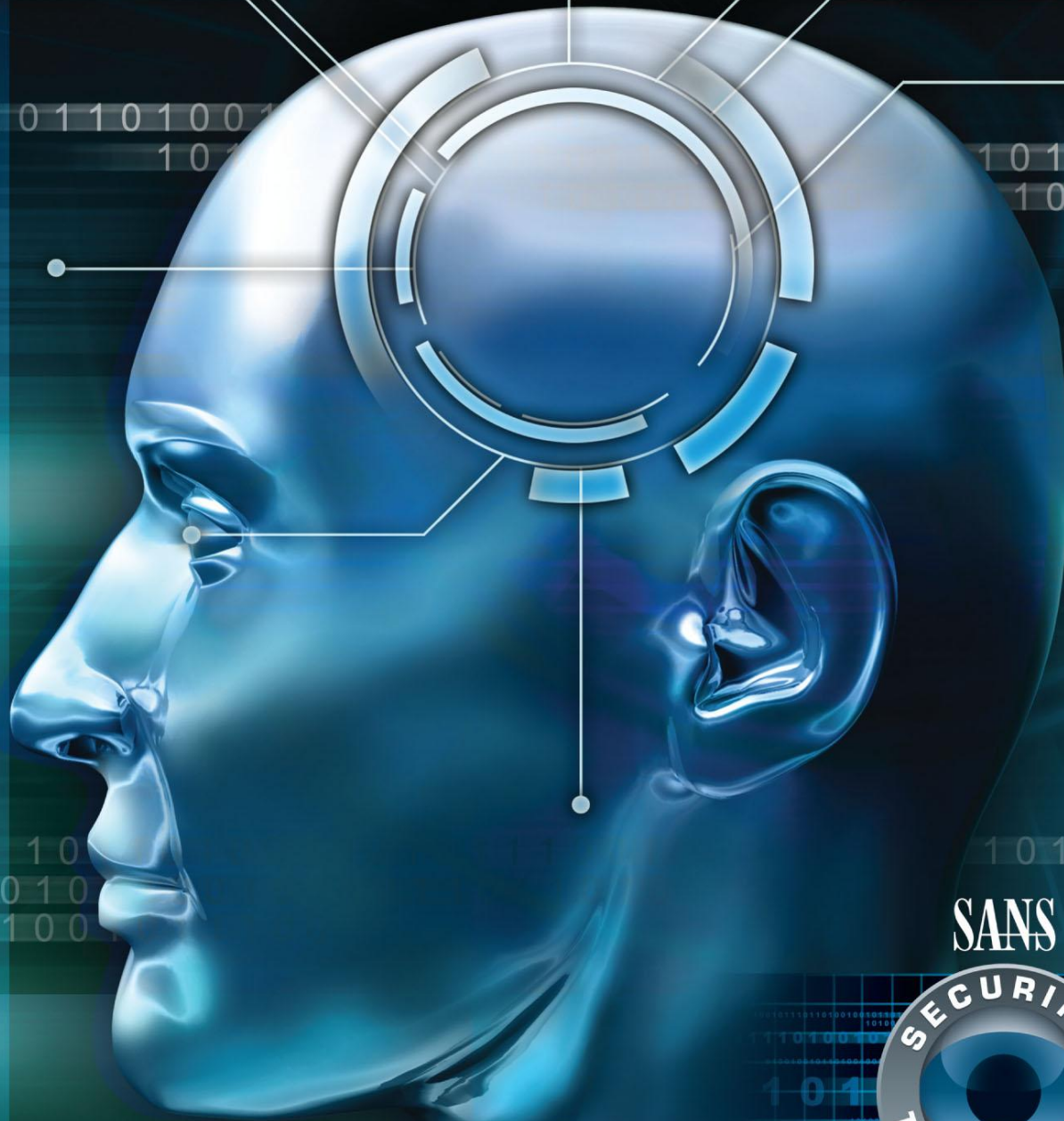


# Security Awareness for the 21st Century

## *SANS Securing The Human*

*"I have never seen such high-quality training, distilled to a perfected message, and compressed into a timeframe that any organization should willingly commit employee time to taking as a risk-reduction strategy."*

-JAMES A. (JIM) RICHARDS III, WV CHIEF INFORMATION SECURITY OFFICER



For more information or to demo the training

[info@securingthehuman.org](mailto:info@securingthehuman.org)

[www.securingthehuman.org](http://www.securingthehuman.org)

US +1 646 257 5875

UK +44 779 257 9875

SANS



[www.securingthehuman.org](http://www.securingthehuman.org)

101101001001011100  
10110100100101101101101



---

# 1. Executive Summary

---

## **Introduction**

There is an old adage, "A chain is only as good as its weakest link." During the past decade, as server-side vulnerabilities have been reduced and companies have improved their perimeter defenses, humans have become the weakest link in the security chain. During the recent RSA attack the attackers were able to exploit the weakest part of the security paradigm, The Humans! In this case, a phishing attack aimed at low level people within RSA. This is not unusual. There are many other examples, including:

- Heartland Payment Systems (130+ million data records compromised)
- Oklahoma Department of Human Services (1 million)
- International Finance Agency (22 million)
- University of California (160,000)
- Network Solutions (5 million)
- European Military Veterans Administration (76 million)
- Australian BlueCross BlueShield Association (987,000)

The important thing to remember is that all of these organizations spent significant money on security. They all had security budgets, departments, policies, firewalls, IDS, and encryption, yet they were still compromised. But as security analyst and researcher Dan Kaminsky recently stated "this nasty habit of blaming the victim from a position of moral superiority has to stop. We're all in trouble, and anyone who thinks they're not potentially compromised today is fooling themselves." The problem is that organizations are doing good things, but they are not focusing in on the right things. They make security more complex than it needs to be. The increase in the volume and sophistication of the attacks leads them to try to fix the symptoms. They get caught up spending money on solutions and still get broken into, which leads to increased frustration.

The root cause of most attacks today is the accidental insider. Attackers have increasingly focused on leveraging human-targeted attacks to compromise organizations, set up persistent back doors, and gain internal footholds in a company's data infrastructure. Many attacks are caused by users simply performing the wrong actions or misconfiguring their systems. No matter how hard organizations try and no matter what they do, it is hard to stop this problem. The trick is to minimize and contain it. In many cases what organizations are missing is an effective user awareness program that addressed the core issues tied to measurable metrics which can lead to a more increased security posture for the organization.

## **Policy, Training and Awareness**

An important thing to remember is that awareness cannot be created in a vacuum. Awareness is actually the third tier in a pyramid that starts with policy and training. It is also important to remember that policy, training, and awareness go together in the following fashion:

- Policy tells the user what to do.
- Training provides the skills for performing it.
- Awareness changes their behavior.



When organizations identify a problem, they often fail to identify and address the root cause of the weakness. If the user does not know what they are supposed to do, it is a policy issue. If they do not have the skills for performing it, then it becomes a training issue. More often than not it comes down to the user not understanding why it is important, which becomes a behavioral issue that needs to be changed through better user awareness. Understanding this relationship is the most effective way to begin an effective User Security Program.

## **Compliance Requirements**

How many times have you heard “Compliance does not equal Security”? But the laws of the land still require that organizations meet certain compliance requirements. In the United States, laws requiring security awareness training apply to:

- The Federal Government (Federal Information System Security Managers' Act, or FISMA)
- The Healthcare Industry (Health Insurance Portability and Accountability Act, or HIPAA)
- Financial Institutions (Gramm-Leach-Bliley Act [GLBA] and Sarbanes-Oxley Act, or SOX)
- Educational Institutions (Family Educational Rights and Privacy Act, or FERPA)
- Publicly-traded Companies (SOX)
- In addition most of the US states and the District of Columbia have passed laws that require customer notification of breaches involving customers' personal information.

For international organizations, security awareness training also applies to:

- Sarbanes-Oxley Act, or SOX
- Payment Card Industry Data Security Standard, or PCI DSS
- ISO 27001

The cost to train an organization's staff to meet its mandated compliance needs (we define this as the average training time per user multiplied by the fully-loaded average hourly cost per user) significantly outweighs the cost of purchasing the most effective security awareness solution for an organization. Certain programs can actually save organizations money because they can deliver the required training in a faster more effective fashion. This reduction in lost production hours doing training means that the training program more than pays for itself.

Organizations need to ensure that the investment they make to train their employees to meet mandated compliance also generates an enhanced security benefit for the organization. This is a more effective use of mandated training dollars.

**“The expense isn't what it costs to train employees. It's what it costs not to train them. You realize that as you grow.” -- Gary Wilber, CEO of Drug Emporium, Inc.**

## **A Framework for Training**

Many organizations do have some type of yearly user awareness program in place. However, because ***most security awareness programs do not map to core areas of risk across the organization, they are often ineffective.*** In order for these programs to be effective, measurable metrics must be used to track the highest risk areas so that awareness programs can be developed to focus on them. Targeted awareness training will reduce risk in these key areas and thereby improve overall security.



Once organizations understand the importance of changing user's behavior, they often struggle on what areas to focus on. **Based on validation and effectiveness, the 20 Critical Controls (<http://www.sans.org/critical-security-controls/>) is a solid framework on which to base awareness.** The critical controls are based on the concept that offense must inform defense. Therefore organizations are fixing the right problems, not just doing good things in the name of security. They provide solid metrics with automation to make it straightforward for measuring and tracking success. By utilizing the 20 Critical Controls, organizations can implement an effective awareness program that allows security to be a business enabler by showing a measurable reduction in both security violations and cost.

## **Measurement**

Measurement is important on two axes. Firstly an organization needs to understand what the level of security knowledge is among their people. This can be done by survey or by test and by performing such a test the organization will understand more effectively what security knowledge areas are deficient and where it needs to focus its User Awareness training. Some ideas that organizations can use to ramp up the intensity of their User Awareness program by using testing include:

- Compare results across departments and divisions. Establish internal competition inside the organization to see which department has the highest rate of security awareness. Turn weekly discussions into opportunities to build friendly rivalry re who is the best.
- Where possible obtain external metrics to understand how your organization compares against other organizations in your industry. Customers and Partners are starting to make their purchase/partner decisions based on who is going to best protect their personal data.

The second axis for security measurement relates to measuring how effective the User Awareness training you deploy actually is. This can be as simple as ensuring that the Users actually attended/watched/listened to the training to more specifically measuring their understanding of the training. Where possible this should be done automatically by using a SCORM-compliant Learning Management System (LMS). An LMS allows you to deploy the training in a formal structured fashion and then measure as your organization deems appropriate.

## **Keeping Content Updated**

Many organizations choose to build their own security awareness program in-house. This is a major mistake for two reasons:

1. It takes a significant level of effort to build a robust security awareness program – especially one that has an effective framework and meets required compliance needs.
2. The level of effort to maintain such a program and keep it updated to the latest attack data is considerable and quite often underestimated. And if it's not done the effectiveness of the program will diminish.

At SANS we advise organizations to find an external vendor for their security awareness solution. Find a vendor that has built their security awareness program on an effective framework. Find a vendor that has a regular schedule for updating their program. This is the key to keeping the program fresh and relevant.



---

## 2. SANS Security Awareness Resources for Users

---

How your organization communicates its awareness program message is as important as what is communicated. You are moving away from training professionals in their chosen field of endeavor to a place where many Users fail to understand the importance of what they're being asked to take training for. This is a significant challenge, a challenge often failed because the suboptimal approach is used.

Several easy to execute

- Try to make the training you deploy personal to the User. If they feel that it is important enough for them to relate the training to their family they will retain the training for longer and work more securely
- Ensure that the training is relevant to your organization. Make sure that the training is branded for your organization. Do not just rely on basic generic training. If your organization requires awareness on specific aspects of your business then custom develop this training either internally or through your vendor.

At SANS we try to simplify awareness training by breaking it down into individual training modules. Each training module focuses on a specific security topic, shows how it affects the employee, and then provides solutions. Each training modules uses multiple communication channels, ensuring the greatest learning impact for your employees. Each training module shares the same images, format, and topic across different materials, ensuring your message is continually reinforced. For example, if you choose a training module on social engineering, you can have a computer-based training video, newsletter, poster, and screensaver for that topic all using the same images and format.

### 1. Computer-Based Training

Computer-based training is a very effective way to train employees and change user behavior. Training videos are easy to access, allowing users to view the training whenever they wish, dependent on their schedule. Online training

- It is cost effective by eliminating the personnel and classroom facility costs for live training and provides an entertaining and flexible medium for organizations to easily distribute training to their different offices.
- It delivers the training in a consistent fashion. It is not dependent on the teaching skill of the individual trainers.

SANS' security awareness training is provided in a SCORM-compliant format, ensuring it can be hosted by either the purchasing organization's own SCORM-compliant LMS or in SANS Virtual Learning Environment (the SANS VLE is a hosted LMS service) should that organization so wish to utilize.

SANS' security awareness training is also US Federal Section 508 compliant, which ensures accessibility for personnel with hearing disabilities.

### 2. Monthly Newsletters

One of the primary methods to reinforce online and on-site training is newsletters. Our awareness newsletters consist of a two-page newsletter that you can provide to your employees every month. Each newsletter is part of a training module, sharing the same topic, images, and format. This reinforces the online training. Each newsletter is branded with your organization's logo and security contact information.

### 3. Monthly Posters

SANS Securing the Human also provides awareness posters. Just like the newsletters, each poster corresponds



---

[securityawareness@sans.org](mailto:securityawareness@sans.org)

[www.securingthehuman.org](http://www.securingthehuman.org)

to a specific training module, using the same images, topic, and format to reinforce your awareness program. Each poster is designed to take the key points from the training module and present them in easy to read bullet point format. Each poster uses high-resolution graphics, ensuring you can print the posters as large as you wish, and can be branded with your organization's logo and your security team's contact information.

#### **4. Screensavers**

Screensavers bring your security message directly to your employees' desktop and their daily work environment. Just like the posters and screensavers, the screensavers will use the same topics, format, and images found in the respective training modules. This ensures the same message will be reinforced in a variety of different media.

#### **5. Security Awareness Webinars (new security awareness training product)**

Certain organizations still like the idea of live on-site training for their employees. However, the cost to bring all the employees to a single location to take the training can be counter-productive. SANS can work with any organization to agree on a list of security awareness topics for a series of customized webinars. A schedule is developed for SANS Certified Instructors to deliver one webinar each month for a 12-month period. The customized webinars are taped and available to the organization for use throughout the year.

#### **6. Surveys and Assessments**

SANS Securing the Human can provide security awareness assessments that you can use in conjunction with your training to establish metrics to track training effectiveness. These assessments have been developed by the assessment and certification body GIAC ([www.giac.org](http://www.giac.org)), which is ANSI-compliant. They are a series of questions designed to gauge employee awareness of specific policies and security behaviors. These surveys are often done online, allowing employees from around the world to quickly and easily participate. These can be used to establish a baseline, which your organization can measure against over time to provide a series of metrics.

#### **7. Language Customization**

SANS Securing the Human video modules are currently available in English. The training can also be made available in additional languages. Voiceovers are all completed using native speakers. Please contact SANS for additional information.

#### **8. Custom Modules**

SANS can also create custom training for your organization. This is a structured process and the quality of the product is the same as that for our core security awareness training. This process is described in detail in Appendix A.



## 3. Training Modules

---

The more information you communicate to your employees, the less likely they will remember it all. Therefore there is a need to prioritize the security topics covered. The modular approach used by SANS gives you the greatest flexibility to deliver an effective security awareness program for your organization.

### **SA-00. Introduction – 0:54 minutes**

We begin the program by explaining what your users can expect in their training. Specifically we explain that this training will teach them who is targeting them, how they are being targeted and why. We also explain the course will teach them how to protect themselves, their families and your organization.

### **SA-01. You Are The Primary Target – 2:08 minutes**

Often employees have the misconception they are not a target. Instead they believe that cyber attackers only target large systems, such as databases or web servers. What they do not realize is that they are often the weakest link in any organization, that they are a target. The goal of this module is to change that misconception and make employees understand that they are often the primary target and under constant attack. In addition, we teach them that what they will learn will not only protect them at work but at home. This approach can resonate and make them more motivated to learn and become involved in the success of your organization's security program.

### **SA-02. Social Engineering – 3:41 minutes**

Many of the attacks and concepts we cover are based on social engineering. We explain what social engineering is and how attackers can fool and exploit humans. One of the most successful ways to explain this concept is to use a non-technical example. We demonstrate social engineering by explaining how your credit card number can be easily stolen from you by simply asking for it after you check into your hotel room. We then show a more technical method using the real world example of a malicious website pretending to distribute anti-virus software.

### **SA-03. Email & Instant Messaging – 6:51 minutes**

One of the primary means of attacks and exploitation is through email. Email is enabled in almost every organization. It is also very simple method for large scale, random attacks and smaller more targeted attacks. We use real world examples including phishing, spear phishing, malicious attachments and scams to demonstrate how employees can be targeted and attacked using email. This module also shows how these same attacks and lessons learned can be applied to Instant Messaging services such as Skype.

### **SA-04. Using Your Browser Safely – 3:09 minutes**

The browser has become the gateway to the Internet; it is the primary tool that employees use to search for information, access different media types, download files and other work related activities. As such, browsers have also become the number one application that attackers focus on. We make employees aware of best practices for using the web, such as keeping the browser updated, avoiding bad neighborhoods, and being careful what they download.

### **SA-05. Passwords – 3:38 minutes**

Passwords are the keys to the kingdom and employees must guard them well. We cover what passwords are, why they are important and how employees can best protect them. We cover what makes a strong password and how they can be easily remembered. We also cover how different accounts should have different passwords, not to share passwords with others, not to use work accounts on public computers such as those at libraries, and other key best practices.



**SA-06. Encryption – 1:54 minutes**

Few employees know or understand what encryption is or its value. This module explains in simple terms what encryption is, how it works and why data should be encrypted. We focus only on the most common uses of encryption, such as encrypting files or encrypted browser connections.

**SA-07. Data Protection – 2:17 minutes**

More and more employees are beginning to use personal devices for work related activity. This module explains the risks of using personal devices for work and why their use is prohibited. Include this module only if your organization prohibits the use of personal devices for work related activities.

**SA-08. Data Destruction – 1:55 minutes**

Employees often mistakenly believe that when they delete data the data is gone for good. They are unaware that it can and is easily retrieved from almost any device. This dangerous misconception is seen in numerous news reports of used computers purchased on eBay with millions of private records, or confidential data recovered from camera memory chips. We explain the concept of wiping and why it is important to wipe, and not to simply delete confidential data.

**SA-09. Policies – 1:07 minutes**

Every organization has to monitor their networks and organization in order to protect it. In the process of this monitoring, the activities and communications of employees may be captured and recorded. Employees should be aware of this. This module covers Acceptable Use Policies (AUPs), such as what websites are not allowed, what email can or cannot be used for, or what applications can be installed on a computer.

**SA-10. Hacked – 2:09 minutes**

No matter how effective a security team and their processes are, there will be incidents. This module focuses on how employees can help by identifying and reporting an incident. We cover things to look for, such as suspicious activity or virus alerts and whom to report an incident to.

**SA-11. Mobile Device Security – 2:18 minutes**

Today's mobile devices are extremely powerful, especially smartphones. In some cases these devices have the same functionality, complexity and risks of a computer, but with the additional risk of being highly mobile and easy to lose. We cover how to use mobile devices safely and how to protect the data on them.

**SA-12. Telecommuting – 2:25 minutes**

For many organizations employees are no longer working at the office. They work from home or on the road while traveling. Since organizations no longer have physical control of the user's work environment, there are unique risks for the telecommuter. This module focuses on how these employees can protect themselves and your organization, including laptop security and creating a secure, mobile working environment.

**SA-13. Physical Security – 2:22 minutes**

While physical attacks against your data are less likely to happen, when such incidents do occur they can have a large impact on your organization. In this module we explain how attackers will attempt to trick and fool their way into restricted areas. We also discuss how employees can protect the physical security of your facilities, including enforcing use of company-issued identification badges.

**SA-14. Protecting Your Computer – 2:02 minutes**

Your employee's computer is ground zero for malicious cyber activity. However, just some basic steps can go a long way to protecting it. We focus on the three most effective steps your employees can take, specifically keeping their computer updated, using current anti-virus and not disabling their host firewall.



**SA-15. Wireless Security – 2:20 minutes**

Often the most common way employees connect to the Internet is through wireless connectivity, usually Wi-Fi. This module discusses the risks of Wi-Fi and steps that employees can take to protect themselves.

**SA-16. Social Networking – 5:02 minutes**

Sites such as Facebook, Twitter and Flickr have exploded in popularity, with employees posting all sorts of private information, not only about themselves but about their daily work activities. This type of data sharing is dangerous for organizations, especially when confidential information is distributed. Cyber attackers often use trust relationships within these sites to spread malicious code. We discuss these risks and simple steps your employees can take to protect themselves and your organization.

**SA-17. Insider Threat – 2:43 minutes**

Insider threats are trusted employees, contractors or third party members that abuse that trust to exploit an organization. This module explains what this threat is, why this threat is so dangerous, and ways to identify and report the threat.

**SA-18. Advanced Computer Security – 4:41 minutes**

This module includes all the information from the Basic Compute Security module but adds greater technical detail, including advanced technical measures to protect your browser, your privacy and use of secure DNS services. Unlike most other modules, this one also recommends specific websites that provide additional free, security services such as Qualys' Browser Check site.

**SA-19. Help Desk – 3:45 minutes**

Help desks are often one of the most targeted groups within an organization. These people communicate with and assist a variety of members of your organization. They are granted a great deal of both trust and power. In addition they deal with a variety of people they do not personally know. As such additional steps must be taken to both educate and protect these individuals.

**SA-20. IT Staff – 3:56 minutes**

Your IT staff are highly skilled individuals with privileged access to your critical systems. However just because they are technical does not mean they are secure. This module teaches them that they are often targeted in cyber attacks and must be extra diligent. Measures include proper use of both their own and administrative accounts, protecting passwords, and limiting the amount of organizational information they share on technical forums. In addition we cover some steps they can take to detect if a system is compromised.

**SA-21. Ethics – 3:04 minutes**

Ethics defines the socially accepted behaviors in your organization and culture. This module explains that employees are expected to behave in an ethical and fair manner, that cheating, stealing or lying will not be tolerated and that if employees are confused or uncertain on what the right actions are, how to get help.

**SA-22. Protecting Your Family – 4:25 minutes**

One of the greatest challenges of being a parent is giving your children the freedom to explore and learn from the Internet, while at the same time protecting them from many of its unique risks, including predators, cyber bullying and in some cases protecting children from themselves. While this module is not specific to securing an organization, many employees find this information extremely valuable. This module helps motivate employees about your overall awareness program and gets them engaged.



---

## Appendix A – Custom Video Development Process

---

SANS uses the structured process below to ensure your customized videos are developed on time and meet your expectations. Just like designing and constructing a high rise tower, training videos are a highly complex solution with many different parts working together, including the integration of images, animation, titles, transitions, sound effects, music and voiceovers. It is important each layers builds on the other. In addition, any changes to a step can have a dramatic impact to other elements, delaying project design. This is why a structured step-by-step process is followed. Each step below must be completed in sequence before we can move onto the next step. If you have any questions about any of the steps, please contact your SANS project manager.

**1. Responsibilities:** The first step is identifying and confirming your primary point of contact for all decisions. While we understand more than one person in your organization may be involved in helping review and decide on materials, we need one contact from your organization that we get all final decisions from.

**2. Video Requirements:** During this step we need you to identify and document all unique requirements for the videos. It is critical that these requirements are identified at the beginning as they have a large impact on how your videos are designed and developed.

- How will you be distributing the videos?
- What file format do you want the videos delivered in (such as QuickTime .mov or Windows Media .wmv).
- Do you have any file size limits?
- What aspect ratio do you want the videos (4:3 or 16:9). 4:3 is the older format used by traditional media, while 16:9 represents the newer High Definition format becoming popular on YouTube and newer TVs.
- Do you have any other unique requirements?

**3. Logos and Images:** Does your video require any unique logos or images? If so we need those images before we start. In addition we need these images as vector based files, specifically .ai or .eps format. These file formats ensure the highest quality of your videos during the design process. If that is not possible then please provide images in .psd format.

**4. Topic:** We work with you to identify the topic of each video. Specifically we identify the title, target and goal of each training video.

**5. Storyboard:** This is the next step is developing your video storyboard. This documents the learning objectives of your videos. Specifically we identify and document the key points you want to communicate. These points can include awareness best practices, your security policies, or any compliance or legal requirements that should be taught. In addition, during this phase we ask you questions if you have expectations on how you want the video to look and if so what those expectations are.

**6. Script:** The next step is to develop and document your script. The original draft will be developed by SANS content creation team, then reviewed, edited and approved by your organization. The scripts determine the voice over for your videos. This is the most important stage in the development of the video. All following steps are based on the script itself. Any changes to the script once this stage is complete can incur extensive additional



---

[securityawareness@sans.org](mailto:securityawareness@sans.org)

[www.securingthehuman.org](http://www.securingthehuman.org)

time and costs to your videos.

**7. Voice Recording:** SANS will provide you at least one male and one female voice over for you to choose from for your voice recordings. This person will then do the recording for the voice over, which will then be integrated in to the training video. We will begin voice recordings upon selection.

**8: Editing, Update and Finalize:** Our team creates the actual training videos combining the elements of the voiceover, imagery and video animation. Your organization is then given an opportunity to review and approve the content. Once approved, any changes after this point can incur additional time and costs.

**9. Sound Effects:** The next step is to bring the existing videos into our sound studio and develop and add professional sound effects.

**10. Final Edit:** The videos updated for any minor corrections, then rendered and exported based on your requirements decided in step 2.

**11. Translation:** If the videos are to be translated all translation happens after the English version is complete. This ensures the highest quality of translation and ensures the different videos match in message and format. Translations normally take four to six weeks, which includes translating the script, recording the voice over and integrating the new language with the video.



---

[securityawareness@sans.org](mailto:securityawareness@sans.org)

[www.securingthehuman.org](http://www.securingthehuman.org)

**“This computer-based training is truly designed for the 21st century employee. It addresses both our compliance requirements and our enhanced security needs.” -- Ahmad Alkamali, Director of Security, Etisalat**

Should you require further information or wish to demo the training please contact:



## Shearwater Solutions

Level 1, 6 Spring Street  
Chatswood  
NSW 2067  
Australia  
Tel: (02) 9488-4600  
[sales@shearwater.com.au](mailto:sales@shearwater.com.au)  
[www.shearwater.com.au](http://www.shearwater.com.au)

or

## John Fitzgerald

Managing Director, SANS Securing the Human Program  
SANS Institute  
8120 Woodmont Avenue, Suite 205  
Bethesda, Maryland 20814  
USA  
Tel: +1 646 257 5875 or +44 7792 579875  
[jfitzgerald@sans.org](mailto:jfitzgerald@sans.org)

Last Updated for APAC: 03 May, 2011