

**SACUBO BEST PRACTICES ENTRY:  
SECURITY AWARENESS, TRAINING AND EDUCATION**

**Stanton S. Gatewood**

Chief Information Security Officer  
Enterprise Information Technology Services/  
Office of Information Security  
The University of Georgia  
Athens, Georgia 30602  
[www.uga.edu/infosec](http://www.uga.edu/infosec)  
[www.eits.uga.edu](http://www.eits.uga.edu)

## **Abstract**

*Horror stories of breaches in security abound, whether the organization is in higher education, government or the private sector. The University of Georgia is certainly not immune to these problems and, in response to growing security concerns, the Enterprise Information Technology Services (EITS) staff has implemented a proactive security awareness program to inform staff of the potential risks and countermeasures to protect campus information.*

*The SANS (SysAdmin, Audit, Network, Security) Institute's Security Awareness Training and Certificate Program is offered online for all EITS staff and may soon be available to the University's administrative and academic units. The long-range goal is to include the entire University System of Georgia in this opportunity. Through real-life case studies, this commercial, off-the-shelf program illustrates the do's and don't's of basic security awareness. Quiz questions are integrated throughout the program to reinforce key concepts. At the end of the training, a passing score on a 50-question final examination rewards the user with a printable SANS Awareness Certificate of Completion, which is valid for one year.*

*The curriculum modules cover a host of security topics and are presented in a manner which is relevant to all levels of the organization, be they front-line staff or executive leaders. The benefits of this program are legion. For a nominal investment (variable cost of \$1.00 per participant and fixed cost of 20 FTE hours to set up the database and monitor training completion for more than 300 accounts), the University EITS staff has implemented an awareness program that has the potential to train all University users (students, faculty and staff) on security policies, procedures and techniques, as well as increase knowledge of the various management, operational and technical controls necessary to secure IT resources. In addition, successful completion establishes a level of accountability for each participant.*

*Thus, this innovative program aligns the security effort with the bottom line – an ever-present concern for a public institution.*

## **Introduction of the Organization**

The University of Georgia (UGA), established in 1785, is the flagship institution among the 35 colleges and universities in the University System of Georgia. As a federal land-grant/sea-grant institution, it holds public service and outreach, along with teaching and research, as key components of its tripartite mission. UGA operates on a \$1.3 billion annual budget and employs more than 9,500 people. Total enrollment stands at approximately 33,000 – about 24,500 undergraduates and 8,500 graduate and professional students.

The institution's academic reputation is rising steadily, resulting in increasingly selective undergraduate admissions and higher faculty quality. For the past six years, the University of Georgia has been ranked as a top 20 public university by *U.S. News & World Report's* "Best Colleges" guide. Since 2001, more than 25 students have won major national scholarships, such as the Marshall, Rhodes, Truman, Goldwater, Gates-Cambridge and Mellon. In addition, private giving to the University soared close to \$100 million in 2004-05, and UGA ranked 22nd among public universities and 34th among all universities in research expenditures, according to the National Science Foundation.

Of relevance to this Best Practices entry, the University of Georgia has also recently been heralded by the *Princeton Review* as one of the nation's top 10 "most connected campuses," with the best technological capabilities for teaching, learning and communicating.

### **Statement/(Restatement) of the Problem/Initiative**

Horror stories of breaches in security abound, whether the organization is in higher education, government or the private sector: a staff member unwittingly opens an interesting attachment, launching a worm that shuts down much of the system; a student researcher stores information on test subjects in her personal files, which is then violated by a hacker, compromising their personal data; or hackers gain access to sensitive admissions data and credit card information by using a common password that is not protected by symbols or numbers. These incidents are not just legend on college campuses, but are very real problems which can result in severe costs for the organization in terms of repair expense, loss of work hours and damage to institutional integrity and reputation.

Regrettably, no institution is exempt from such security violations, and several such situations have occurred at the University of Georgia and other University System of Georgia schools. To guard against further breaches and to take a proactive approach to promote better awareness in general, the University's Enterprise Information Technology Services (EITS) staffs have implemented an online security awareness program. The SANS Online Security Awareness Training and Certificate Program informs staff of the potential risks and educates them about countermeasures to protect campus information.

## Design

The UGA Office of Information Security recognized early in the process of information security program development that the most efficient and effective way to reduce the risks and threats facing the institution was systematically to educate, enlighten and empower employees, who provide the front line of any security defense. When bad things happen, it is usually because the employees simply did not know better. Security-savvy employees have a distinct advantage because their training influences their behavior.

It is widely reported by industry leaders such as the Gartner Group and *CIO Magazine* that security awareness, training and education offer the best return on investment for organizations seeking to improve their information security. Budget-wise security awareness, training and education via presentations, handouts, websites and the usage of international and national best practices provide an effective means to achieve a strategic security objective.

Making computer system users aware of their security responsibilities and teaching correct practices helps users change their behavior. It also supports individual accountability, which is one of the most important ways to improve computer security. Without knowing the necessary security measures (and to how to use them), users cannot be truly accountable for their actions.

A strong IT security program cannot be put in place without significant attention given to training all users (students, faculty and staff) on security policies, procedures and techniques, as well as increasing knowledge of the various managerial, operational and technical controls necessary and available to secure IT resources. Failure to provide adequate attention to the area of security training puts an institution at great risk because security of an institution's resources is as much a *human* issue as it is a technological issue. A comprehensive IT security awareness

and training program is *the* vehicle to be used to communicate security requirements across the institution.

Rather than merely facilitating passive learning by providing users with a policy manual to read on security procedures, the EITS managers decided to pursue a more interactive and engaging template. They settled on a commercially available, online awareness training program to inform all EITS staff about the risks and threats they face and the simple countermeasures they can take, regardless of their technical skills and/or abilities. The SANS Institute is a cooperative research and education organization, dedicated to information security training—an ideal resource for institutes of higher education.

### **Implementation**

The Office of Information Security requested and stated a need for funding the online security training for the entire central IT organization, EITS. The Information Security Team's total time to develop the awareness program was minimal due to the fact that the online course material was readily available and quite intuitive. The provisioning of the accounts was a trivial task handled by the Information Security staff, with assistance from the Director of IT Communications. The provisioning process lends itself well to small and large organizations/institutions.

The EITS staff developed a communications plan, including a webpage dedicated to the SANS \$1 per seat campaign. In addition, the Chief Information Officer distributed a memo to all EITS staff directing them to participate in the SANS training program. The Chief Information Security Officer led the division directors toward completion of the online course.

The SANS online awareness program offers the utmost convenience to the individual user because it can be accessed from any location at any time, as long as the user has a Web

browser and an Internet connection. The program consists of two to five hours of security modules on such common security topics as passwords, computer viruses, malicious code, data back-up and storage, incident response, personal use and gain, environmental issues, inventory control, physical security and social engineering. The training is communicated via real-life stories that illustrate the do's and don't's of basic security awareness. The user takes a 50-question exam at the end of the training and, if a passing grade is earned, receives a printable SANS Awareness Certificate of Completion valid for a full year.

Implementation of the program has been extremely convenient and cost-effective for the University. The expense is nominal: a fixed cost of 20 FTE hours to establish the database to track awareness training completion and a variable cost of \$1.00 per student, faculty or staff member who participates in the training. Set-up of the program is minimal and can be done via online communications (website forms and email), and estimated time from registration to availability is 10 working days.

The potential payoff for this minor investment is significant when all the possible losses in work hours, operational funds and reputational damage from a major breach in security are considered.

## **Benefits**

The benefits of this program to the University of Georgia are legion. A robust institutional and system-wide awareness and training program is paramount to ensuring that people understand their information security responsibilities, organizational policies and how to use and protect the resources entrusted to them. Training employees also demonstrates that a standard of due care has been taken in protecting information. Simply issuing policy, without follow-up to implement that policy, will not suffice. There can be no accountability without awareness.

Among other factors, the Security Awareness Online Training and Certificate Program:

- educates staff about computer and Internet security risks;
- conveys security “best practices” to help prevent damage due to avoidable mishaps;
- increases security across the organization in a cost-effective manner;
- empowers the individual to perform IT security best practices;
- supports the organization’s security efforts and investments from the bottom up to the top of the organization; and
- aligns the security effort with the bottom line.

The SANS Security Awareness Online Training and Certificate Program offers proof that a training program need not be elaborate nor expensive to be effective. For a very reasonable investment of money and staff time, the University of Georgia has implemented a comprehensive security awareness program that will yield tremendous benefits in the future. It is a prime example of a best practice which can easily be transferred to other higher education institutions in order to better protect all of us from security breaches in this high-tech age.

## **Retrospect**

The University of Georgia's experience with the SANS Security Awareness Online Training and Certificate Program has been positive. Still, heeding a few lessons learned would enhance the level of success for other schools. Specific recommendations include:

- Purchase more seats to distribute to other administrative and academic units across UGA and University System.
- Purchase the SANS online security awareness program and fund the hardware and software for in-house access control: e.g., administration, registration and certification process.
- Solicit interest within our professional schools and colleges to incorporate the program as a tool to be used in class instruction by faculty.