The Ten Commandments of Information Security Awareness Training

Mark B. Desman

Probably the most consistently frustrating aspect of creating a solid program of information security within virtually any installation is to gain the cooperation of the staff who use the organization’s information assets on a daily basis. By and large, they are not steeped in information technology wisdom, nor do they care much about those who are. To the average non-IT employee, “techie” is a term of scorn more often than admiration. And, unfortunately, “techie” is the descriptive name they assign to anyone in the computer-oriented world.

I hasten to add that I am not necessarily talking about someone who is completely computer illiterate. Today, finding one of those anywhere who is familiar with pavement and electricity would be a daunting task. These folks work with PCs every day, but know whom to call when anything untoward occurs: “Call the techies, it’s down again!”

The teaching of information security awareness, then, must be directed toward persons who know what a PC is, have varying sophistication in its use, but are not fluent in technical acronyms, data flow, or network topology. They know the box; they know little of what goes on inside of it or once their transaction has begun its journey down the line. Most of all, they know they are busy with their day-to-day duties and will not spend time on something they deem not to be worthwhile.

This situation then creates another area of communications concern: how much knowledge exists out there and how do I convey information to the largest percentage of the audience at hand? Unfortunately, no simple answer exists. There is homework to be done — first to identify the audience and, second, to ascertain their level of sophistication. That being accomplished, we need to explore methods to get out a meaningful message and to make certain that the largest number possible receive and process your words.

The following ten tips in reaching your audience are not really new (Exhibit 1). They have been bandied about in a number of publications — including my own — for some time. What I have attempted to do here is to encapsulate them in an organized man-
ner so they can be applied to a program in a step-by-step manner. Taken from the top down, compliance with them should give you the greatest chance to get your message across.

What I have done here is to list the “commandments” in order and expand on the meaning of each. In this format, we can take an orderly approach to synthesizing our program.

THE TEN COMMANDMENTS OF INFORMATION SECURITY AWARENESS TRAINING

I. Information security is a people, rather than a technical, issue.
All technical tools, access control software, firewalls, hardware identifiers, or any other hardware/software measures, are directed at controlling human access to systems assets. Therefore, the cooperation of the people using such tools must be enlisted. Baseline policies, standards, and procedures are the foundation of this concept.

The consistent error that information technology professionals have made since the days of pure mainframe processing environments is to think that technology will provide all the answers. Somehow, they have missed the fact that what we process is for people and the output is used by people. In today’s environment, we give them the ability to control their own processing and to carry corporate information assets far afield in pursuit of their daily tasks and the needs of the business.

We know where all of our equipment and information is and we (hopefully) know its value. It is the user outside the computer center and maybe outside the company walls that we must educate in the safe utilization of the considerable information access we have granted them. We can use all the hardware and software tools we wish, but they must be aware of their own responsibilities in protecting what they use daily from external threats.

Communicating with them is the most important single point of the overall information security system.

II. If you want them to understand, speak their language.
In general, people are intelligent. However, people from different backgrounds and work environments might not be familiar with the jargon of the information technology (IT) field. Learn to speak their language; communicate with them in it.

In South Florida, where I currently reside, Spanish is often more commonly heard than English, and to get along, one must learn at least the rudiments of the language. There have been occasions when to order in a Cuban restaurant, Spanish had to be used to be understood. English, the official

EXHIBIT 1

The Ten Commandments of Information Security Awareness Training

I. Information security is a people, rather than a technical, issue.
II. If you want them to understand, speak their language.
III. If they cannot see it, they will not learn it.
IV. Make your point so that you can identify it and so can they.
V. Never lose your sense of humor.
VI. Make your point, support it, and conclude it.
VII. Always let the recipients know how the behavior that you request will affect them.
VIII. Ride the tame horses.
IX. Formalize your training methodology.
X. Always be timely, even if it means slipping schedules to include urgent information.
language of this country, just is not always serviceable in this area.

My comments are not meant as a political or sociological statement, but rather to indicate that we need to make adjustments in our presentation to be understood. Just as people from Latin America have problems with English, so do non-IT-based users. They might well have a jargon of their own or at least be hopeful that communications are in common English, rather than stilted or technical terminology.

III. If they cannot see it, they will not learn it.
Search out the means for reaching the greatest percentage of your audience. If that percentage comes out to be less than 100 percent, locate other means to force an overlap of coverage until the entire audience is reached — successfully and frequently.

Every company has some type of internal newsletter, or journal, either in print or online, that is published periodically. Also, there is e-mail and often even a Web page as a means to reach all staff members.

Before going to great efforts to create new forms of communications media, make a point of exercising what means are available. They have the multiple advantages of reaching all or most of the staff and are already well recognized as a source of information. Your input will not only enrich what they offer, but will reach the widest audience.

IV. Make your point so that you can identify it and so can they.
Every communication must have at least a single point to be communicated. Make sure that it is readily identified, and its purpose likewise. Each point should contain the reason for the communication, along with the actions requested and the reasons for them.

Always have a theme for a news bulletin or release. Generally, you will make these contacts to address a certain condition, whether it is writing business e-mails or addressing a virus. Policies and standards will cover many points but should be in outline form, so as to designate the different points.

V. Never lose your sense of humor.
No matter how serious an issue is, it can be handled without biblical overtones. There are places to make light of the subject; learn and apply a bit of humor to them. This is not to suggest that your communication should be a humor piece, but it need not be so dry as to deter readership.

Anything you prepare has two goals in mind: to be read and understood, and for any ensuing items to be likewise accepted. If your releases are readable and light, where lightness is appropriate, people will enjoy reading them. No one says that imparting knowledge has to be painful for the audience. Find a way to sugar-coat your message without diluting it.

VI. Make your point, support it, and conclude it.
Do not bury people under verbiage. Second pages of reports or releases are not often read. The presence of a third or more pages will decrease the chances that any of it will be seriously read and will do so at a rate inversely proportional to the number of pages presented.

All of us tend to let our muse take over at times. When the opportunity to write presents itself, we jump in with both feet. Unfortunately, as with any business communication, excessive length tends to lower readership. Even in the most detailed reports, there is a management summary that rarely exceeds two pages despite the volume of what follows it. Try to keep that term — summary — in mind when writing.

Our efforts are to inform, not to create the “great American novel” or to put words on paper to be ignored. Brevity is often the best means to do that. Choose your words carefully, review them for clarity, and ask yourself whether the point is clear and completely addressed. Finally, have you told your readers what they must do?

People want to understand what taking a specific action will buy them. Always answer the question: “What's in it for me?”
VII. Always let the recipients know how the behavior that you request will affect them.
People want to understand what taking a specific action will buy them. Their understanding of the need for security might well be in stating how the profitability of the organization is directly related to their position and income. Always answer the question: “What’s in it for me?”

Unfortunately, people are still driven by what affects them personally. When asked to behave in a certain way, some will follow blindly while others will want to know why they are expected to perform as requested. It is the latter — usually the majority — to whom you must address your communications. Make it clear that performing a specific action in a specific manner is good for the company; for example, reflects on the bottom line. What benefits the organization will benefit those who draw their income from it.

Do not be afraid to draw profitability, stock prices, exposure to loss, or litigation into the conversation. Remember: your audience uses the systems you protect every day. They probably know more shortcuts and loopholes than the developer. Worse, they perform their daily functions well outside your field of view. It is up to you to help them understand how important their continued compliance is to the organization, to their income, and, ultimately, to their positions and themselves.

VIII. Ride the tame horses.
Every company has communications media in place and people who maintain and distribute them. They are generally hungry for good copy and can assist you in getting your message across. Take advantage of their skills and the vehicles already in place.

Likewise, learn and make use of any art or copy production departments within the organization. Your message will be better received if cleverly presented.

We used to refer to this point as “reinventing the wheel.” As I see it, inventing is a matter of thinking and testing. Breaking a wild horse, on the other hand requires hard, physical work and a lot of time, things that few of us have in abundance. Why not, then, climb onto an already trained horse? They are usually available with only a little searching.

Forgive my rustic analogy, but its point is to demonstrate that your time and effort can be better utilized in creating copy than in finding ways to distribute it. As mentioned, there are usually plenty of internal communications media available in which to publish, and such publications have the added advantage of already being in place and recognized as a news source by the majority of staff. Better yet, rarely do any of them have enough people writing copy for them. If your work is good, it will usually be happily accepted. Therefore, make certain that your work is carefully edited for content, style, and accuracy. If the publication has length or reading-level standards, be sure to comply with all of them.

In those instances where the publication has problems keeping its editions to a reasonable length (yes, it does happen!), your work must be good enough to displace something else. You now have the combined responsibility to put forth a submission that is not only completely within standard but important enough to warrant publication. Be ready to explain why your piece should be selected for publication.

On those occasions when you need “something special,” be aware of any groups within the organization that can provide help in printing, poster making, making copies, or even Web design. Most of these departments can be of great assistance in getting your message across. It is better to work with a current Web designer than to take HTML courses to get your work published.

Enjoy your ride!
IX. Formalize your training methodology.
Try to build a program that includes brief but formal classwork as well as written or oral communication. Keep records as to who has taken the class and when. Put a formal “security agreement” in place that must be renewed annually. With printed or electronically distributed media, be sure to maintain a reasonable and minimal number of such communications within a given timeframe. For example, using an e-mail newsletter on a monthly basis does not demand that it be delivered on a given date, only that it appears approximately 12 times a year. Space them far enough apart so that there is usually one per month.

There is never a better time to introduce your information security program than to have a formal presentation during new employee orientation. This is a good time to present documentation and to introduce the locations where policies and standards can be found. If you have a sign-off form for the acceptance of responsibility, this is the natural place to include it.

With normal staff turnover, it will take several years for everyone in the organization to go through the class materials, so it is good practice to have it available in another form for current staff. If the company’s training format is sufficiently sophisticated, a computer-based training (CBT) tool can be developed that current employees can use at their own pace. Hopefully, that capacity is tied to a system that maintains records of who has taken what class. By such means, the course can be directed to certain individuals. If all else fails, present the class for general distribution a few times a month.

Maintain a presence by keeping something in front of staff on a regular basis. This might be an article in a company newsletter, on a Web page, or in a separate bulletin.

X. Always be timely, even if it means slipping schedules to include urgent information.

New viruses are not released on schedule, nor do hackers work nine to five, Monday through Friday. If an issue arises, get the communication out now! In a very short time, staff will begin looking for your releases when an event occurs. Assuming a complete and honest report of the situation, what is being done, and what is expected of them, users will look forward to receiving these reports. Not only will they be getting the needed information, but also each communication will support the concept of overall information security.

A hot topic is like a hot tip on a racehorse: you have to have it on time or it loses value rapidly. Viruses and denial-of-service (DoS) attacks must be addressed on an ASAP basis. Once the mail channels were clogged with Melissa’s spawn, it was really pretty late in the day to start posting warnings against opening e-mail attachments. That race had already started.

An e-mail, or even paper, bulletin system can keep staff aware of current conditions and threats extremely well. If some of the writing tips in earlier commandments are utilized, as well as leveraging other departments, a very presentable message can go out regularly.

DISCUSSION

Well, there you have them, the Ten Commandments of Information Security Awareness Training. There is nothing particularly earth-shaking in any of them, but the combination will allow you to better put forth your training objectives. The most important thing to remember is to get all the information to all the people in a timely manner and in a format they can understand. Along with their understanding of the issues, you will want to impress upon them the importance of their participation in the overall program. That would be the answer to the “What’s in it for me?” question.

Fortunately, the need for information security is being trumpeted in all the media, accompanying each new virus, hack, or DoS attack. No longer are these adventures simply grist for the technical publication issue, but are found prominently in the mass press. Use these items to your advantage, making sure that you use...
information from the various media (and credit accordingly). For whatever reason, when a bit of information comes from the press, it is more readily acceptable to a large portion of the population than is something directly from you. What with the reputation some of them have earned, it rather makes you wonder a bit. Still, someone is still even buying those tabloids next to the checkout counter.

Build your program to include every source of information that you can find in the technical media as well as the mass versions. Relate what you quote to the conditions at your installation and ride the added credibility.

Above all, remember to come at the issue from all the angles listed. Make sure there is face contact with training sessions and written contact in all of the company periodicals as well as in separate documents you publish. Talk to the audience in all spoken, CBT, or written media. Find out the “language” they speak and put your information in those terms. Make your point clearly, concisely, and briefly so that it will be read and, more importantly, noticed. A short, ubiquitous document tends to get read, no matter how disinterested the reader might be at first. Example: Have you ever availed yourself of any product or service offered by the flyers some stranger has placed under your windshield wiper? Still, have you ever failed to at least glance at the paper? Simply by literally placing it in front of your face, the shadowy distributor has caught your attention enough for you to at least scan his message.

Imagine the effect of a carefully crafted document placed “before the face” of your entire staff. Having used the training methods listed, you will not be talking to someone who is trying to remove a sight blocker from his or her windshield, but someone who knows that what is contained therein is important, that they are responsible for knowing it, and that complying with what is requested is to the company’s advantage and, ultimately, to theirs.