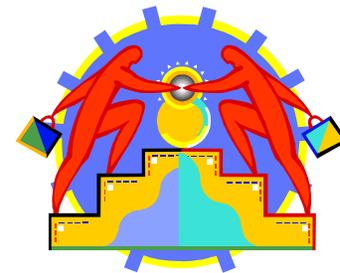


Ten Easy Steps to Creating an Effective Information Security Outreach and Marketing Plan



November 2008



Multi-State Information Sharing and
Analysis Center (MS-ISAC)

www.msisac.org

Table of Contents

Introduction.....	3
Step 1: Unearth Your Baseline.....	6
Step 2: Start Small, Feed It, and Watch It Grow.....	9
Step 3: Target Your Intended Audience (But Don't Shoot Them).....	11
Step 4: Reach Out to Your Outreach Channels.....	12
Step 5: Make Advocates Out of NaySayers and Non-Believers.....	14
Step 6: So You're Not in Sales--Hit the Road Anyway.....	16
Step 7: Sing! Sing! Sing Your Plan Like a Mocking Bird	21
Step 8: Confront Your Challenges, Spin Them into Opportunities	21
Step 9: Measure Your Successes.....	22
Step 10: Do It All Over Again, But Better.....	23
Conclusion.....	24
Appendix A Sample Survey Questions.....	26

MS-ISAC State and Local Government Outreach and Marketing Workgroup: Special thanks and recognition to the following individuals listed below for lending their time and expertise to the development of this Guide. This effort was a great collaboration among all levels of government, with the goal of helping to enhance our collective cyber security readiness and response.

Co-chairs: Colleen Pedroza, CA; Peggy Ward, VA; Sandy Graham, Chesterfield County, VA; Tina Post, NY (MS-ISAC) with Andy Atencio Greenwood Village, CO; Mike Abel, Association of Counties, ND; Rafael Diaz, IL; Linda Erickson, MN; Greg Fay, IA; Randy Foshee Little Rock, AR; Edward Knittel Association of Boroughs, PA; Sue Ann Lipinski, WV; Theresa Masse, OR; Dave Plzak, Tarrant County, TX; Jim Reiner Sacramento County, CA; Jean Schultz, Johnson County, IA; Kevin Winegardner, MT; and the U.S. Department of Homeland Security NCSD and past members: Kevin Dickey, Contra Costa County, CA; Dan Lohrmann, MI; Steve Troester Linn County, IA; and Mark Weatherford, CA.

Appendix A Sample Survey Questions

Some questions regarding information security outreach and marketing that you may want to ask include the following:

- Does your organization have an information security outreach program?
- What key information security topics are of interest to your organization?
- What means of communication are of interest to you in reaching your audiences?
- Does your organization establish regular goals and objectives for tracking its outreach progress?
- How does your organization measure outreach growth or progress?
- Does your executive management support your program? If so, how is this support demonstrated?
- Does your organization conduct trainings around specific information security topics? If so, how often? How are the topics determined?
- How do you distribute information/information security awareness materials?
- Does your organization partner with other entities/associations/organizations in support of any of these efforts? If so, who and in what capacity?
- Does your organization have an information/information security website? If so, how many hits does it receive?
- How many attendees come to your events? Is this information collected through pre-registrations, overall registrations, or sign-in sheets?
- What type of participant feedback do you receive from events?
- How many users do you have on your listserv roster?
- How do you maintain the list?
- Do your organization's information security policies and standards match your marketing and outreach messages

them as a measurement of your program's success and where you need to direct more effort.

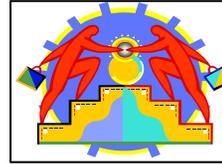
- Outreach is about developing a partnership with those individuals and organizations you want to reach. It's not a one-way communication channel and it is not just about personalities – establish processes that can live on after people or positions change.
- Approach everything in a collaborative way. Say "Let's work together!" and mean it.
- Look for other security partners to work with and potentially carry your message for you to their constituencies.
- Walk the walk and talk the talk. If you practice what you preach, the majority of people will follow and want to be involved.
- Keep raising the bar! A lot of people will find their comfort zones and become part of the "status quo." Don't let that happen to you and your team. Keep raising your expectations of yourself and your program.
- Make it fun! Enjoy what you do! Be passionate about it. And share your passion with others – you will be surprised how your passion helps attract new allies.

Conclusion

Ten Easy Steps to Creating an Effective Information Security Outreach and Marketing Plan does not discuss what components make a good information security program. It is meant to outline a process for focusing and executing outreach and marketing activities to enhance your organization's information security programs.

Images © 2008 Microsoft Corporation. All rights reserved

Introduction



The Multi-State Information Sharing and Analysis Center (MS-ISAC), established in 2003, is a collaborative organization comprising representatives from all 50 states, DC, as well as local governments and U.S. Territories, whose mission is to provide a common mechanism for raising the level of information security readiness and response within state, local governments and U.S. Territories. The MS-ISAC provides a central resource for gathering information on cyber threats to critical infrastructure from the states and providing two-way sharing of information. The MS-ISAC serves as a critical point of contact between the states and the federal government through the U.S. Department of Homeland Security.

The MS-ISAC's State and Local Government Outreach and Marketing Workgroup (Workgroup) has been working to help improve each member's effectiveness in reaching out to their key stakeholders in communicating the importance of information security. The Workgroup identified the need for an outreach plan for the members.

The *Ten Easy Steps to Creating an Effective Information Security Outreach and Marketing Plan* was developed to assist your efforts based on lessons learned and best practices. The purpose of this guide is to lay out an approachable and repeatable process for focusing and implementing your information security program's outreach activities and marketing services and products. To effectively use this Guide you will want to carefully consider how your organization will grow and where resources need to be focused. These considerations can include the following:

- current or desired capabilities, or specific qualities for performing a function, such as a more effective community information security education program or improved interactions between stakeholder groups;
- desired outcomes of the outreach effort, such as a more cyber aware community or increased participation from the private sector in information security efforts;
- types of organizations you work with or want to work with on a regular basis; and
- support enjoyed or needed from stakeholders including organizational leaders and decision makers.

What is Outreach?

This Workgroup defines outreach as two-way communication between entities to establish mutual understanding and develop relationships. Outreach, for the purposes of this guide, is driven by the overarching

goal of improving information security awareness at the State and local levels nationwide through an increased number of distribution channels to a variety of entities.

The activities executed as part of outreach can be focused on a number of audiences, depending on the particular needs and strategic goals of your organization. Audiences identified by MS-ISAC members include federal, state and local government entities, educational institutions and organizations, law enforcement, emergency responder communities and the private sector.

What is Marketing?

Marketing for the purposes of this document addresses researching who the audience for a product or service is, identifying what the capabilities of your marketing program are and defining the messages you will use to let your audience know about the information security products and services your organization has to offer them.

Outreach and Marketing Lifecycle

While an important part of planning marketing activities revolves around tactically introducing or “rolling out” specific products and services your organization has or will produce, outreach is a more strategic endeavor of building a variety of communication channels. It is based on careful consideration of what capabilities your organization seeks to develop, the types of organizations it works with and wants to work with both on a targeted and regular basis, and obtaining support from the various stakeholders including organizational leaders and decision makers. Think of outreach as the various routes on which a truck carries cargo to defined locations. Based on the marketing plan, the truck follows carefully planned routes to ensure that the specific cargo is delivered to the appropriate recipients at the correct times.

Outreach is the process of defining a variety of federal, state, and local government and private sector entities that share an interest in learning more about the overall topic of information security. Outreach involves identifying each entity’s size and specific interests within the topic.

The marketing plan developed will vary with the entities and routes selected for receiving the “cargo” (i.e. specific product, service, and/or message) based on the entity’s needs and perceptions. Taking time at the onset will help to ensure accurate and efficient delivery. The diagram below depicts the lifecycle of the Outreach and Marketing. It consists of four major phases: Planning, Development, Execution and Evaluation. Each of the Ten Steps this document

Using this process for planning, developing, executing, and evaluating an outreach and marketing plan will help to make sure your efforts and resources are maximized and your information/security program evolves appropriately. Remember to use these steps to guide you in the process.



Images © 2008 Microsoft Corporation. All rights reserved

There are many good resources available, such as the MS-ISAC, to help you with that effort. Once you have a good program in place, you need to know how to effectively market it to help spread the word about information security. Remember to make information security outreach fun. The more passionate you are about your program, the more others will notice it. We already know information security is important; let’s spread the word.

For assistance with building and launching your outreach strategy, feel free to contact the MS-ISAC at isac@cscic.state.ny.us.

Step 10: Do It All Over Again, But Better

Solicit Feedback and Reassess your Strategy



You have identified what works or doesn't work, and found gaps in your program. You are now ready to find ways to address the gaps and make improvements. Determine why some of your strategies are not working; should they be revised or stopped? Maybe you are not reaching the right audience with the right messages. Check the

feedback and consider the following:

- Are you collecting feedback from targeted audiences effectively?
- Which messages are not being heard or understood? The technical? The general?
 - Are the technical messages, such as vulnerability and threat information, reaching the right technical staff that can make the necessary adjustments or changes?
 - Or are they too technical for most to understand?
- Is the information presented too dry or boring? Did you lose your audience?
- Are the messages too long so that the point is lost?
- Is the message communicated well?
- How is the message portrayed by the media?
- Are you posting important information on the Internet/ Intranet website in a timely fashion?
 - Is it the right information?
 - Is different information needed?
 - Are you posting information in the right place so it is easily found?
- Are the newsletters and other materials read, or ignored?

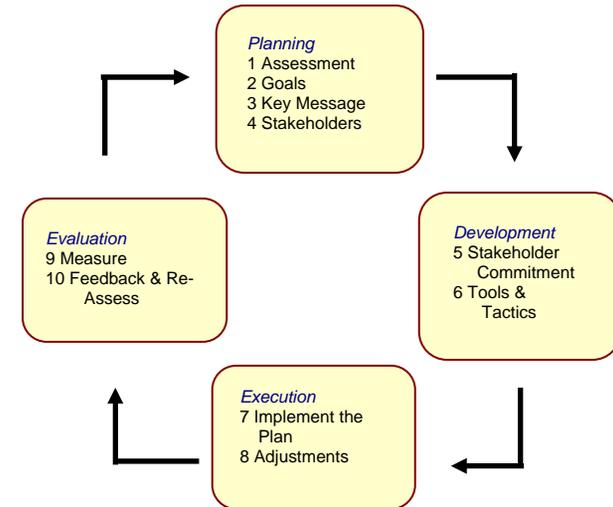
Reassess

There are no easy solutions to developing a good outreach and marketing plan for your information security program. As your program matures, you will want to continually improve it. Some words of wisdom:

- Don't make the same mistake over and over again. If something is not working, do not be afraid to stop and try a different approach. Make adjustments to your plan when necessary.
- Set metrics and track your performance against them. Use

describes occurs within these Outreach Lifecycle phases.

Outreach & Marketing Lifecycle



The Ten Easy Step Outreach and Marketing Process

Ten Easy Steps to Creating an Effective Information Security Outreach and Marketing Plan lays out ten distinct steps which outline the basic actions that should be taken to better ensure success in reaching out to stakeholders within your communities.

At first glance, reading, understanding, and walking through these steps may seem time intensive and resource consuming. Outreach and marketing, while vital to any healthy information security program, can sometimes get placed on the back burner due to other priorities that compete for staff time and resources. However, it's important for you to recognize two important characteristics of outreach and marketing planning.

First, not all the activities in this guide need to be completed at once. Time and reflection are essential to creating robust and relevant outreach and marketing strategies and tactics. The process is intended to help you and your staff more effectively prioritize and coordinate your information security outreach and marketing activities by focusing energies along a logical course of action, not hold you back with burdensome tasks.

Second, you and your organization may already be engaging in this

type of planning, or various components of it, without recognizing it. Chances are, you already have a pretty good understanding of your information security community, are aware of your organization's plans for increasing capacity and rolling out new products, services and messages in the near future, and can identify specific means for expanding strategic partnership opportunities. Much of this information will be very useful in the outreach and marketing development process and will require a minimal amount of effort on your part to incorporate it into the process.

Alexander Graham Bell once said, "Before anything else, preparation is the key to success." Information security including outreach and marketing for information security products, services and messages are serious topics and deserving of proper attention to raise awareness of their importance and expand your influence. Make sure you support your programs with appropriate and effective outreach planning. Now, let's jump in!

Step 1: Unearth Your Baseline

Establish the Current State of Affairs



Before you know which direction you need to take your information security program, you need to dig around to see where you are in the big picture. By understanding at the onset which capabilities your program possesses, you can ensure better use of both your staff and stakeholders' time and resources, more easily replicate successes, understand where improvement need to be made, and demonstrate growth to your leaders and managers. It also assists all involved parties in making informed decisions based on thorough research, established priorities, and a common vision.

Before you complete your outreach and marketing plan to enhance information security awareness and preparedness, you should understand the current state of affairs for your program. The best place to start is with research. While many of us may cringe at the memory of spending hours sorting through books or online databases for school projects, research for developing your outreach strategy can be much more practical and enjoyable. There are a number of methods you can utilize to gather information on where your program is, where you want it to go, and what others think of it. Some of these include the following:

- conducting personal interviews and ad hoc discussions with your staff, partners and stakeholders including organizational leaders and decision makers;

Step 9: Measure Your Successes

Evaluate your Outreach Strategy



As you learn what works well and what doesn't, be sure to measure your successes against the original survey and other strategies, your stated goals and objectives, and the metrics you have established. It's probably best to do this effort every six months or so, to be sure you are reaching the right audience with the right message and that people are beginning to take notice of your program. You set goals and objectives earlier in Step 2 of this process using **SMART**: **S**pecific, **M**easurable, **A**chievable, **R**ealistic, and **T**ime-related. Now it's time to measure those goals!

Another important factor is to document all the work you are doing. For example, keep a log of all the presentations you have made, the number of employees you have trained, the number of hits your website has received, and the number of employees who have received the newsletters. Some anecdotal analysis could also include the following:

- Did someone in your audience refer someone else to you?
- Did a presentation you gave somewhere increase participation at one of your outreach events?
- Has someone in your targeted audience asked to be part of your outreach channel?

Documenting these factors will really help you to focus on the successes and create metrics that can be used to measure the effectiveness of your program. Collecting results through your metrics may help you justify the need for additional resources and funding, and elevate your program to the appropriate level of importance the topic of information security warrants.

Also, remember to keep track of the contacts you make throughout your outreach efforts. You should keep careful records on the following:

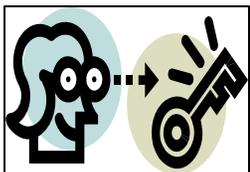
- whom you plan to contact
- the progress you are making
- how you plan to develop that relationship once the connection is made
- how you plan on formalizing that relationship into a process that will endure even if there is a change in staff

As you execute your outreach plan, you will see that list of supporters and collaborating organizations grow and evolve.

place a link on their website to your website. The more places you can link from, the greater the chances your site will be accessed.

Review all the ideas identified in Step 1 for improving your information security communication program. If you haven't implemented some of them, consider doing so. In many cases, someone may have already done the work of identifying and taking advantage of an opportunity; all you have to do is ask if you can use it.

Step 8: Confront Your Challenges, Spin Them into Opportunities



Make no bones about it; you will be confronted with challenges. Your management will tell you that you can't do something because of the cost, or it has been determined that you don't have the resources. Perhaps you are having trouble establishing a good relationship with an important stakeholder. Maybe you don't have the

audience or support to deal with specific issues or problems. You might find people aren't opening their doors to you.

Fear not! With diligence, hard work, and persistence, you will find a way to turn these challenges into opportunities. You won't win them all, but you can win the majority of them. For example, if you have a limited budget, research grant options or public health funding opportunities to see what might be available. Investigate the possibility of bringing in a student intern or a volunteer. Many states have volunteer or student programs in place that can be used to locate a volunteer or student best suited to your business needs. When in doubt, remember to collaborate! Use the MS-ISAC tools or put out a call to other partners to see what approaches they have used to convert a challenge to an opportunity! And don't forget to share these through the MS-ISAC.

- reviewing internal policy documents, internal memorandum, and meeting summaries and minutes;
- analyzing open source materials such as newspapers, magazines, newsletters, public Websites, blogs, or wikis;
- hosting focus groups, both formal and informal, of audience segments whose opinions you are seeking; and
- conducting a survey.

Personal Interviews

If you choose to conduct personal interviews using either developed questions or ad-hoc discussions, please be aware that the information you collect will be granular and qualitative in nature. Qualitative information can be great for understanding the current state of affairs in the form of stories, but can be harder to directly measure as it may not be quantifiable. Further, information may be limited if people are unwilling to participate openly in interviews. You can reduce this possibility by setting out neutral objectives for improving information security outreach and marketing efforts and establishing realistic expectations on length and content area at the onset.

Internal Documents

Reviewing internal policy documents can be a great way to find both channels and roadblocks to your information security outreach plan. Any roadblocks found in existing policy may be a jumping off point for suggesting change of internal policy, or finding alternatives to those particular situations. Be especially careful to adhere to any restrictions about the access or dissemination of an organization's product's services or messages.

Open Sources

Analyzing open source materials and news items can provide a wide sampling of sources, which can give greater insight into current stakeholder awareness. This can help you identify gaps in information security outreach and marketing available and develop a more targeted outreach and marketing plan to address these areas of need. Limitations may include lack of available open source communication channels or information disseminated to stakeholders that is not directly relevant or is outdated.

Focus Group

Conducting a focus group can result in identifying very specific insights from a targeted group such as best methods to communicate with the group as well as their specific areas of interest. While there is no substitution for the level of detail an in-depth conversation with 6 to 12 members of your target audience can provide to focus group planning can be time consuming and resource intensive.

Surveys

Another highly effective tool for gathering opinions is surveying. A survey is a sampling of facts, figures, or opinions taken to approximate the results of a larger group. It is one means to collect quantitative information for statistical analysis, about items or issues in a population. By developing your own survey and administering it to your stakeholders, leadership, staff, and colleagues, you can control the types of questions that are asked as well as ensure the questions are consistently delivered. This ability will greatly assist in aggregating and analyzing the data you collect.

A good survey will assist you in identifying ways to uncover insights into where improvements can be made to your outreach and marketing program, how to best reach key member groups, and how to properly craft appropriate messages and communication vehicles. Your survey should address issues directly relating to your various stakeholders and entities that may have a vested interest in information security.

Survey Development

Survey development should begin by targeting the entity with which you plan to establish communication channels. It should be based upon information you know or have recently received or collected from as many sources as possible.

- Target specific groups to identify what they have done or are doing in the realm of information security outreach.
- Determine what information needs to be collected. Such as optimal distribution channels and the specific interest areas of the entities. Develop the questions before you begin creating the survey. See Appendix A for some sample questions.
- Determine how you will conduct the survey. It can be administered through a number of means, such as via paper questionnaire, email, in person, telephone, or online. There are numerous survey design tools available on the Internet, for little or no cost.

Regardless of which method is used, you should pilot the survey with a sample audience to assess the clarity of the questions and elicit useful responses. A survey that is ambiguous will be confusing to the individual taking it and, as a result, will significantly affect the quality of the information you are trying to collect. Ask two or three co-workers to answer the survey questions and to provide recommendations for improvements or word choice.

Once you have developed and edited the survey, you should focus on

and organizations to regularly educate them on up-to-date information security information and initiatives.

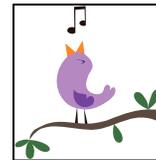
- Ask to present a timely information security topic to further develop greater situational awareness with electronic crimes task forces or similar organizations.
- Reach out to state and local fusion centers in your area to schedule a time to brainstorm ideas on how to improve information sharing and collaboration in preparation for potential future information security incidents.

Organizations and Associations

- Get involved in local chapters of the Information Systems Security Association (ISSA) or the Federal Bureau of Investigation's local InfraGard chapter.
- Write articles for magazines, security websites, community organizations, small business associations, and economic development councils.
- Involve yourself in speaking engagements and opportunities attended by members of these organizations and find opportunities to network with them.

Step 7: Sing! Sing! Sing Your Plan Like a Mocking Bird

Implement the Outreach and Marketing Plan



All your preparation will now be put to good use. Once you have your outreach and marketing plan in place, spread the word. Don't be shy! Share your program's key messages with others. Ask them for their input and feedback for improvement while you verify you are reaching out to the right audience in the correct manner.

Your public information officer may be helpful in spreading the word about your program so remember to get him or her excited about your plan and obtain their buy-in if you have not already! If your organization has a privacy officer, get him or her involved as well. It is widely understood that one can't have privacy without good security. Other stakeholders should also be excited to help.

If you haven't already done so, create a website about information security. In case you have not seen the information security sites of MS-ISAC member states, a list can be accessed at www.msisac.org/members. Conduct research on the Internet to see what might work best for you and your organization. Once you have done this, work with your established partners and stakeholders by asking them to

representatives.

- Reach out to chief information officers and their councils. Ask to present on an emerging cyber-related topic they are facing.
- Get to know your agency's chief information officer, public information officer, human resources staff, privacy officer, auditors (internal and external), and legal counsel. They can partner with you on many security-related topics and reviews and assist you in reaching a greater level of participation.
- Reach out to your training or personnel office. It may be able to help you identify speakers for conferences and meetings as well as to assist you in marketing and advertising training and speaking engagements. A good example of this is the Iowa Training Office newsletter advertising computer security training that is included in Appendix B.
- Get to know the staff in your finance and budget offices. Helping them understand why certain security levels are needed and the associated costs will help them be more educated and supportive of budget allocations for security initiatives.
- Your data center representatives can help you look at security from an enterprise level.

Education

- Partner with information security officers, universities and community colleges, including their respective Boards of Regents, CIOs, and IT staff.
- Partner with your education departments, such as your State Superintendent, to reach out to the K-12 community. Elect to be a speaker at a local high school or partner with them, through their technical staff, on a security-related project.
- Involve your local parent teacher associations, or other organizations that provide direct K-12 services or events.

Cities and Counties

- Partner with the security professionals and executive management of local jurisdictions. In many cases, states share data/information with their city and county agencies. Establishing a relationship with them will help to develop a plan for handling information security events and attacks before one takes place. This process will go far in building trust and confidence between your organizations as well.

Law Enforcement and Homeland Security

- Reach out to law enforcement agencies or district attorney offices that handle information investigations, forensics, and prosecutions. Schedule regular meetings with these agencies

the following:

- Determine how you will provide a summary of the results.
- Develop a draft format of the summary to help clarify what information you will analyze, how to present it, and to whom it will be presented.
- Decide if you would like to further demonstrate your results in a spreadsheet or a word processing document.
- Decide if you want to report quantitative (numerical) data, qualitative (stories) data, or a combination of the two.

The results should offer a current baseline for your organization's outreach and marketing efforts, as well as point to appropriate means for measuring how to gauge progress and improvements. As you document the results from the survey, share it with partners and interested parties. The information will be a useful measuring tool the next time you conduct a survey to show effectiveness and continued improvement in your program.

Overall, the above information gathering strategies come with inherent positives and negatives. Carefully consider which method is most appropriate for your needs. Please keep in mind that it may take a variety of information gathering methods to thoroughly define your current situation.

Step 2: Start Small, Feed It, and Watch It Grow

Set Goals and Objectives



With the baseline established, it is now time to examine what you want to achieve with your outreach strategy and marketing tactics. Now you should set your goals and objectives toward desired outcomes.

A goal is a projected state of affairs which an organization intends to achieve or to bring about through various activities. Goals articulate to an organization's internal and external stakeholders the intention to achieve an envisioned end state. They also illustrate what needs to be accomplished and offer insights into how to appropriately direct resources. Your outreach goals should be clearly defined and acknowledge that the process starts small, requires constant feeding, and takes time to grow.

Goals

Your outreach strategy and marketing tactics should be designed to achieve specific goals. For example, goals could include the following:

- raising the profile of the Information Security Office so that it is well-known and respected - you exist and you have information and services of value to your customers;
- increasing stakeholder acceptance of methods to mitigate information security risks to critical infrastructure systems;
- expanding your organization's information security program into new organizational areas by expanding stakeholder support; and
- obtaining buy-in from key stakeholders to actively promote and utilize the available resources for increasing information security awareness.

Objectives

Objectives are specific points, activities, or metrics that contribute to achieving defined goals. Think of objectives as milestones that will help you to gauge your progress toward achieving your goals. Including a timeline for marking goals, objectives, and anticipated results is useful for tracking your progress. For example, it may take several years to identify your stakeholders and your audiences, establish the delivery options and develop the specific marketing tactics for the services, products and messages so that the target audiences and stakeholders become more fully versed in the security threats facing your information; however, you can establish individual objectives for getting them there. One objective could be to identify the outreach strategies and marketing tactics for an "Introduction to Information Security Briefing." You may look at various outreach channels such as posting information on your organization's website or developing a new listserv contact is more productive for achieving your goal.

To help identify and articulate how you will proceed, remember the rule that your objectives should be **SMART**: **S**pecific, **M**easurable, **A**chievable, **R**ealistic, and **T**ime-related. Examples could include the following:

- Identifying three new sources and communication methods in the next three months for presentation of a topic on information security awareness;
- targeting ten new groups each month for the next six months for receipt of the MS-ISAC monthly newsletter to send to; or
- increasing the number of participants from your organization in the National Webcast Initiative by ten percent in the next six months.

websites or portals

- email distribution lists and listservs
- focus groups or project workgroups
- library of information security awareness materials available to your stakeholders
- attendee feedback forms after training, events, and presentations
- contests or giveaways with information security-related themes
- rewards programs where letters of appreciation, and other forms of public recognition are given out
- placement of articles, features, letters to the editors, and profiles on information security in internal and external newsletters, local newspapers and publications

Some examples of Outreach channels currently used by MS-ISAC members may be found at www.msiscac.org/members/.

Based on feedback from surveys and MS-ISAC member's own experiences, here are some audience-specific tools and tactics to consider in engaging in outreach:

Elected Officials

- If possible, obtain approval to occasionally attend a Governor's Cabinet meeting to share ideas about addressing top information security concerns.
- Also try to reach your Lieutenant Governor and other elected officials, such as members of Legislature, the Attorney General, the Department of Education, or staff for the Secretary of State. Sending them relevant information that could help them with educating their constituent base on information security might help with building your base of support.

Executive Branch Departments

- Get to know your State's Information Security Office, Office of Emergency Services, or State Homeland Security advisor or lead. Involving them in disaster and incident recovery operation discussions will help improve your plans and establish good relationships should disaster strike.
- Meet as frequently as you can with department directors, commissioners, and agency heads. Be sure to offer ideas and solutions; don't just bring the problem or concerns.
- Schedule regular meetings or forums with your information security officers and other security professionals; have interesting topics and speakers. Include your city and county

selecting those most appropriate will ensure that the right message is heard by the right audience at the right time. This may involve a trial and error process to find the fit for a particular organization and how you choose to engage them. The experience you receive in doing this will help tremendously with future engagements.

Your messages must both educate and motivate, but there is not a “one size fits all” communication plan for all audiences. Use your research to determine what types of communications methods to which a particular group or individual will respond positively to. Some communication tools include the following:

- briefings to other advocates and stakeholders
- communication products, such as toolkits for managers and

**Illustrative
Information Security
Outreach Channels**

Each of the following outreach channels has been employed to conduct outreach activities

- Forums - such as town hall meetings, conferences, roundtables, presentations, seminars, symposiums, discussion panels, meetings, fairs, and community events where key stakeholders gather
- Collaboration with your local media outlets
- Membership in National, State, or Local information sharing initiatives, industry associations, etc.
- Employee (internal) communications
- Participation in broader homeland security, critical infrastructure preparedness activities
- Physical and Cyber Exercises and Drills

leaders that contain posters, fact sheets, videos, FAQs, and brochures

- video and audio news releases and podcasts
- brochures, pamphlets, mouse pads, calendars, posters, screensavers, banners, bookmarks, and other promotional items
- notices or informational flyers in paycheck stubs or other human resource materials
- public service announcements created in partnership with local media
- videos on websites and during training
- email newsletters with “Do and Don’t” lists
- conduct brown bag lunch or impromptu meetings
- customized user logon messages
- annual training and awareness days, using computer-based, teleconferencing, in-person, or instructor led sessions
- Internet and Intranet

Develop suitable actions in your strategic plan to maintain focus on the big picture. Leverage what works well in your organization, based on research of past outreach and marketing efforts. You can always recruit and enlist additional stakeholders to assist with your goals and objectives; involve them early in the process, making implementation easier. In your strategic plan, identify roles and responsibilities necessary to execute it. For example, you may decide that you really need to focus on gaining executive management’s buy-in as a first step. Make time to explain your expectations of management’s role and responsibilities with regard to establishing the goals and promoting the program.

Your plan should account for and be flexible enough to adapt to organizational changes, audience perception changes, or other events that may call for different outreach tactics. Be especially mindful of how these changes will affect your goals; objectives; service offerings and capabilities; operational procedures; or relationships with stakeholders. Include regular reviews and clear processes for updating the plan, when needed. Once you set your goals, establish a timeline, align objectives and plan for change -- you are on your way!

**Step 3: Target Your Intended Audience
(But Don’t Shoot Them)**

Use Key Messages



You have completed the survey or other information-gathering strategy, and objectively analyzed the results. You have established clear goals and objectives. It is now time to define *who you will be engaging* in your outreach activities and *what key communication channels you will use as well as what key messages the various entities are interested in learning more about*. Your audiences are related directly to what you are trying to accomplish. Audiences are defined by both their relationship to you, their communication mechanisms preferences and the key messages that interest them.

You will identify multiple audience segments that will be the groups or individuals who may have an influence over your budget or the decisions affecting your organization, possess resources that can assist you in expanding your programs, and even play a role in your outreach and marketing program’s success. Carefully defining each of your audiences and understanding the areas of their interest will

greatly assist in developing strategies to deliver the products, services and messages to engage them.

Key Messages

Key messages are those themes or topics selected to be delivered. Your marketing plan must tailor the key messaging themes to each audience segment to specifically address the unique needs and concerns of each in line with your outreach goals. The survey results should help you identify the primary key messaging themes of interest to your stakeholders. Designing outreach channels and recipients as well as marketing tactics for communicating key messages within an appropriate context will more effectively engage stakeholders and convey the right information at the right time. Your ultimate purpose is to clearly identify the outreach stakeholders, communication channels and the key message areas of interest to provide effective outreach and marketing!

Some key message themes include the following:

- Information security is everyone's responsibility
- Information security is essential to your organization's growth and stability
- Information security crimes

It is important to provide consistent communication channels in your outreach campaign. For example, if you have decided on three different ways to deliver key messages, (i.e. website, flyer, and email) be consistent with your messages across communication channels.

A good general rule to follow is the Rule of Seven. "The Rule of Seven" references the old adage that it takes an average person seven times to hear a message in order to comprehend the full meaning and scope. Developing consistent key messaging and delivering the message in a variety of formats is important to your outreach program, as people have diverse ways for learning new information. Repetition is important, and will allow for the message to be remembered and contemplated by stakeholders. The desired outcome of consistency, diversity of delivery, and repetition is to encourage stakeholders to become advocates of your cause.

Outreach and Marketing Tools and Tactics

Step 6: So You're Not in Sales--Hit the Road Anyway



Information security professionals are often thought of as always saying, "NO!" Find innovative ways to ensure security is viewed as a business enabler, not an impediment consisting of unnecessary burdens, costs and resources. Find a way to get to a solution or reasonable compromise that mitigates the risk, and allows you to say "YES."

Just like a salesperson, sell your product. If you don't have good communication skills, develop them or engage someone who does have them. Be sure to not talk over the heads of people who may not understand information security and what it means to them, their business needs, or their projects. Find positive, proactive, and fun ways to reach out to explain the value of information security. Remember, it is a collaborative effort and good networking pays back in a big way! Every opportunity you have to talk about your program, do so. This effort will get the message out and help improve your presentation and communication skills!

Carry a handful of your favorite brochures or handouts wherever you go, and give them away. A good approach might be to carry a handful of the MS-ISAC Local Government Cyber Security series of handbooks with your Office's contact information label on them. You can download the handbooks at www.msisac.org/localgov. That way, you can advertise the important work of the MS-ISAC and promote your Office at the same time. Keep a thirty-second elevator (prepared) speech in your mind to extract at opportune moments. Also be prepared with positive affirmations of your work, such as success stories and kudos for doing a great job. Success breeds more success.

Tools

Tools are devices or mechanisms that will help you deliver a desired end result in a mission. Tactics are conceptual actions used to advance or achieve a specific objective. Tactics can include creative ways to deliver your message by creating strong audience interest. Developing outreach tools and tactics to deliver key messages is a critical element in your approach.

Evaluating the impact of various methods of communication and

empowering for both you and the affected individual. Asking them to speak at a presentation about their experience and the lessons learned can be powerful and compelling for you and your partners. Turning a negative into a positive will reinforce the importance of cooperation, and people will begin to feel comfortable approaching you.

Obtaining management support is critical. This may be difficult however, because information security can be a difficult concept to understand, and management may not always see the value of such programs. Explaining it to executives, whenever you get an opportunity, in non-technical, layperson terms can go far in helping to promote your program. Once they understand the value of information security and how it is protecting them, they may be more proactive with assisting in finding resources and funding for your programs.

Outreach Resources

If you are struggling with finding assistance or direction in enhancing your program, there are many resources available from a variety of organizations.

- Multi-State Information Sharing and Analysis Center (MS-ISAC), www.msisac.org
- U.S. Department of Homeland Security National Cyber Security Division, www.dhs.gov/xabout/structure/editorial_0839.shtm
- United States Computer Emergency Readiness Team (US-CERT), www.us-cert.gov
- National Institute of Standards and Technology (NIST), www.nist.gov
- National Association of State Chief Information Officers (NASCIO) www.nascio.org
- InfraGard www.infragard.net
- The SANS Institute, www.sans.org

Don't forget other departments within your government or other governments in your area that may be willing to share their experience and, possibly, a copy of their outreach program.

Don't reinvent the wheel; borrow and retool!

Step 4: Reach Out to Your Outreach Channels

Identify Stakeholders in Order to Reach Out To Them



Stakeholders - one aspect of your initial audience - are individuals or organizations with a legitimate and possible financial interest in a given situation or cause, in this case, efforts to increase state, local governments and U.S. Territories information security outreach. They are your partners who are directly affected by the decisions your organizations make and with whom you share success and failures. Properly defining stakeholders is a key element in planning and delivering any successful outreach plan.

Depending upon your particular situation, you may want to consider how the groups in the adjacent box could potentially benefit from your program as well as assist you in reaching out to other audiences to broaden the impact of your program activities.

Example of Information Security Stakeholders

Each of the following stakeholders has been listed by other MS-ISAC member states as important to their individual programs.

- State legislators and elected officials, including city, county, and state levels
- City and county managers and representatives, such as information security officers and chief information officers
- Private industry, local businesses, or chamber of commerce officials
- Local K-12 education community
- Librarians
- Higher education community including community colleges and universities, both public and private
- Executive management, managers and supervisors, technical staff
- Employees and contractors, volunteers, retirees, interns and student help, and others who access your agency's systems and information
- First responders - such as law enforcement, emergency management, fire department, and emergency medical services
- Information security organizations and associations, such as the Information Systems Security Association (ISSA) or InfraGard
- Consumers and those who use your agencies' services, products, systems, or information
- Members of the media - such as TV news directors, reporters for local newspapers, magazines, or websites

Each of these stakeholder audiences will possess unique characteristics that can be leveraged toward gaining their attention and buy-in. For example, your state or local police department may be interested in establishing links between its computer crimes division and the state's information security incident response team. There may be a need for subject matter experts to assist in training to make this possible. Or the local police department may be interested in enlisting your organization's influence with other information security experts to build further support of their operation to protect people from identity theft or improve their own information security.

Build a list of contacts that can be reused. Various contact lists can be obtained from many already established resources within your state, such as Internet listings of elected officials, or an existing Information Security Officer list. Ask if you can prepare a message and whether the owners of these lists would consider sending it to their members on your behalf. You may find that most owners are readily open to accommodating these types of requests. Know where to go and don't be afraid to ask. As you develop communication channels to reach targeted audiences and stakeholders, you may find these lists and communication channels beneficial for a variety of specific purposes such as communications during a crisis.

Step 5: Make Advocates Out of NaySayers and Non-Believers

Overcoming Challenges by Creating Advocates – Stakeholder Commitment and Engagement

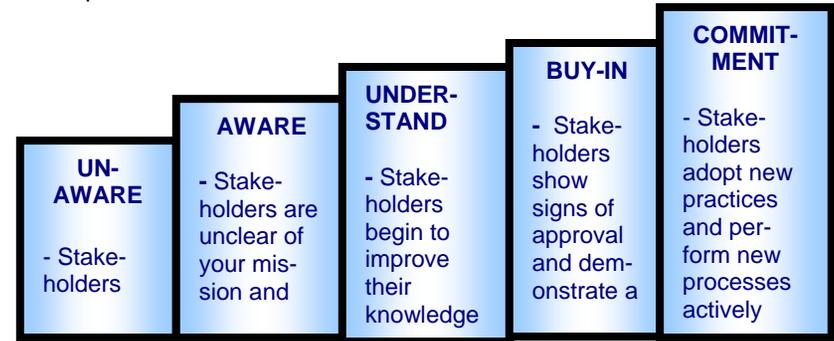


The purpose of any strategic outreach plan is to identify key stakeholders and potential partners, and gain their active support of your organization's mission. It is important to note that this type of involvement does not happen overnight and the opinions of each of the audiences and individuals you reach out to will develop as you successively engage each. Relationship building, as you know, can take time and effort to ensure all involved parties are moving in a direction that makes sense and is beneficial.

Phases of Stakeholder Commitment

As depicted in the following chart, the process for gaining stakeholder commitment evolves over time. The strategic objective is to move your stakeholders' perceptions of your programs and initiatives from

“unaware” to “commitment” using various resources, tools, techniques.



How you engage your stakeholders will depend of their level of awareness or commitment; groups with only little or no understanding of your programs will need information that is more general in nature to “get them up to speed” on what you can offer them. Moving them toward commitment may require more effort and time than would take for an organization that has already bought into your program and is, for example, regularly involved in your typical operations and activities.

Sometimes, moving a potential partner through the commitment process requires overcoming additional challenges because there may be pre-existing misconceptions about your organization or program. It's important to find ways to communicate your message and provide an opportunity to turn a potential skeptic or “naysayer” into an advocate for information security. In some cases by simply involving them in the process and giving them a role in the program you can achieve that goal.

There are times that you might have to take a proactive role in engaging an organization or individual who may not necessarily fully understand your perspective on information security. Consider having an informal conversation, say at lunch, or over coffee, to ask for his or her feedback on certain issues. Listen to what he or she has to say and do your best to implement his or her ideas and feedback into the program. You may find that this person becomes a strong advocate.

Another example might be to talk honestly, in a non-threatening tone, to an individual who has been involved in or even responsible for a security breach. These individuals may often feel embarrassed and defensive because of the incident. Asking them for their input on how to better ensure the breach doesn't occur again can be very