The Habits of Highly Successful Security Awareness Programs: A Cross-Company Comparison

Researched and Written by

Samantha Manke
Samantha@isag.com

Ira Winkler, CISSP
ira@isag.com

Sponsored by

35 Sunset Drive
Severna Park, Maryland 21146
www.isag.com

4620 Henry Street
Pittsburgh, PA 15213
www.wombatsecurity.com

Executive Summary

Although security professionals talk about the value of security awareness programs, these programs vary greatly in quality and effectiveness. Security awareness is a difficult type of program to implement, because it requires actively engaging an audience that often does not understand security, and frequently vigorously fights security. Today, many companies have awareness programs, and many companies are required to demonstrate that 100% of their employees participated in the program. The failings of such programs can be catastrophic, creating not just a security related loss, but also critical damage to the brand and reputation of the organization. Additionally, security awareness programs are allocated limited budget, and security managers need to know how to make the most use of what limited resources they have. By comparing what works and what does not across companies of different sectors and sizes, clear recommendations of the most effective security awareness strategies emerge.

To determine the critical success factors of security awareness programs, the security awareness programs of Fortune 500 companies were studied using qualitative (interviews) and quantitative (surveys) methods. To validate the results, end users and members of the security staffs were also surveyed. Analysis of the findings led to the determination of what habits can greatly improve security awareness efforts.

While the study produced many recommendations, and this white paper discusses all of them, the measures that created the greatest likelihood of security awareness success are:

- Obtaining C-level support
- Partnering with other key departments
- Proactive metrics collection
- Security awareness programs administered in 90 day cycles
- The use of creativity in disseminating materials
- Participatory training versus video-based training

It is also notable that many of the most common awareness measures proved to be ineffective in improving security behaviors among end users. Perhaps the most critical issue is that the once a year mandatory video sessions that are the core of many security awareness and compliance efforts are not only ineffective in improving security-related behaviors, they cause the end users to have negative feelings towards security efforts.

The information presented in this white paper can help security departments create new security awareness programs, as well as enhance and improve ongoing security awareness programs. It is most important to note that these recommendations are not to improve training techniques, but to create a program that impacts user behavior.

Contents

Executive Summary ii

Introduction 1

Study Methodology 2

Analysis of Interviews 3

- **Company A** 3
- **Company B** 3
- **Company C** 4
- **Company D** 4
- **Company E** 5
- **Company F** 6
- **Company G** 6

Analysis of Survey Data 7

- **Security Employee Responses** 7
- **End User Responses** 12

Findings 16

Study Limitations 18

Recommendations for Security Practitioners 19

- **Acknowledge Security Awareness is a Distinct Discipline** 19
- **Assess Organizational Security Culture** 19
- **Obtain Executive Management Support** 19
- **Choose Topics Most Relevant to the Business and Culture** 20
- **Partnering with Other Departments** 20
- **Utilize Participatory Awareness Tools** 20
- **Use Creative Measures** 20
- **Collect Metrics Proactively** 21
- **Consider Outsourcing Training and Awareness Tasks** 21
- **Department of How** 21
- **Implement 90-Day Security Awareness Plans** 21
- **Multimodal Awareness Materials** 22

Short-term and Long-term Tasks 23

Summary 25

Contact Us 26

Introduction

Although security professionals talk about the value of security awareness programs, these programs vary greatly in quality and effectiveness. Security Awareness is difficult to implement and security awareness efforts frequently meet with resistance from end users and frequently even security practitioners. While people and the news media highlight humans as the most vulnerable attack vector, there are few countermeasures that seem to adequately address the problem. Many decree security awareness as the most powerful security countermeasure you can employ, yet we see countless examples of security awareness failings that lead to devastating losses.

Clearly, it is not that security awareness is a flawed security strategy, but that the people managing security awareness programs employ measures that vary greatly in both quality and effectiveness. The technical analogy would be comparing a well-maintained, commercial firewall with a poorly maintained firewall, written by a security enthusiast in their spare time. Sadly, when security awareness is concerned, the acknowledged discipline of using high-grade countermeasures that are properly maintained does not follow into security awareness efforts.

Many security practitioners seem to acknowledge that good security awareness programs utilize scientific principles, just like a good firewall is created with good software engineering principles. Therefore, there is value in determining what principles to utilize when creating and managing security awareness programs. To address this issue, a study was performed that examined a variety of factors related to what leads to the success or failure of a security awareness program. The lead researcher is well versed in sociology and anthropology, which allows for a thorough examination of the factors that lead to security culture improvements.

The last point is perhaps the most critical aspect of the study. Per NIST 800-50, there is a distinct difference between training and security awareness. Specifically, training, at least as far as information security is concerned, involves ensuring specific guidance is provided to an individual so that they understand risks and know how to avoid them. Training is appropriate for providing the specific knowledge required by compliance standards, such as HIPAA and PCI, as well as to reduce organizational risk of employee susceptibility to all cyber-attack. For example, the standard 15-minute video that companies give to their employees once a year ensures that there is a program in place that provides required information, however it shouldn't be considered training. It does not ensure that the people will behave securely, but they have at least been told what the risks are.

Alternatively, awareness training specifically intends to change behavior and culture. It aims to provide information that impacts daily actions. That requires a drastically different approach than just providing information. This is why most security awareness programs fail. As many security professionals confuse training with awareness, they provide basic security training to end users and then attribute security incidents to awareness as a failed security countermeasure, as opposed to the quality of the overall awareness program.

For these reasons, it is worth examining what are the elements of a good awareness program. User awareness can prevent a wide variety of technical and non-technical failings. Additionally, they are also low cost when compared to other security countermeasures. This white paper discusses the findings from a study designed to determine the critical success factors of good security awareness programs.

Study Methodology

Security awareness practitioners of Fortune 500 companies were approached and asked to participate in the study. Those companies that agreed were subjected to both quantitative and qualitative data collection.

The quantitative data collection first involved a questionnaire that collected data anonymously from the participating companies' security staff. A total of 50 security personnel responded to the survey request. They were asked to answer the questions using a Likert scale. A neutral option was purposefully left out to force participants to answer the questions. They were given the option to choose "Non-Applicable" as not every question would pertain to every member of the security team, if they were not directly involved in security awareness.

An anonymous questionnaire was administered to end users in the participating companies to garner evaluations of the effectiveness of the programs. A total of 40 end users responded to the survey request. The idea behind this survey was to obtain the opinion of a non-biased source as to the success of a company's security awareness program. This data was coded by way of highlighting commonly used words to analyze and spot significant trends among companies using security awareness programs.

Qualitative research involved interviews with the people responsible for the security awareness programs in their respective companies. This was a highly successful component of this study as participants were very open and willing to share their experiences. The data from these interviews was analyzed to find commonly reported answers and experiences. From an analytic perspective, qualitative data collection, which involves thorough data collection, assists in mitigating concerns about small sample sizes.

The data was analyzed to determine what security awareness measures are considered effective. Successful measures were also extrapolated based upon the factors that led to failures. For example, a critical failing of most security awareness programs is that they did not collect metrics prior to beginning awareness programs. Proactive metrics collection was therefore identified as a factor that should be part of an effective awareness program.

We additionally validated the research by conducting roundtable sessions at security conferences around the world. More than 200 senior security practitioners provided their opinion of effective and ineffective security awareness measures. The roundtables, while not a complete scientific validation of the findings, confirmed that that the geographical limitations and relatively small sample size did not impact the validity of the findings.

Analysis of Interviews

The following sections summarize the interviews with the people running the security awareness programs within their organizations. Anonymity was promised to all participating organizations, so the market sectors and other potential information that can be used to identify the companies has been removed. All participating companies are Fortune 500 companies. In total, the participating companies represent 5 major market sectors. Most companies are considered multinational, and all are considered major players in their market sector.

Given the size of the companies, most companies must adhere to a variety of regulations and compliance standards. For example, most companies need to adhere to HIPAA regulations, while many companies must adhere to PCI standards.

All interviews were face-to-face and were not recorded to provide a comfort level to the people being interviewed. The steps that would be taken to protect the anonymity of the participating organizations were identified. The interviewer has extensive training in interview techniques.

Company A

Company A utilizes a variety of methods to engage their employees. They use posters, a website, department presentations, lunch and learn sessions, and weekly awareness campaigns. This company recently started their program. It is a relatively new program within the organization, but is run by security staff that specializes in security. It received complements from the local security community, particularly for being a start-up program. The security team has been able to see a change in several ways. The program improved relations between the headquarters and remote locations. The remote locations have been included in the initiative and given supplies to use for their employees. Non-headquarters' employees are traditionally excluded from corporate activities. The team already received increased cooperation from these sites on other projects. It also built relationships with other departments that the security department collaborated with for special topics (i.e. Legal for document retention and Marketing for social media). To measure the success of their program, the security department studies the metrics of the number of visitors to their site regularly, but also following special events to look for a spike in activity.

Security is a new department for the company; this is the first time that the company has had full-time security staff. This company only has to comply with limited HIPAA regulations. The security team struggles outside of the security awareness initiative with a weak security culture. Many employees actively fight security by way of filing business cases against security initiatives and management regularly decides against the security department. A common comment given to the security team is that the company's business negates the need for security.

Company B

Like Company A, Company B has a relatively new security awareness program. They hired a new director of security three years ago who has drastically improved the security posture of the company. Prior to that time, there was only a loss prevention department. The people managing the security awareness program have a security background. Despite the strength of this awareness program, there is significant room for growth. It is not where the company wants it to be. It is fairly limited right now. They conduct monthly meetings within I.T and have quarterly awareness meetings. They also utilize posters, a yearly preparedness month, and an information security

week. They also have an internal social media site that they utilize to broadcast security related policies and incidents. A common comment the security team receives is "Why do we need to care about I.T. security?" The spirit is there but the security culture at this company is weak. They are trying to grow the security awareness effort and know the C.E.O. believes in it, but not enough to push the message down. Accordingly, they still receive pushback from other departments. The corporate security culture is permeated with the belief that security impedes business processes. About 40% of end users, understand the need for improved security practices, but the remaining employees shun enhanced security practices.

Company C

Company C has a well-developed and successful security awareness program. They also have the largest security awareness budget of all companies studied. The large budget resulted from executive management concerns about security, and this allowed for a massive overhaul of security awareness efforts. The awareness team credits requirements for the amount of funding they receive. They have to prove that they educate every employee about security awareness. They also credit the T.J. Maxx security breach as a trigger for the revamping of their program.

The company is quite creative with their initiatives. They use a lot of "guerilla marketing" in their campaigns to build up excitement, before they reveal that security is behind the initiative. For example, they printed coffee cozies (the cardboard bands that go around coffee cups to protect your hands) with different security slogans for a week before revealing that security provided them. They have done similar things with posters. They created a cube in the main lobby with 10 security violations and held a drawing for employees that could identify all violations. They have also set up an event where employees could come watch a security-related movie and enjoy popcorn. They also have handed out toothbrushes and other things to bring home with the idea that if people practice security at home, they will be more likely to behave securely in the office. They created amusing videos for their corporate and retail employees. They also conduct contests and distribute prizes to engage employees. Lastly, they have a website and a bi-weekly newsletter with security tips. They believe that more fun activities get employees to think positively about security on a regular basis, which helps with engaging employees on less appealing tasks. They created an email address that allows employees to easily send security-related questions to the security staff. This effort is extremely successful and they have a difficult time responding to questions in a timely manner.

Company C hired a non-technical employee, with a communications and advertising background, to manage the security awareness program. The security department struggles to gain respect within the company, and strives not be seen as the "no department". They get many questions about the money the department receives and comments about how other employees think security awareness efforts are a waste of company resources. They remind people that a single incident can result in huge fines and a loss of brand reputation, which can cost the company hundreds of millions of dollars. Most employees assume they are doing things correctly unless told otherwise.

Company D

Company D like the first few companies, has a relatively new security awareness program. They had a mediocre program for many years, but decided to start from scratch 3 years ago. The former person in charge of the program would visit their sites and tagged apparent security violations, but there was no follow up to correct the violations. They hired an employee with no security background, but a specialty in communications, to manage the program.

They use a variety of mechanisms, but rely on a newsletter and trips to each of their clinics to do security presentations as the main source of education. An incentive of lunch was added to the presentations to increase attendance. They recently renovated the security awareness website. They also perform prize drawings and hold a security awareness week in October. They hand out lunch bags with their company's security slogan during this event. They have two characters that they use as mascots on their printed materials. The lunch bags are reportedly popular within the company. They use some posters as well. Some of their efforts focus on issues related to home security with the idea that if employees are secure at home, that will improve security practices in the workplace. They also do their own semi-annual survey to measure the success of their initiatives. Lastly, they began to partner with Privacy, a separate department, to conduct mandatory training. They also partnered with Acquisitions, and also work with the Human Resources department to perform training for new employees.

Company D's security department really struggles to be successful. They receive pushback on almost all efforts. They often hear that security is getting in the way of their company's initiatives. The organization is subject to regulations and will face significant fines if violations are found. The security department believes they have their work cut out for them when it comes to security awareness, because few people seem to care about security efforts, unless it appears that the security team is telling them not to do something. The security awareness team avoids educating end users on security related policies, because they believe no one reads them. Corporate communications frequently rejects security awareness related internal distributions. The company has the perception and reputation of being secure but they feel they don't have enough money or people for this to be a reality.

Company E

Company E has a relatively new security awareness program. There was a management change about 18 months prior to performing this study, and executive management ordered an enhanced security awareness program. Company E has hired an employee with a marketing background, instead of a security background, to manage the program. The company has many of the same concerns of other participating companies, specifically complying with regulations. However, they run their security awareness program differently. They do not use the soft, friendly approach that other companies implemented. They instead focus their efforts on training. They have a newsletter and created a list of security tips for employees to keep on their desks, but do not use any of the same techniques as the other companies studied. They felt that training was the best use of their resources. They partner with their Privacy department to help force their employees to complete the training. They offer an incentive, specifically if employees can pass a test before taking the training, they do not have to complete the training. The test is not particularly difficult, but it does require some security knowledge.

Like every other company, Company E fights to change their security culture. They feel generally disrespected by other departments and are seen as the "Department of No" as well. They say that it has been difficult to change the corporate security culture. Security awareness is not seen as a fun component, but a challenging component of the security team's work. They find it hard to engage their general population. They say that employees generally understand the different regulations that apply to their company, but the employees do not understand how it affects their day-to-day work. They often hear that "this is how we've always done things." Outside of their team, they also find it difficult to get support, especially from management. They have to "twist arms" to put up posters.

Company F

Company F is unique from the other companies interviewed, as they have an older security awareness program. This company is subject to regulations and will be heavily fined, if they are found to be in violation. They spend most of their budget on training, but the training is mandatory for every employee due to the compliance requirements. For this reason, they focus most of their efforts on educating on their particular compliance needs. The company also utilizes some posters, but it doesn't seem like the security team values posters as a medium for spreading education within the company. They also develop quarterly magazines and hold security trivia contest for employees, with the opportunity to win prizes.

Their security culture also seems to be exemplary. They do not receive much pushback from other departments, because every employee seems to understand, at least on a basic level, how important security is to the industry. The security awareness effort also receives strong support from upper-management on their projects. They have been credited with reducing attacks on their company as a result of their awareness efforts.

Company G

Company G is a processed and packaged goods company. They use many of the methods that other companies use. Their program has been in place for more than a decade. What is however unique about the company's security awareness effort is the management of the program. Specifically, while a single person is assigned management of the program for a three-year period, the security awareness team uses one person from each of the company's business unit to staff the effort. They collectively meet the third week of each month over a web conference to include employees from remote locations. At the meeting, they discuss what they would like to accomplish for the month and employees can sign up for the tasks that they find interesting. This helps encourage participation, as they are not forced to, for example, write an article on a topic that they do not find engaging.

The company engages in many of the same activities as the other companies studied, such as handouts, posters, and a week devoted to security awareness that includes, games, prizes, and other various activities. They do several things that other companies do not do, including bringing in speakers. Past speakers included local security experts, who present topics that will be interesting to the larger population of the company. They do live broadcasts of these talks, as well as record the sessions and place them in an archive to allow employees to watch the session at a convenient time. They place some emphasis on policy and physically pass out new security policies to employees when they are released. They plan to have training modules in the future but have not yet integrated that into their program.

Like the other companies, they have no metrics available to assess the success of their program. They face some of the same struggles in trying to engage a population that is not excited about security. They report that the security culture is changing since the instatement of a new manager. They have been actively trying to break the "Department of No" mentality.

Analysis of Survey Data

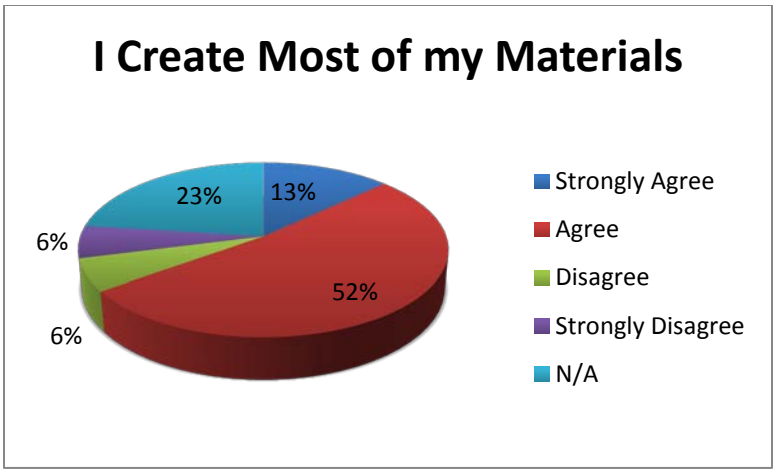
Presented below are a selection of questions and responses posed to the relevant employees within the participating companies. While these results are not broken down by the individual companies, they do represent a comprehensive view of security programs.

Security Employee Responses

The following questions were posed specifically to employees in Security departments within the participating companies.

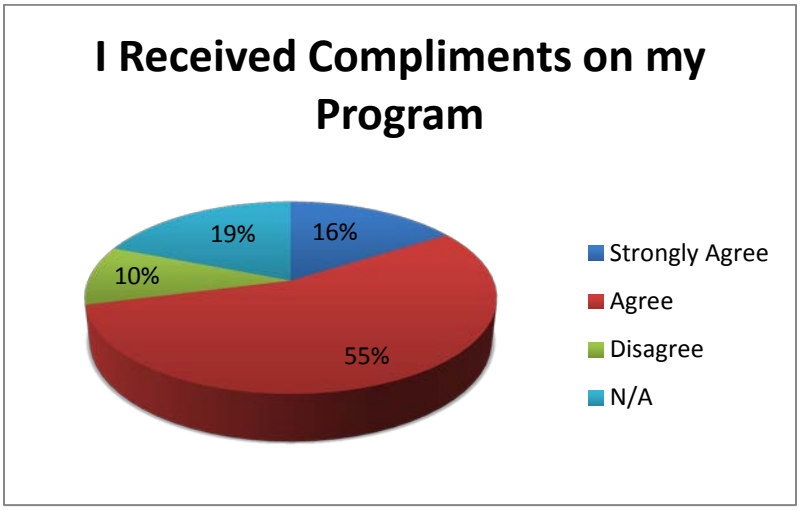
Graph 1.1—Gauging the Success of the Security Awareness Program

Interestingly, the reported responses to this question differ greatly from the reported responses to this question when administered in a face-to-face interview. During the qualitative portion of this study, respondents reported that their programs were not successful or at the very least, had room for improvement. As evidenced in the graph above, 87% of respondents reported that their programs are successful.



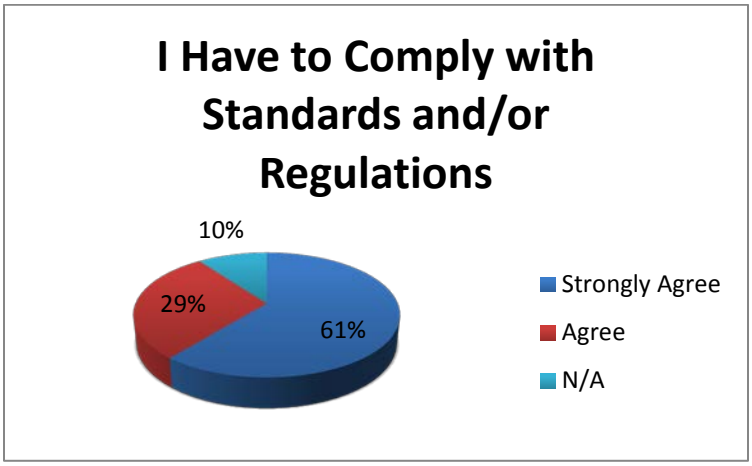
Graph 1.2--Creation of Awareness Materials

Security awareness materials can be created to be specific to the needs of a company. There are also vendors that create materials that can be purchased and distributed, but that will not be tailored to the specific needs of the company. These materials address common topics that have mass appeal. This question was designed to find out how much effort companies devoted to the creation of their materials. The majority of companies create most of their materials, with the minority of 12% purchasing their materials from vendors. As security employees who are not familiar with the details of the security awareness program participated in the survey, this explains the "N/A" as they are likely unaware of the exact components that are used in their company's program.



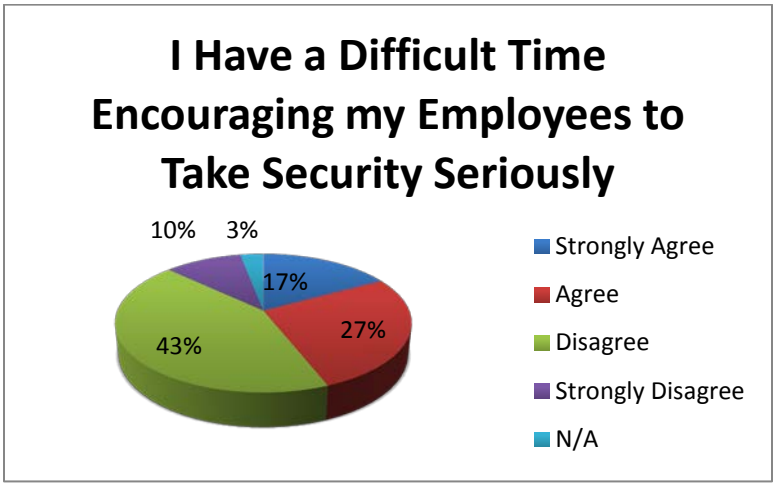
Graph 1.3—Compliments on Program

This question was designed to gauge how others within the respondents' companies view the security awareness program. The responses to this question also differ from the responses received when gathering qualitative data. Many respondents voiced frustration and a feeling of a lack of respect from their co-workers concerning their security awareness program and security in general. As evidenced above, 71% of respondents reported that they had received compliments on their program. This does not negate the reported qualitative data, as it is possible that employees receive both compliments and criticisms of their program.



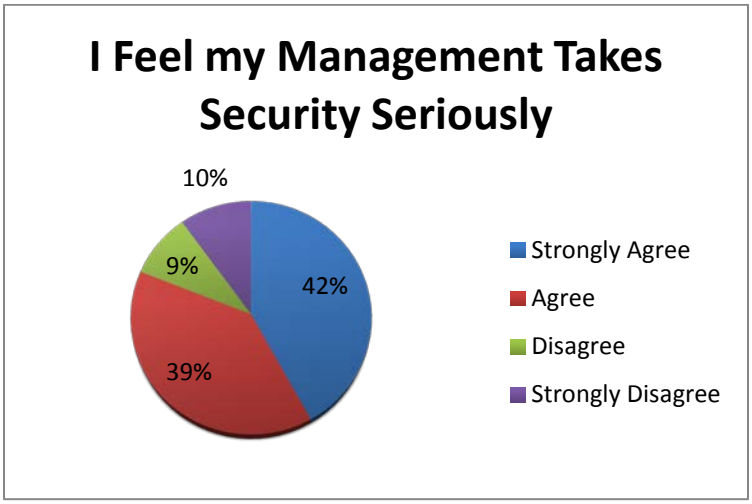
Graph 1.4—Compliance and Regulatory Requirements

This question is pertinent, as many standards and regulations require companies to prove that they have a security awareness program in place that reaches every employee within the organization. As evidenced above, every company has to comply with at least one standard or regulation. As every company stores personal information about their employees, every company has to comply with HIPAA, even to a limited extent. Many participating companies also had to comply with PCI regulations, which require security awareness programs. If companies did not have to comply with standards or regulations it may have affected the quality of their security awareness programs.



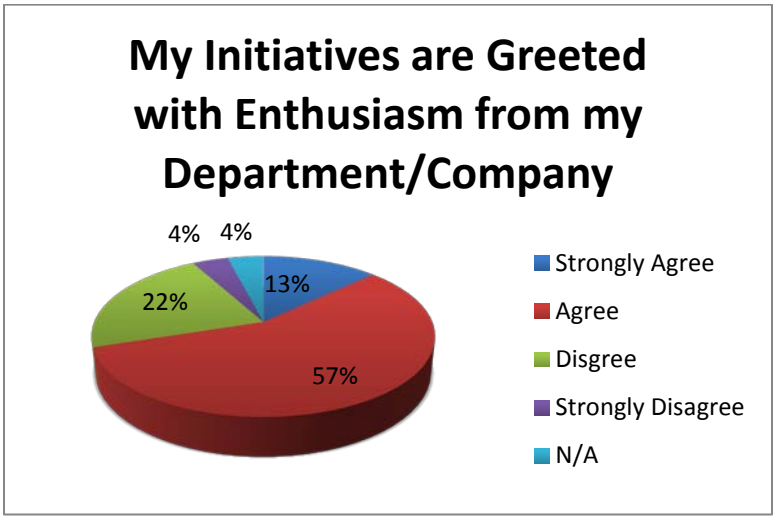
Graph 1.5—Perceptions of Employees Views on Security

This question gauged the security culture at the participating companies. The responses were almost an even split of 50% agreeing and disagreeing with the posed statement. This is an important finding because it highlights the need for security awareness. Even if roughly 50% of respondents have difficulty encouraging their co-workers to take security seriously, this leaves an incredible amount of room for improvement. It also highlights the opportunity for further study; specifically why do employees fight security so vigorously?



Graph 1.6—Management's Attitude Towards Security

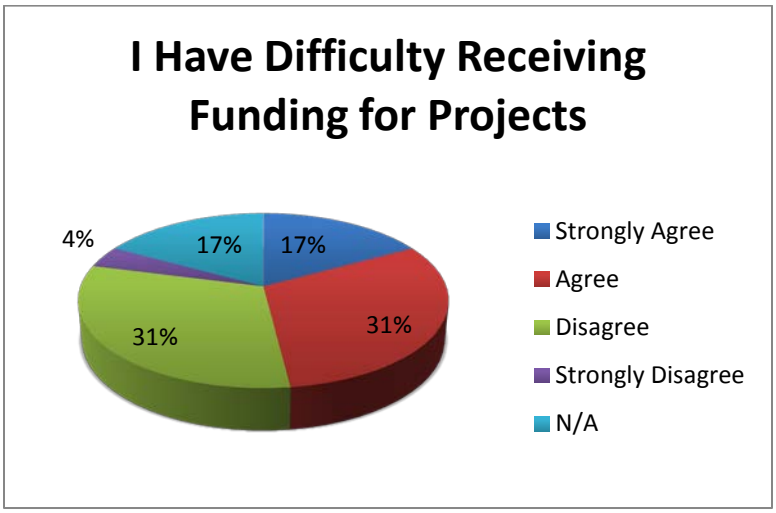
The responses to this question also differ greatly from the reported qualitative responses to the same question. Many respondents reported a lack of support from their management during face-to-face interviews but only 19% of anonymous respondents reported feeling a lack of support from their management. This would be an incredibly positive result, if it didn't differ so greatly from the reported qualitative data. The reason for the discrepancy can only be surmised, but it is likely that respondents were more uncomfortable with reporting a lack of support on an anonymous survey, because it was in writing and was traceable via an I.P. address, and while the qualitative data gathering was not anonymous, it was not recorded.



Graph 1.7—Enthusiasm Within the Security Department

The responses to this question are also in stark contrast to the reported answers given during the interviews. Many interview respondents reported feeling a lack of support and enthusiasm for their program. Some respondents reported a lack of support from key departments that created an impediment to even distributing materials. Others

reported the snide remarks they heard from their co-workers to the effect that they felt that security awareness was a waste of money for the company. Despite this, only 26% reported similar feelings on the survey. Again, the reasons for the discrepancy can only be guessed, but it is an interesting finding nonetheless.



Graph 1.8—Ease of Funding

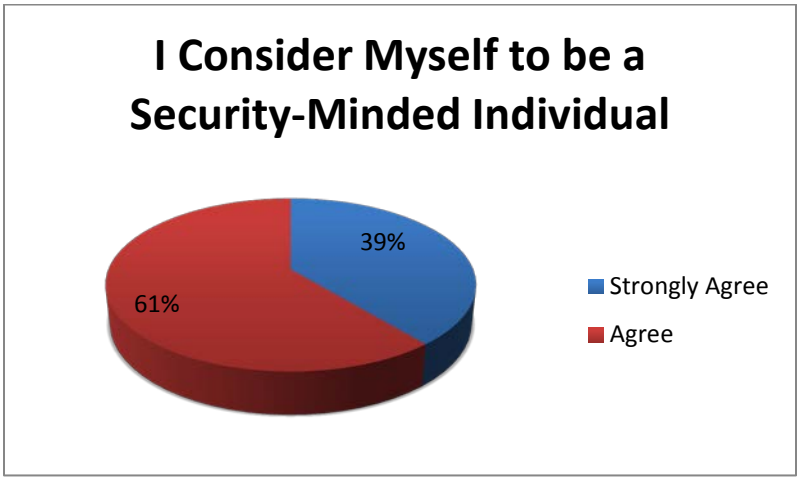
Many respondents reported having difficulty receiving funding during interviews. This is an indication of a lack of support for security and security initiatives within these companies, which seems to be in complete contradiction to the findings from quantitative data represented above. It could be the symptom of a larger problem within the organization that there is a general difficulty in receiving funding, but it is interesting to note and warrants further investigation. A more effectual pitch to upper management explaining the benefits and cost-effectiveness of security awareness programs may help with budgetary issues.

End User Responses

This section details the questions asked to employees that can be from any department within the participating organizations, except for the Security department. These people represent what we would refer to as the End Users.

Graph 2.1—Educational Value of Security Awareness Programs

100% of all non-security employees reported having learned something from their company's security awareness program. This is a significant finding as no matter the amount of struggles the security respondents reported, their programs are at the very least somewhat effective in educating their employees on security concerns or the reported statistics would likely be much different.



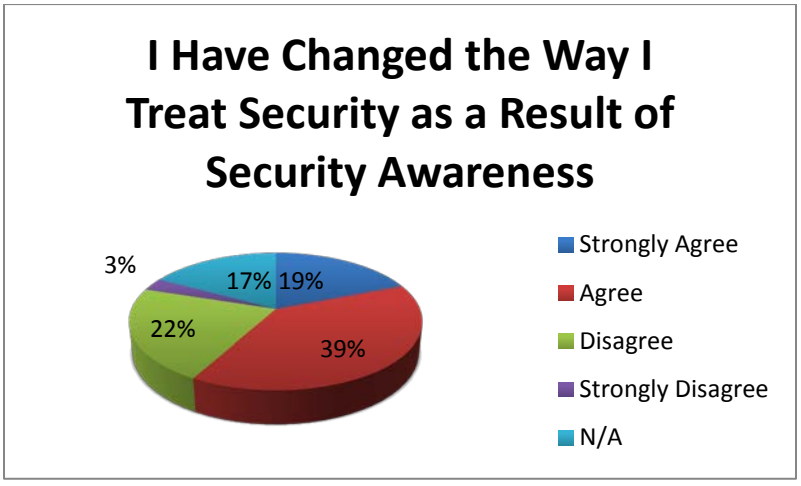
Graph 2.2—Security Self-Perception of End-Users

This finding is interesting because it differs from the reported responses from the security team, both qualitatively and quantitatively. 100% of surveyed end-users reported that they consider themselves security-minded individuals. This provides an opportunity for further study to see what behaviors stem from this security minded attitude: does being a security-minded individual translate to security behaviors?

It is also important to consider that if end users believe they are "security minded", they may believe that they are exercising the proper behaviors by default. However, as stated, the security teams do not believe their end users are security minded, which means that they do not exercise proper security behaviors. It is therefore likely that the end users do not realize that their behaviors endanger themselves or their organization.

Graph 2.3—Perceived Success of Security Awareness Among End Users

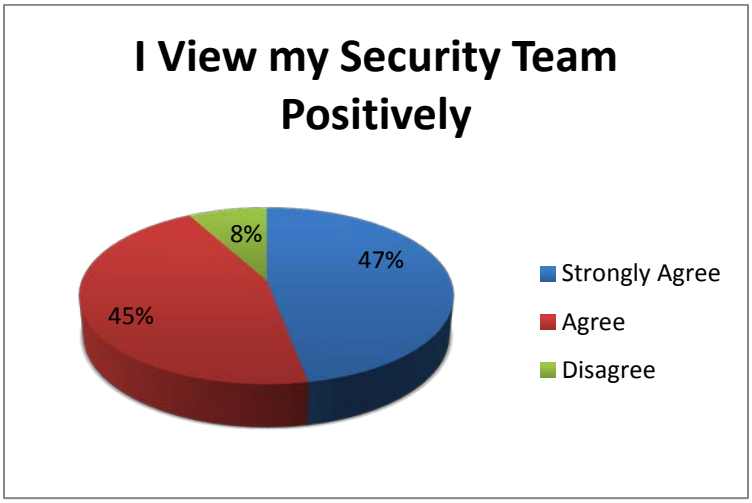
This graph is also telling: 100% of end-users reported that they find their company's security awareness program successful. As these respondents were not included in the qualitative portion of the study, there is additional opportunity to interview end-users to gauge what they consider a successful program to be. The limitations of the study may have impacted the responses to this question but only further study could confirm this. If the limitations of this study did not affect the responses to this question, this is a very positive finding.



Graph 2.4—Resulting Behavioral Change

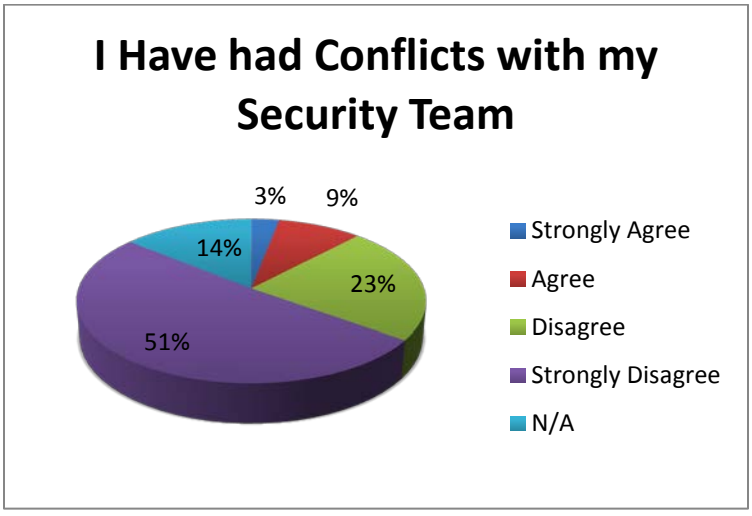
This question specifically examined the perception among end-users as to if awareness training accomplished its fundamental goal of creating improved security behaviors, and therefore strengthening the security culture of the organization. This finding is very interesting, especially in conjunction with the previous findings. Only 60% of

respondents reported having changed the way they treat security as a result of their company's security awareness program. While 100% have reported learning something from the program, only 60% alter their behavior as a result of what they have learned. This also presents an opportunity for further study of how to change the behavior of 100% of employees who learn something from their company's security awareness program.



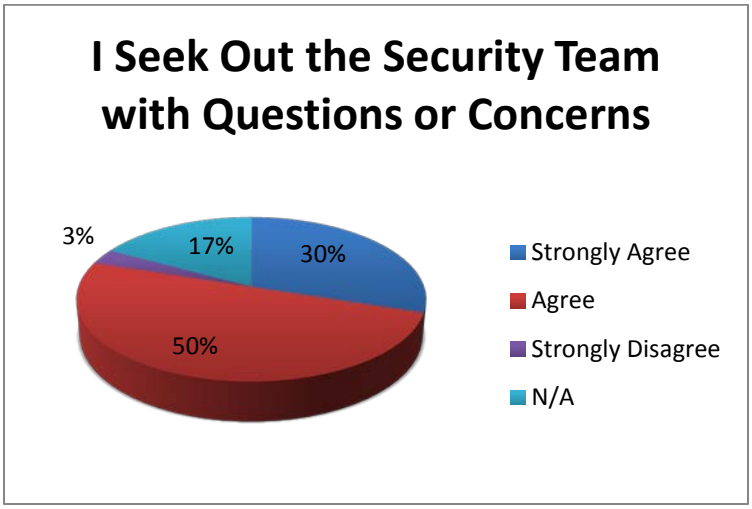
Graph 2.5—Perception of the Security Department

The results from this question are also worthy of note. Despite the reported results, both qualitatively and quantitatively, only 8% of non-security employees report viewing their security team negatively. Many security employees reported negative attitudes from end-users within their organizations with regard to their security awareness programs and other initiatives. This may be due to the reported limitations of this study but would necessitate further study to confirm this possibility.



Graph 2.6—Conflicts Between Security and End Users

Similar to the finding above, the responses to this question seem out of line with the reported responses from the security employees interviewed for this study. Only 12% of respondents reported having conflicts with their security team. The security employees reported conflicts as commonplace at their companies. This, again, may be due to the speculated limitations of the study but warrant further study to confirm this theory.



Graph 2.7—End User Comfort Seeking Out Security

This question was posed in order to examine the security culture from another angle. End-users were asked if they had conflict with the security department but were also asked if they sought out the security team. An overwhelming 80% of respondents reported seeking out their company's security team with questions or concerns. This fits with some of the responses given by security employees as some companies have a devoted channel for employees to pose questions or concerns. The response seems incongruent with the reported hostility that security employees feel at their companies but warrants further study.

Findings

Based on the surveys and interviews, an analysis of the collected data produced the following findings. While there are other findings that may be identified, these are the ones that can be generalized from the research. While some of them might seem obvious, by identifying them through research, we are able to identify potential measures to mitigate problems, as well as proliferate measures that can improve security.

Security is difficult to administer at most companies

Nearly all respondents reported having conflicts with other departments and employees outside of security. The mentality that security is synonymous with enforcement and prevention is really prevalent throughout all participating companies. There are varying degrees of reported difficulty: some experience it with C-level management and obtaining funding, others with the general user population, and still more within the "I.T" or "I.S." departments and a lack of respect from would-be peers. Changing these attitudes and perceptions would be cause for additional research. Research into changing these attitudes and perceptions is strongly warranted. The process to change these conflicts would be conducted on a case-by-case basis and the same process would not work for every company.

PCI compliance helps with enforcement and awareness

One recognizable trend is that companies that are forced to comply with the PCI regulations are more successful in gaining respect and support when it came to enforcement of security practices and administering an awareness program. PCI, as previously stated, requires the affected company to show that they have taught every user about their security policies and that they have a security awareness program. This makes funding easier to achieve, as there is an easily demonstrable need. A company that does not have to comply with PCI regulations will surely have information that is important to protect but they will not face the same fines if they are found to have breached sensitive data. They may suffer a loss of revenue or reputation but it is more difficult for them to sell the need for a security awareness program to upper-level employees that control their budget. Companies that have to comply with the PCI regulations also report having an easier time gaining the cooperation of other departments in their efforts, for example Corporate Communications. Companies that have to comply with HIPAA regulations or no regulations report difficulties in gaining the same level of cooperation.

Creativity and/or participatory training are the key to success

While heavily based in security culture, companies that have more creative endeavors are more successful than companies that rely on basic awareness measures such as posters and trinkets. Companies that thought outside the box to create their own materials and activities not only had greater engagement from employees but also increased cooperation from other departments that they worked with to administer their security awareness program.

While the previous paragraph implies that internally developed programs are the most successful, there are two important caveats to that statement. First is that this only applies when "creative" training is applied. This implies that the security awareness practitioners actively attempt to create new methods for reaching the company. The second caveat is that high quality, commercial training tools, that provide participatory training experiences, are also highly effective.

Companies that used participatory training as a component of their security awareness program were more

successful in gaining the cooperation and the participation of their employees. Training tools from Wombat Technologies provide an experience that end users consider fun and engaging, and led to more effective change in security behaviors.

Companies with more top-level support are more successful

This finding may be obvious but it is important to note: Security departments that have garnered the support of top-level management are more successful in all of their endeavors, including security awareness. They are able to procure more funding than departments that lack this support and they have an easier time initiating security awareness programs. The responsibility of obtaining this support rests with each security department, as they need to prove the value of their work and the added value of having a security awareness program at their company.

Study Limitations

All research has limitations, which do not represent flaws in the research, but point to areas where further research can be performed. Also, proper disclosure of the limitations allows practitioners to determine the practicality of applying the research findings to their environments.

Some limitations could have been prevented, but may have resulted in decreased levels of participation. For example, participating companies were allowed to distribute the link or paper survey to participants in a manner that they saw fit, but were told that it should be a random sample. The overwhelmingly positive responses from end users creates suspicions as to whether the surveys were randomly distributed or they were sent to end users who were friends with the security staff. As previously noted, the findings from the survey of the security practitioners produced different findings than the one-on-one interviews with the people running security awareness programs.

For those reasons, our recommendations are primarily based on the interviews. It is our determination that the interviews produced honest responses, and those findings were consistent with the results from the roundtable workshops held with security practitioners from around the world. Similarly, while the study involved a small number of companies in a limited number of market sectors, the roundtable findings confirmed our resulting findings and recommendations.

We however encourage further research to expand on our findings.

Recommendations for Security Practitioners

We base our recommendations on information that was either clearly defined by an analysis of the data, or can be readily extrapolated from the findings. A previously stated example is that given that a lack of metrics was said to be a failing of all security awareness programs studied, proactive metrics collection would clearly lead to stronger awareness programs. While not all recommendations are directly applicable to all organizations, they are a starting point for creating or improving all security awareness programs.

Acknowledge Security Awareness is a Distinct Discipline

While this recommendation might seem extremely basic, it is unfortunately ignored. All too frequently, since security awareness is not a specific technical discipline, it does not get the respect of requiring a unique knowledge base and skill set. The research found that many people assigned to security awareness efforts did not take on those responsibilities by choice. While some of those people do put together adequate programs, they do not approach the awareness effort in a coordinated effort. Many practitioners are not familiar with the social sciences that can enhance the effectiveness of their programs.

Security awareness should be viewed as a science itself, requiring a specific knowledge base to implement proper programs. Just like poorly engineered software can be slow, problematic and difficult to maintain, poorly engineered security awareness programs can exhibit the same traits. If practitioners are not familiar with the appropriate sciences, they should seek outside support in putting their programs together.

Assess Organizational Security Culture

Before beginning any security awareness effort, it is critical to understand your corporate culture. You need to understand if end users and management consider security a help or hindrance to their daily tasks. If security is well supported throughout the organization, you can proceed more efficiently, and take on more critical issues. If the security culture is poor, you will need to tackle more basic issues than you may prefer.

Likewise, the methods that you use to communicate with the company will be driven by security culture. If you have strong support, you can incorporate senior management in your efforts. We find that some companies do not even allow the security awareness team to send out e-mails to the company. You need to understand what you have to work with, and against, so that you can target your organization most effectively given your limitations.

Understanding the security culture can allow you to also provide the most return for your business. If you understand how security can best facilitate business processes, you are more likely to obtain support for your efforts.

Obtain Executive Management Support

When you have executive support, you clearly obtain more resources and support. This support inevitably leads to more freedom, larger budgets and support from other departments. Anyone responsible for running a security awareness program should first at least attempt to obtain strong support, before focusing on anything else.

Obtaining senior executive support can be difficult, but our research also found best practices on how to obtain this support. Successful efforts frequently highlighted that security awareness was required for compliance and that awareness efforts provided a return on investment that will inevitably save the company money. They also created special materials specifically for upper-management, such as newsletters and short articles that highlighted relevant news and tips that were specific to executives.

Choose Topics Most Relevant to the Business and Culture

The programs that were determined to be least successful seemed not to have a focus on topics that were relevant to the business. Specifically, they represented a random set of topics that were either driven by vendor provided materials or were created from a random list of topics chosen by the awareness staff. As previously implied, the security culture and business needs should drive the topics highlighted by the security awareness programs. These topics can be driven by news related topics, such as the recent LinkedIn password hacks. New corporate directions, such as the company allowing mobile devices to access the corporate network, can also drive them. The security awareness program should always support business functions, and focus efforts accordingly.

Partnering with Other Departments

When security awareness efforts were able to involve other departments, they were found to be more successful. The other departments include Legal, Compliance, Human Resources, Marketing, Privacy and Physical Security. While it is easier to get this support if you have the senior executive support, these departments frequently have mutual interests and might be amenable to providing additional resources, such as funding or distribution. Frequently, these departments can make security awareness efforts mandatory. For example, the Legal and Compliance departments carry a great deal of influence throughout the organization and can make security awareness a required component of other processes, such as new hire indoctrination.

To obtain this support, you might find that you have to incorporate the needs of the cooperating departments with the general security awareness efforts. For example, you might suggest that you can use a security awareness newsletter to include compliance content. If it gets you the support you need, the effort is definitely worth the trouble.

Utilize Participatory Awareness Tools

Awareness measures that were interactive were found to be significantly more effective than passive measures. Tools, like those from Wombat Technologies, were found not only to be more fun and engaging, they allow for deeper comprehension and long term memory of the lessons provided. When users are engaged in security related activities, they also have a better impression of the security department as a whole. More important, they have a better impression of the security department's efforts and are more likely to support those efforts.

Use Creative Measures

While a large budget helps, companies with a small security awareness budget have still been able to establish successful programs. Creativity and enthusiasm can make up for a small budget. The description of Company C's efforts demonstrated a wide variety of creative efforts. Another effort included giving out boxes of chocolates that

included the security policy document, on Valentine's Day. Employees reported that they felt compelled to read the document, because they liked the chocolate. These are just examples, but clearly there are an unlimited number of options.

Collect Metrics Proactively

One of the key factors in having a successful effort is being able to prove that your effort is successful. The only way to do this is to collect metrics prior to initiated new awareness efforts. Without having a baseline, it is hard to demonstrate that your efforts had more than assumed success.

The metrics can include surveys on attitudes. They could also include the use of phishing simulation tools to include pre and post awareness training. You can also examine the number of security related incidents, such as attempted visits to banned websites. When you can show measurable improvements in any aspect of security, you can justify your program, and obtain additional funding and support. Just about every department in a company has to prove their value, and security should not expect to be an exception.

Consider Outsourcing Training and Awareness Tasks

As previously described, security professionals creating proper awareness and training programs utilize the appropriate sciences in the creation of the materials and the programs themselves. This makes the programs significantly more effective. For example, metrics, which again are key to demonstrating success, are embedded within great training tools, such as Wombat. Likewise, for determination of the appropriate metrics to collect proactively, it benefits calling in awareness experts who are very familiar with a wide variety of indicators that can be used to measure an increase or decrease in secure behaviors. Metrics are just one area where someone might seek outside support. The design of participatory training materials and the development of other aspects of security awareness programs are other efforts where calling in experts is warranted.

Department of How

As previously mentioned, security awareness efforts should focus on supporting business needs and processes. Awareness efforts that focus on how to accomplish actions are more successful than those that focus on telling people that they should not be doing things. Clearly there are actions that should not be allowed, but those should be the exceptions and not the rule. For example, it is not realistic that you can tell employees that they should not be on social networks, but it would be useful to them if you tell them how they can be on social networks safely.

The security department should never be perceived as standing in the way of enabling business. The ideal situation is for security to be called in whenever there are new endeavors being pursued. Security awareness can then proactively assist in generating employee behaviors that facilitate those endeavors, while protecting corporate interests.

Implement 90-Day Security Awareness Plans

Most security awareness programs follow a one-year plan. Those plans also attempt to cover one topic a month. This is ineffective, as it does not reinforce knowledge, and does not allow for feedback or to account for ongoing events. Programs that relied on 90-day plans, and reevaluated the program and its goals every 90-days, are the

most effective. The most successful program focuses on 3 topics simultaneously that are reinforced regularly throughout the 90 days. Every 90 days, the program is reevaluated to determine what topics need to be addressed moving forward.

There are clearly many details required to implement a 90-day plan. There is a variety of guidance available to format the plan, and the details can be inferred throughout this paper. However a full description of a thorough 90-day Plan is extensive. Please contact the Internet Security Advisors Group via whitepaper@isag.com for further information.

Multimodal Awareness Materials

The most successful programs are not only creative; they rely on many forms of awareness materials. While there is a potential place for learning management system training modules, too many programs rely on them completely as an awareness program. Successful programs incorporate a variety of awareness tools. This includes newsletters, posters, games, newsfeeds, blogs, phishing simulation, etc. The most participative efforts appear to have the most success.

Another issue to consider is that materials should attempt to connect with different generations. For example, some videos seem to connect best to young males. You then need to use other videos or materials that connect with older employees and females. There is definitely no such thing as “One Size” security awareness.

Short-term and Long-term Tasks

While the previous recommendation are applicable for strategic planning, the below tables represent the most critical tasks that security awareness practitioners should incorporate into their planning process.

Short-term Tasks			
What	**Who**	**Why**	**Cost**
Create a plan	The Security Awareness Specialist and the Security Team	Creating piece-mealed components to create a robust Security Awareness program does not lead to success	Several hours of each team members time
Partner with key departments	Legal, Corporate Communications, Privacy, Compliance	Building strong partnerships will ease the implementation of the program and will create non-security stakeholders	Several hours of key partners' time per fiscal quarter
Create materials for upper-management	C-Level employees	Creating materials targeting a population to educate them on items that may not otherwise catch their attention will increase their support of the program	Several hours of the Awareness Specialist's time per fiscal quarter
Create monthly materials	The Security Awareness Specialist	Creating materials on a monthly basis will keep the program relevant	Several hours per week of the Awareness Specialist's time

Long-term Tasks			
What	**Who**	**Why**	**Cost**
Assess efforts by way of self-evaluation and surveys	The Security Awareness Specialist and the Security Team	To ensure that the efforts and components used to promote the program are successful and provide the info to change them if they are not	Several hours of each team members time, twice per fiscal year
Create materials for distributed locations	The Security Awareness Specialist	Security does not only exist within the walls of Corporate Headquarters	Several hours to tailor messages to particular sites
Focus on more difficult security topics	The Security Awareness Specialist	As the program progresses, more difficult security topics can be introduced when a baseline knowledge has been established	Several hours of the Awareness Specialist's time per fiscal quarter
Utilize more creative efforts	The Security Awareness Specialist	More creative endeavors can cost more and should be utilized over time to not drain the budget	Several hours per fiscal quarter of the Awareness Specialist's time

Summary

Security awareness is a very distinct discipline within the security profession, but it is frequently treated as an afterthought of many security programs. This white paper summarizes one of the few cross-organizational studies that examines the factors that contribute to the success or failure of security awareness programs.

Unfortunately, most security awareness programs are not successful because of fundamental flaws in the planning of the programs. With a more systematic and scientific approach to security awareness and training, not only can security awareness significantly improved, it will result in significantly fewer security related incidents and also improve the acceptability of all security efforts.

The recommendations in this paper can assist people in creating and implementing a comprehensive and cost effective awareness program. While all recommendation might not be applicable for all companies, there are clearly many measures that can be implemented. It is time security practitioners acknowledge that there is as much of a scientific basis in good awareness programs as there should be in all security countermeasures.

Contact Us

For questions about the research or to learn about turnkey services for security awareness programs contact: Samantha Manke at samantha@isag.com or visit http://www.isag.com.

To learn more about the participatory software-based security training solutions provided by Wombat Security Technologies email info@wombatsecurity.com or visit our website at www.wombatsecurity.com.

Internet Security Advisors Group

The Internet Security Advisors Group (ISAG) is a world leading security service firm providing strategic security services. ISAG specializes in providing security awareness services that are based on scientific principles, and can assist any company in creating better security awareness programs. Our security awareness managed service allows companies to outsource their security awareness efforts to experts, providing a security awareness program that is less expensive and more effective.

Wombat Security Technologies, Inc.

Wombat Security Technologies, Inc. is the first and only company to offer a complete suite of anti-phishing and security awareness training products that leverage progressive training techniques of professional educators to effectively improve human response against cyber-attacks up to 70%. Wombat's breakthrough software-based training solutions teach users how to recognize and avoid the most advanced attacks involving phishing, password security, social networking, smartphones, safe browsing and working outside of the office.

All of Wombat's security awareness training solutions are part of their award-winning Security Training Platform which integrates interactive training modules, mock attack services, analysis and reporting and administrative capabilities in one easy to use interface.

Organizations from small to large, including Fortune 500 companies and large government agencies, around the world are deploying Wombat's training and filtering solutions to protect them from cyber-attack.

