and overall professional business practices.

Analysis of Responses to True-False Questions

Provided in this section of the ISATP Assessment Report is an analysis of the responses received from the participating OD and Finance personnel to the True/False questions. This analysis is provided in the following table. The table provides the following information:

- Question: A reiteration of each question contained in the True/False portion of the PAQ
- Finance and OD Responses: Contains a tally of the number of "True" and "False" responses received from the respondents
- Desired / Correct Response: The desired / correct response is indicated by the True/False response that is shaded in green for each question
- Commentary: Provides rationale and additional insights into each question that was incorporated in the questionnaire
- Observations: Provides an evaluation of the responses received to each question, and accompanying recommendations / considerations

| Question | Finance Responses | | OD Responses | | Commentary and Observations |
|---|-------------------|-------|--------------|-------|---|
| | True | False | True | False | |
| I independently use my best judgment when determining whether I will share confidential financial and general ABC information with other ABC employees, or individuals not employed by ABC. | 14 | 1 | 11 | 1 | <p>Commentary: The intent of this question is to understand if the respondent makes educated decisions regarding how confidential ABC information is shared. The desired response is "true," which would indicate that ABC personnel do not frivolously divulge confidential information.</p> <p>Observations: Using each employee's best judgment in sharing confidential information is among ABC's most effective protective mechanisms. It is reassuring that a vast majority of responses received from both participating Finance and OD personnel indicate they are cognizant of the importance of how confidential ABC information should be shared.</p> |
| I dispose of most / all printed financial documents in my garbage can once they are no longer of use to me. | 7 | 8 | 1 | 11 | <p>Commentary: The intent of this question is to understand if the respondent destroys / shreds confidential ABC information before disposing of it in garbage cans. Dumpster diving is still a prevalent threat resulting in the unauthorized access to confidential information. All confidential documents should be shredded and not disposed of in shared / easily accessible garbage containers.</p> <p>Observations: While this question was specifically referring to financial documents, and therefore oriented towards the Finance audience, one OD respondent indicated that such information is disposed of their garbage can.</p> <p>Nearly 50% of the Finance respondents stated that they dispose of financial documents in their garbage can rather than using some other means such as a shredder. ABC and Eclipsesecurity should consider emphasizing the importance of properly destroying confidential documents prior to disposal in subsequent awareness / training sessions.</p> |
| When working with a contractor, temporary employee, or other appropriate third party, I do whatever I can to provide them with whatever information they may need to complete their tasks. | 9 | 6 | 7 | 5 | <p>Commentary: Information sharing among non-full time employees and contractors can result in the disclosure of confidential information that is not deemed appropriate for their employment status. It is quite common for a contractor or part time employee to receive priority information-sharing status. However, this can lead to situations where information is inappropriately disclosed to broader audiences.</p> <p>Observations: More than 50% of both participating Finance and OD personnel indicated that they share whatever information temporary employees and contractors may deem as necessary to support their job responsibilities. Contractor and temporary employees may present a considerable threat to ABC.</p> <p>ABC and Eclipsesecurity should consider emphasizing the risks associated with disclosing information to contractors and temporary employees in subsequent awareness / training sessions. Further, ABC should consider developing, implementing, and enforcing a governing security policy and supporting operating procedures to help further mitigate the likelihood of this form of inappropriate disclosure of information from occurring in the future.</p> |

| Question | Finance Responses | | OD Responses | | Commentary and Observations |
|--|-------------------|-------|--------------|-------|---|
| | True | False | True | False | |
| I have a strong understanding and recall most of my responsibilities as they are outlined in the ABC Code of Conduct and the ABC Employee Handbook. | 13 | 2 | 11 | 1 | <p>Commentary: The intent of this question is to validate ABC employees' understanding of the subject matter addressed in the ABC Code of Conduct and Employee Handbook.</p> <p>Observations: The ABC employee handbook requires an annual sign-off stating the employee reviewed the content. The responses demonstrate that this requisite sign-off process is effective in achieving desired understanding of the ABC Code of Conduct and the ABC Employee Handbook among the participating Finance and OD personnel.</p> |
| While I have witnessed inappropriate activities that were performed by a ABC employee, contractor, temporary employee, or third party, I have not found the need to notify anyone that these inappropriate activities have occurred. | 3 | 12 | 0 | 12 | <p>Commentary: Any inappropriate behavior / activities observed by ABC personnel should require immediate notification to ABC Information Security. The intent of this question is to discern if the respondents are using their own discretion in reporting events regardless if they believe they have witnessed inappropriate behavior / activities.</p> <p>Observations: It is alarming that 20% of the Finance respondents indicated that they witnessed inappropriate activities being conducted in the workplace, but did not report them accordingly. Allowing observed personnel-related incidents to transpire without reporting them accordingly can result in highly undesirable outcomes that otherwise could have been preemptively prevented.</p> <p>ABC and Eclipsecurity should consider emphasizing the importance of reporting all witnessed suspicious activities to ABC Information Security. Further, it should be stressed that it is ABC's commitment to its employees to ensure all reports are received and maintained in strict confidence. Further, ABC should consider developing, implementing, and enforcing a governing security policy and supporting operating procedures to help further reduce the likelihood of observed inappropriate behavior / activities from not being reported in the future.</p> <p>OD appears to understand the implications associated with not reporting inappropriate activity.</p> |
| It is common for a group of ABC employees that I work with to go out after work or on the train and discuss various aspects of our jobs. | 4 | 11 | 7 | 5 | <p>Commentary: Eavesdroppers and shoulder surfing is very prevalent and can provide an excellent means to understand current political, financial, and inter-workings of an organization.</p> <p>Observations: Nearly a third of Finance respondents and more than half of the OD respondents indicated that they discuss various aspects of their jobs in public environments. Caution should always be exercised by employees to ensure confidential or proprietary information is never discussed in a public environment.</p> <p>ABC and Eclipsecurity should consider emphasizing the risks associated with discussing various aspects of their jobs in public environments. Further, ABC should consider developing, implementing, and enforcing a governing security policy and supporting operating procedures to help discourage this form of dialogue from occurring in public environments in the future.</p> |

| Question | Finance Responses | | OD Responses | | Commentary and Observations |
|--|-------------------|-------|--------------|-------|--|
| | True | False | True | False | |
| For ease of use while at my ABC office and while off-site (e.g., while at home), I store most files on my computer's local hard drive, CDs, USB drives, or other portable storage devices. | 2 | 13 | 4 | 8 | <p>Commentary: Local storage of information increases the possibility of inappropriate disclosure of information; especially if the storage device is easily portable.</p> <p>Observations: 13% of Finance respondents and 33% of OD respondents indicate that they store information on portable media and computer systems for ease of use. ABC and Eclipsecurity should consider emphasizing the ramifications associated with storing confidential ABC information on portable devices in subsequent awareness / training sessions. Additionally, the broader topics of mobility and necessary security in a mobile environment should be considered for inclusion in the training / awareness materials.</p> <p>Lastly, ABC should consider developing, implementing, and enforcing a governing security policy and supporting operating procedures to effectively manage this aspect of its business operations.</p> |
| The virus issue is exaggerated...I do not have any concerns when I read emails and open accompanying attachments. | 0 | 15 | 1 | 11 | <p>Commentary: Virus attacks are still a very large concern in most organizations, and the ability for one piece of software to disrupt the entire system / network environment is greater than ever before. The caution exercised in this question is to avoid too much security "hype," as it may eventually serve as a detriment to ABC by causing its personnel to downgrade the importance and viability of associated potential threats.</p> <p>Observations: It appears that participating Finance and OD personnel understand the tremendous threats viruses may introduce to ABC.</p> |
| I keep all of my documented account passwords in a discrete location in my workspace so that I do not have to commit them to memory. This prevents me from having to bother Help Desk when I forget my password, and enables me to be more productive during my workday. | 4 | 11 | 4 | 8 | <p>Commentary: The intent of this question is to determine if ABC employees are documenting their passwords. It is in organizations' best interests to ensure all passwords are committed to memory.</p> <p>Note: The respondents who provided a "false" response may have indicated they do not store their documented passwords in a discrete location, but it is suspected this interpretation is highly unlikely and not representative of the respondents participating in this questionnaire.</p> <p>Observations: More than a quarter of the Finance respondents and a third of the OD respondents appear to store their passwords in a retrievable location. A contractor, temporary employee, or even a full time employee may be able to locate these passwords. Accessing users' passwords can result in an individual gaining unauthorized access to ABC's confidential information. Further, these unauthorized individuals would be accessing ABC's information systems under the auspices of the violated user / employee.</p> <p>ABC and Eclipsecurity should consider emphasizing the importance of having ABC users / personnel committing their passwords to memory, or at a minimum not storing their passwords in locations where they may be easily retrieved from unauthorized individuals. Further, ABC should consider developing, implementing, and enforcing a governing security policy and supporting operating procedures to help manage this issue.</p> |

| Question | Finance Responses | | OD Responses | | Commentary and Observations |
|--|-------------------|-------|--------------|-------|---|
| | True | False | True | False | |
| I frequently print financial information to shared printers in my work area. | 9 | 6 | 2 | 10 | <p>Commentary: It is common for unauthorized personnel to unintentionally, maliciously, or simply due to curiosity, to retrieve documents from shared printers. The intent of this question is to determine respondents' awareness of the implications associated with not retrieving printed documents in a timely fashion. Further, received responses should provide an indication of consideration applied to the nature of information the respondents print on shared printers (e.g. confidential, proprietary, and public knowledge). A contractor or part time employee may easily have access to confidential ABC information.</p> <p>Observations: Almost two-thirds of the Finance respondents and nearly 20% of the OD respondents print information to shared printers. This is a vital concern since both Finance and OD indicated they frequently generate, handle, and print confidential ABC information. ABC and Eclipsesecurity should consider emphasizing that documents printed using a shared printer should be retrieved in a timely fashion. Alternatively, ABC should consider procuring printers that may be privately used by personnel printing substantial amounts of confidential documents. Further, ABC should consider developing, implementing, and enforcing a governing security policy and supporting operating procedures to help manage this issue.</p> |
| It is somewhat challenging to distinguish confidential / sensitive ABC information from other types of ABC information that I frequently review while performing my daily business activities. | 2 | 13 | 0 | 12 | <p>Commentary: ABC personnel must be capable of distinguishing confidential / sensitive information from other types of information they manage as part of their daily business activities. Operating in the absence of such an understanding typically results in a lack of understanding of how the information should be shared and protected accordingly.</p> <p>Observations: Nearly 15% of Finance respondents stated that it is difficult to discern the difference between confidential information and other types of information they work with on a frequent basis. Although the percentage is low, a clear understanding of the sensitivity of information is required to ensure information confidentiality and integrity is preserved accordingly. Further, ABC should consider developing, implementing, and enforcing a governing information classification security policy and supporting operating procedures to help manage the manner in which the confidentiality of ABC information is designated, and the manner in which its confidential information should be protected accordingly.</p> |
| I am aware of ABC Information Security's objectives, but I am currently unfamiliar with their documented security policies. | 11 | 4 | 9 | 3 | <p>Commentary: An understanding of the current security policies is imperative to increase assurance that the confidentiality, integrity, and availability of ABC's information is established and preserved accordingly.</p> <p>Observations: Nearly 75% of the Finance and OD respondents indicated that they are not familiar with ABC's documented information security policies. ABC and Eclipsesecurity should consider emphasizing ABC Information Security's current direction with its corporate security policies, and the current status and ramifications associated with the development of its policies. It may also be effective to reference the ABC Information Security website as a mechanism for personnel to use as current and new policies and procedures are developed. Thorough distribution, awareness, and continued evaluation of the employees' understanding of the security policies should be maintained.</p> |

| Question | Finance Responses | | OD Responses | | Commentary and Observations |
|---|-------------------|-------|--------------|-------|---|
| | True | False | True | False | |
| During the workday, to give myself some short breaks from what I am working on, I like to spend some time surfing the Internet for various items / topics of interest (e.g., games scores, jokes, MP3's, free software programs, or merchandise from Amazon.com or eBay). | 3 | 12 | 4 | 8 | <p>Commentary: It is typically at the discretion of organizations whether Internet surfing is deemed to be acceptable. However, Internet surfing should be based upon an Acceptable Use Policy. The types of Internet usage should be limited; such as, the ability to download and install free software programs, MP3s and other potentially harmful content. The intent of this question is to determine if ABC personnel use the Internet for purposes other than to support their business activities. This question may help ABC understand the risks associated with its personnel's use of the Internet since many security breaches introduced to organizations are due to their personnel's Internet surfing practices / activities.</p> <p>Observations: 20% of Finance respondents and a third of the OD respondents indicated that they use the Internet during the workday for personal activities. It may be worthwhile to incorporate content in the training / awareness session indicating what ABC Information Security deems as acceptable Internet Use. Further, ABC should consider developing, implementing, and enforcing a governing acceptable use security policy and supporting operating procedures to help manage the manner in which various ABC resources are used.</p> |
| I do not typically use a cable lock, or alternate devices, to prevent the theft of my company laptop computer while working at my ABC office since I feel comfortable trusting my peers. | 4 | 11 | 6 | 6 | <p>Commentary: Physical protection of information should be taken seriously and practiced regardless of its location. At a minimum, due to the nature of confidential information that is generated and handled by Finance and OD, all lap top computers should be physically secured while working at ABC facilities. Lap top computer theft is very prevalent.</p> <p>Observations: Nearly a third of the Finance respondents, and 50% of the OD respondents indicated that they do not use physical security safeguards for their computer systems. There are several mechanisms thieves may use to access information stored on stolen lap top computers. It is important for ABC personnel to trust their peers, however, insider threats continue to be regarded as one of the most prevalent threats currently facing organizations. ABC and Eclipsesecurity should consider emphasizing the importance of physically securing computer systems in subsequent awareness / training sessions. Additionally, the broader topics of mobility and necessary security in a mobile environment should be considered for inclusion in the training / awareness materials. Lastly, ABC should consider developing, implementing, and enforcing a governing lap top security policy and supporting operating procedures to help mitigate lap top theft.</p> |

| Question | Finance Responses | | OD Responses | | Commentary and Observations |
|--|-------------------|-------|--------------|-------|---|
| | True | False | True | False | |
| As a kind gesture, there have been occasions where I have held doors open for individuals I did not know that were in close proximity of myself while entering ABC facilities. | 7 | 8 | 1 | 11 | <p>Commentary: Known as people chaining, individuals wait for the appropriate opportunity to attempt to access a restricted area without the correct credentials / authorized access. Kindness should always be fostered, however, security policies and procedures should be instituted to ensure the continued safety of the workplace, and to prevent unauthorized access to ABC facilities from occurring.</p> <p>Observations: Nearly 50% of Finance respondents indicated that they hold doors for other individuals that they do not necessarily know while entering ABC facilities. People chaining and social engineering are very common mechanisms used by unauthorized individuals to breach physical security. Such physical access commonly results in the unauthorized access to, and theft of confidential and proprietary information. ABC and Eclipsesecurity should continue to emphasize the importance of physical security, and to continue to impart an understanding of social engineering attacks.</p> <p>OD appears to understand the ramifications associated with allowing unknown individuals to access ABC facilities.</p> |
| I rarely find the need to lock my desk, file cabinets, etc. | 10 | 5 | 5 | 7 | <p>Commentary: Physical protection of information should be taken seriously and practiced regardless of its location. At a minimum, due to the nature of confidential information that is generated and handled by Finance and OD, all office furniture used to store confidential ABC information should be locked when offices are unattended.</p> <p>Observations: Two-thirds of the Finance respondents and nearly 50% of the OD respondents indicate that they rarely lock their office furniture that is used to store confidential information. This is alarming due to both Finance and OD respondents indicating the confidentiality of the information they handle on a daily basis. Further, ABC personnel storing information in shared workspaces (e.g., cubicles) increases the likelihood of inappropriate disclosure or theft of confidential ABC information. It is important to note that one of OD's primary security choices during the initial interviews was to lock desks and cabinets.</p> <p>ABC and Eclipsesecurity should consider emphasizing the importance of physically securing office furniture in subsequent awareness / training sessions. Lastly, ABC should consider developing, implementing, and enforcing a governing security policy and supporting operating procedures to help address this concern.</p> |
| I find email to be very useful when I need to provide authorized third parties with sensitive financial information. | 3 | 12 | 5 | 7 | <p>Commentary: Email is inherently an insecure application, and can lead to the inappropriate disclosure or theft of sensitive information. Employees need to be aware of transmittal policies to ensure the proper application and methodology is applied based upon the sensitivity of the information.</p> <p>Observations: 20% of Finance respondents and nearly 50% of the OD respondents indicated that they use email to transmit sensitive information to third parties. ABC and Eclipsesecurity should consider emphasizing the inherent insecurity of using email to transmit sensitive information to third parties in subsequent awareness / training sessions. Lastly, ABC should consider developing, implementing, and enforcing a governing email acceptable use and information classification policies and supporting operating procedures to increase assurance that its confidential information is sufficiently protected.</p> |

| Question | Finance Responses | | OD Responses | | Commentary and Observations |
|--|-------------------|-------|--------------|-------|---|
| | True | False | True | False | |
| To help myself with my daily duties I use a search companion such as MSN toolbar, Yahoo Companion, or Google's search bar. | 5 | 10 | 6 | 6 | <p>Commentary: Search bars provide increased productivity in the ability to quickly allow an individual to receive results from a search query. However, these same applications require users to abide by license agreements, require the modification of organizations' standard web browser deployments, and allow every URL accessed by the employee to be tracked accordingly. In this scenario, the employee in this case has signed the organization into a legally binding contract (the license agreement), and has potentially opened up internal web queries to MSN, Yahoo, or Google.</p> <p>Observations: 33% of the Finance respondents and 50% of the OD respondents indicated that they use search bars to aid in web content retrieval. ABC and Eclipsesecurity should consider emphasizing the ramifications associated with using search bars in subsequent awareness / training sessions. Lastly, ABC should consider developing, implementing, and enforcing a governing Internet acceptable use policy and supporting operating procedures to discourage the use of search bars. This is a critical consideration due to security threats that have been identified during the past 18 months regarding the use of search bars.</p> |
| Anti-virus software and/or a firewall are not installed on the computer I use to check ABC email while off-site (e.g., while at home). | 3 | 12 | 1 | 11 | <p>Commentary: All security controls on portable or remote controls must be maintained on the computer itself. These computer systems are not centrally maintained by infrastructure-based controls, and therefore must be equipped with isolated security applications, such as anti-virus and firewall software. Without these capabilities, most computer systems may be compromised very quickly.</p> <p>Observations: 20% of the Finance respondents and nearly 10% of the OD respondents do not use antivirus and/or firewalls on their remote computer systems. ABC and Eclipsesecurity should consider emphasizing the importance of using anti-virus and software firewalls on their remote computer systems in subsequent awareness / training sessions. Further, ABC should consider developing, implementing, and enforcing a governing security policy and supporting operating procedures to effectively manage the security of remote computer systems.</p> |
| When selecting my own passwords, I try to keep them as short and simple as possible so they are easier to remember. | 8 | 7 | 5 | 7 | <p>Commentary: Password selection continues to lead to an easy entry point for a malicious individual. Weak passwords, such as those that are short and simple in nature, are much easier to remember. However, these types of passwords are also much easier to guess / attack, resulting in the unauthorized and masqueraded access to ABC's information systems.</p> <p>Observations: More than half of the Finance respondents and nearly half of the OD respondents are currently using short and simple passwords. The awareness training session should continue to stress the importance of password selection and cover in detail the requirements and recommendations presented in ABC Information Security's password policy.</p> |

Analysis of Short Answer Responses

Provided in this section of the ISATP Assessment Report is an analysis of the responses received from the participating OD and Finance personnel to the short answer questions in the PAQ. Outlined below is each short answer question that was presented in the PAQ, and an analysis of the responses that were received from the respondents. Each series of responses are evaluated for each participating business unit / department (i.e., Finance and OD).

Finance

1. You receive a phone call from a vendor requesting ABC's internal phone directory, how should you respond to this solicitation?
 - All responses were respectable, appropriate responses. Most of the respondents indicated they would communicate that they were unable / unwilling to provide such information.
2. What types of financial information / documents do you feel are the most sensitive in your department / business unit? Please explain your response.
 - 8 of 15 respondents indicated that all financial information is sensitive.
 - The following types of financial information were identified by the respondents as being sensitive in nature: Budget, forecast, volume, and rate analyses, ABC bank information (i.e., routing numbers), ABC procedure manuals, ABC contracts, monthly financial statements, audit work papers, and employee's personal information.
 - The Finance respondents demonstrated a strong understanding of the sensitivity of the information they generate and handle as part of their responsibilities.
 - The Finance department / business unit generates and processes an extensive amount of confidential / sensitive information. It is imperative that ABC applies the security mechanisms necessary to ensure this confidential / sensitive financial information is protected accordingly. Additionally, appropriate governing ABC Information Security policies and supporting procedures should be instituted, implemented, and enforced to increase assurance that its confidential / sensitive information is sufficiently protected.
3. Please provide some examples outlining scenarios when you have or would contact someone in ABC Information Security for assistance.
 - 7 of 15 respondents have never contacted ABC Information Security for assistance, and/or could not think of an instance when they would contact ABC Information Security for assistance.
 - 3 of 15 responses related to the topic of computer viruses.
 - ABC and Eclipsecurity should consider communicating the most prevalent reasons / scenarios outlining when ABC Information Security should be contacted in subsequent awareness / training sessions.
4. Describe how you currently use your available file storage locations, such as the G: and S: network storage locations, your local computer desktop and My Documents, and any other external storage device (USB flash drive, hard drive, iPod, etc).
 - While the responses were diverse in nature, one consistent theme is confidential / sensitive ABC information is stored on network drives, as well as on ABC personnel's workstation hard drives and external storage devices. It is imperative that ABC applies the security mechanisms necessary to ensure its network environment is sufficiently secure to protect its confidential / sensitive information. Additionally, appropriate governing ABC Information Security policies and supporting procedures should be instituted, implemented, and enforced accordingly to increase assurance that its confidential / sensitive information stored locally on workstations and external storage devices is sufficiently protected.
5. Are there any situations you would like to share (personal or ABC related) where you experienced or know of someone that experienced a compromise (such as a personal computer that was

infected by a virus, spyware that was installed which caused an excessive number of pop-up advertisements, or a physical break in)? Please describe (if applicable).

- None of the respondents indicated any awareness of or involvement with compromises to computer systems. However, there appears to be a discrepancy since several respondents indicated in question 3 (above) that they have or would contact ABC Information Security with virus-related issues.
 - It is recommended that ABC institute acceptable use security policies and applicable procedures to help effectively address risks associated with virus exposure.
6. Please outline your biggest concern regarding the potential disclosure of highly confidential financial information. Do you feel this scenario is likely to occur at ABC? Please explain your response.
- 7 of 15 respondents indicated their biggest concern was individuals gaining unauthorized access to ABC's confidential information.
 - Responses to this question were mixed and in general very few comments were made indicating they believed inappropriate disclosure of confidential financial information could occur at ABC. Insider trading, early public release of information, information taken home that may be lost or leaked, dumpster diving, unauthorized access to files, and perceived credibility of information were concerns that were identified by the respondents.
 - It is recommended that ABC Information Security should consider developing a strategy, in addition to the ISATP, to help ease (yet not eliminate) these concerns to instill a greater confidence of ABC's secure business operations.
7. If you were to ever suspect unethical behavior was being / had been performed by one of your peers / supervisors, how would you report this issue? To whom would you report this issue?
- All responses were respectable, appropriate responses.
 - 11 of 15 respondents indicated they would inform their manager / supervisor (assuming it didn't involve their manager / supervisor).
 - 5 of 15 respondents indicated they would inform OD.
 - 2 of the 15 respondents indicated they would inform ABC's Ethics Hotline.
8. Which method of accessing email remotely do you prefer (e.g., Portal or Outlook Web Access)? Please explain your preference.
- 11 of 15 attendees responded to this question.
 - 6 of 11 respondents indicated a preference for OWA.
 - 1 of 11 respondents indicated a preference for the Portal.
 - 4 of 11 respondents indicated no need to access email remotely.

OD

1. You receive a phone call from a vendor requesting ABC's internal phone directory, how should you respond to this solicitation?
 - Similar to Finance; all responses were respectable, appropriate responses. Most of the respondents indicated they would communicate that they were unable / unwilling to provide such information.
2. What types of financial information / documents do you feel are the most sensitive in your department / business unit? Please explain your response.
 - All respondents indicated that OD information is sensitive
 - The following types of OD information were identified by respondents as being sensitive in nature: Salary, ABC benefits and personal information (social security number, date of birth, I-9, address, and tax information), promotion Forms, ABC confidential organizational issues (mergers and acquisitions, re-organizations), health related information.
 - A substantial amount of confidential information resides within OD related to the organizational structure and internal operations. To ensure the safety of ABC staff, contractors and temporary employees the information residing within OD must be protected using substantial measures to ensure the confidentiality and integrity.
3. Please provide some examples outlining scenarios when you have or would contact someone in ABC Information Security for assistance.
 - 5 of 12 respondents have never contacted ABC IS for assistance and/or could not think of an instance when they would contact ABC IS for assistance.
 - 3 of 12 responses related to the topic of computer viruses.
 - Similar to Finance; ABC and Eclipsesecurity should consider communicating the most prevalent reasons / scenarios outlining when ABC Information Security should be contacted in subsequent awareness / training sessions.
4. Describe how you currently use your available file storage locations, such as the G: and S: network storage locations, your local computer desktop and My Documents, and any other external storage device (USB flash drive, hard drive, iPod, etc).
 - Similar to Finance; while the responses were diverse in nature, one consistent theme is confidential / sensitive ABC information is stored on network drives, as well as on ABC personnel's workstation hard drives and external storage devices. It is imperative that ABC applies the security mechanisms necessary to ensure its network environment is sufficiently secure to protect its confidential / sensitive information. Additionally, appropriate governing ABC Information Security policies and supporting procedures should be instituted, implemented, and enforced accordingly to increase assurance that its confidential / sensitive information stored locally on workstations and external storage devices is sufficiently protected.
5. Are there any situations you would like to share (personal or ABC related) where you experienced or know of someone that experienced a compromise (such as a personal computer that was infected by a virus, spyware that was installed which caused an excessive number of pop-up advertisements, or a physical break in)? Please describe (if applicable).
 - A respondent is quoted in saying "A friend caught a virus with one of the computers I bought from ABC during their annual sale. I'm not sure if it was the computer or the emails they received that caused the virus. They used AOL as an internet provider."
 - It is recommended that ABC develop a policy regarding data remnants ensuring all storage-oriented systems all fully sanitized from ABC sensitive or proprietary information. The policy should be inclusive of not only laptop or desktop computer systems, but also other storage mediums such as cellular phones, pagers, blackberries, USB flash drives; any device with the capabilities of storing information.

6. Please outline your biggest concern regarding the potential disclosure of highly confidential financial information. Do you feel this scenario is likely to occur at ABC? Please explain your response.
 - 9 of 12 respondents indicated their largest concern was related to unauthorized access to ABC confidential and personnel information; 3 respondents did not have any concerns.
 - Responses varied; however they ranged from social security number theft, local My Document's folder protection, shared and personal drive access, and email transmission of confidential information.
 - One of the respondents noted an incident without resolution; the respondent stated "Health Documents are hard copy and the PC is not used to document health issues. We do not transmit personal info through email. I have experienced a break in to the HCC where personal records were found to be missing, along with medical supplies and the sharps container was stolen. ABC Security was informed and asked to document the missing files supplies. No resolution ever came."
 - Similar to the Finance recommendation, ABC Information Security should consider developing a strategy, in addition to the ISATP, to help ease (yet not eliminate) these concerns to instill a greater confidence of ABC's secure business operations.

7. If you were to ever suspect unethical behavior was being / had been performed by one of your peers / supervisors, how would you report this issue? To whom would you report this issue?
 - Similar to Finance; all responses were respectable, appropriate responses
 - 6 of 12 respondents indicated they would inform their manager / supervisor (assuming it didn't involve their manager / supervisor).
 - 5 of the 12 respondents indicated they would inform ABC's Ethics Hotline.
 - 1 respondent did not submit an answer.

8. Which method of accessing email remotely do you prefer (e.g., Portal or Outlook Web Access)? Please explain your preference.
 - 11 of 12 attendees responded to this question.
 - 4 of 11 respondents indicated a preference for OWA.
 - 2 of 11 respondents indicated a preference for the Portal.
 - 4 of 11 respondents indicated no need to access email remotely.
 - 1 respondent did not know the naming difference between the two systems.

Analysis of ISATP Presentation Evaluations

The ISATP Presentation Evaluation form consists of two sections. The first section is comprised of three (3) short answer questions. The second section consists of fourteen (14) questions. Each of these 14 questions is accompanied by a ten-point rating system where a rating of one (1) is the worst possible rating, and a rating of ten (10) is the best possible rating. As indicated in the Introduction of this ISATP Assessment Report, the primary objective of this evaluation form was to understand aspects of the pilot ISATP sessions that were effective, and aspects of the sessions that should be improved upon / enhanced.

Analysis of Short Answer Responses

The responses received from the respondents were very diverse in nature. The responses indicated that the participants derived strong value from the awareness and training session. While the responses received to the question inquiring what should be changed for future sessions were diverse, a somewhat prevalent theme was they the duration of the sessions should be reduced. This is a consideration that should be applied to future content that is developed and ultimately delivered by Eclipsecurity.

Analysis of Received Responses to 10-Point Rated Questions

Provided in the table below is a summary of the responses received from the participating Finance and OD personnel. The table provides the following information:

- Question: A reiteration of each question contained in the ISATP Presentation Evaluation form
- OD and Finance Results: Contains both an average and median of the ratings received from all respondents for each question
- Overall Results: Contains both an overall average and median of the ratings received from all respondents for all questions collectively
- Analysis of Responses: All averages and medians that are bold and red in color indicate concerns that are subsequently addressed by Eclipsecurity in this section of the ISATP Assessment Report. Each of the highlighted averages and medians are accompanied with an analysis. The purpose of the analyses are to provide insights explaining why these areas of concern are suspected to have occurred, and recommendations outlining how they may be addressed in future sessions. Each highlighted average and median is accompanied by a letter so the analyses may be correlated to each corresponding question.

| Questions | OD Results | | Finance Results | |
|---|-------------------------|------------------------|-------------------------|----------------------|
| | Average | Median | Average | Median |
| Was the purpose clearly stated? | 8.00 | 8 | 8.23 | 8 |
| Did the message support the overall purpose? | 8.17 | 8 | 8.31 | 8 |
| Were you able to relate to the content and find applicability in your daily duties? | 8.25 | 8 | 8.46 | 9 |
| Was the presentation content consistent with the stated purpose? | 8.25 | 8 | 8.15 | 8 |
| Do you feel that this is a reasonable amount of time to spend for attending this session? | 7.00^A | 7.5^A | 6^A | 6^A |
| Was the breakout session relevant to the covered material? | 7.29^B | 8^B | 7.69^C | 8^C |
| Did the session enhance interaction among participants? | 6.00^B | 6^B | 6.62^D | 7^D |
| Did the speaker show sufficient enthusiasm to maintain audience interest and participation? | 9.42 | 9.5 | 7.62^E | 8^E |
| Did the presentation flow smoothly? | 8.92 | 9 | 8.54 | 8 |
| Did the speaker build credibility on the topic? | 9.42 | 9.5 | 8.54 | 9 |
| Was the pace of the content appropriate? | 8.42 | 9 | 6.46^F | 6^F |
| Did slide structure support the presentation purpose and organization? | 8.25 | 8 | 8.15 | 8 |

| | | | | |
|---|------|------|------|------|
| Did slide visuals and movies support the presentation purpose and organization? | 8.25 | 9 | 8.23 | 8 |
| Were slide effects eye-catching and interesting without being distracting? | 8.58 | 9 | 7.62 | 8 |
| Overall Results | | | | |
| | 8.16 | 8.32 | 7.76 | 7.79 |

- A. Several respondents voiced concern over the longevity of the session; however, all attendees felt the content delivered was appropriate and required. A virtual delivery capability needs to be devised to complement the in person training session thereby reducing the required number of hours for any given period. An example of this is to leverage computer based training for the security awareness fundamentals, reducing the instructor led session to 2 – 2 ½ hours total.
- B. The OD session coupled the breakout session with a lunch-n-learn. Several respondents indicated that they did not even know that the session occurred. For future sessions a reduced timeframe for the awareness program and the removal of the lunch-n-learn will complement each other to ensure the attendees benefit from the breakout session.
- C. During the Finance session, it was articulated by several individuals that the breakout session movie clips were not very realistic examples for the ABC. For example, the pink slip virus was considered unrealistic by one individual who seemed to believe that ABC’s virus protection would prevent this scenario from happening. This is an opportunity for future sessions to address the “realism” of certain events that seem “unrealistic” at first sight.
- D. The Finance session was extraordinarily interactive throughout almost every aspect of the materials. The breakout session itself could be modified to create a two team approach, versus the instructor provoking thoughts on the movie clips (which may have lead to lower than expected scores).
- E. The lower than expected scores in this category are surprising, as the Finance session was extraordinarily interactive during almost every section of the program. It is suspected that the time of the day (e.g., attendees wanting to catch the train) and overall length of the session significantly contributed to these ratings.
- F. It was very apparent that attendees viewed the length of the session as too long (in this case, the pace of covering the materials as being too slow). Although the length of the program was required for the agreed upon content, it is clear that a shorter version of the session should be developed for the company-wide roll-out. In addition, the session ran right up to 5:00pm and it was noticed that the attention of the attendees may have been diverted towards leaving for the day. This outcome suggests that the duration of the presentation and the time of day remain important considerations for future sessions.

Analysis of ISATP Presentation Survey

The ISATP Presentation Survey consists of two sections. The first section is comprised of six (6) short answer questions. The second section consists of an area for participants to provide any comments they would like to have reviewed by ABC Information Security and Eclipsesecurity. As indicated in the Introduction of this ISATP Assessment Report, the primary objective of this evaluation form was to address aspects of ABC’s business operations that are of particular interest to ABC Information Security.

Analysis of Short Answer Responses

All questions, with one exception, contained in this section of the ISATP Presentation Survey were the same as the short answer questions contained in the PAQ. The responses received from the respondents were consistent for the most part with the responses received in the PAQ. However, it is interesting to note that the responses provided to the question inquiring about participants worst fears regarding information security were much more insightful and sophisticated than the responses originally provided in the PAQ. This is a good indication that knowledge transfer occurred during the pilot ISATP session, and that heightened security awareness had been achieved.

The one unique question relating to what participants' believed to be security risks that are currently being ineffectively addressed by ABC contained a resounding consistent set of responses. Six (6) of the eight (8) total participants that responded to this question (i.e., 75% of all respondents) expressed concerns related to ABC's physical security practices. Each of these respondents requested that ABC's physical security be enhanced accordingly.

Eclipsesecurity Lessons Learned

Outlined below are various insights that Eclipsesecurity gleaned during this pilot phase of the ISATP. It is the hope of Eclipsesecurity that these considerations be applied to all future activities that are conducted in support of ABC's ISATP.

1. The resounding response from the attendees was to include more internal ABC policy and adherence requirements. The attendees exuberated their need for guidance in information security.
2. Attendees were overall very eager to share their concerns, and had many questions about how what they do personally can significantly impact the ABC. This communication itself provides great evidence that employees are seeking answers and awareness to even the most fundamental information security concepts.
3. Attendees' discussions and interactions during all stages of the sessions demonstrated their ability to grasp and understand more complicated information security concepts such as why a remote access policy would be a good thing for ABC. The attendee's willingness to interact on security related topics is a good indication that the program will provide a very positive impact on the ABC's overall information security program.
4. It became evident that attendee awareness of ABC specific information security policies and procedures varied widely. This ranged from strong familiarity with policies to not realizing a policy even existed. It was also evident that certain policies were simply not followed (e.g., most attendees said employees don't display their ID badges) or were viewed as outdated and not applicable. This is another example that would support the need for continued awareness of ABC information security policies, standards, and procedures.
5. We noticed that the attendees were very interested in the "proposed" policies and procedures that were discussed during the session (such as the pending remote access policy). Attendees indicated some surprise that these policies were not already formally in place. This provides evidence that employees would embrace rolling out new and updated security policies versus viewing them as another information security group obstacle.
6. All attendees felt the covered material was on target in regards to content applicability; however, several voiced concern regarding the length of the course overall. A topic of conversation has been to move the generalized security awareness training in to a web-based session, thereby reducing the overall length of the instructor led session to 2 – 2 ½ hours. The web-based course can be made mandatory and required by attendees to review prior to attending the instructor led session.
7. Morning based sessions provide a much better venue for the delivery of the content versus afternoon sessions. The attention level and aptitude to learn new material required for the ISATP needs to be at its highest level and studies have shown that responsiveness and capabilities to learn are at their peak during the morning hours.
8. Breakout sessions should not be mandatory for each delivery of the ISATP as in the current deliveries of the course interaction was already at its peak simply by delivering the content. It is recommended that the breakout session material developed be used to reinforce concepts or provide an interjection of humor to the delivery of the program if needed. The breakout sessions can also be used to force interaction if necessary. The concept could also be used as a reinforcement mechanism (potentially an online version) to sustain certain aspects of the ISATP.
9. Consider moving some of the Operations Security slides to the beginning of the session to stimulate a broader range of attendee interaction and participation.
10. During the Finance session, attendees expressed great interest in understanding exactly what cookies are and how they are used by browsers and websites. Adding a slide on this topic could be valuable to participants.