

# Security Education within the IT Curriculum

Charles Border, Ph.D.  
Department of Information Technology  
Rochester Institute of Technology  
102 Lomb Memorial Drive  
Rochester, NY 14623-5608  
585-475-7946  
cborder@it.rit.edu

Ed Holden  
Department of Information Technology  
Rochester Institute of Technology  
102 Lomb Memorial Drive  
Rochester, NY 14623-5608  
585-475-5361  
eph@it.rit.edu

## ABSTRACT

As IT educators we have been asked to bring an increased awareness of information security into our classrooms and to help our students to gain a better awareness of the security implications of many of the things that they do. IT is not, however, a monolithic field, rather it is a discipline made up of several fairly well defined interest areas each of which have their own pedagogical concerns and issues, only some of which are in the area of security. This study is designed to gain a better understanding of the extent to which IT programs and the interest areas within them have changed to include a greater security component, and the means by which this has been accomplished (e.g. through the addition of new courses or the modification of existing courses).

Data to support this area of inquiry has been drawn from several sources. Surveys were sent to attendees of CITC3 that directed them to a web form that gathered information about their perceptions of the need to change their programs and the means by which they had carried out the changes. Interviews were conducted with RIT teaching faculty during bi-monthly interest area meetings and a sample of survey respondents to gain a more in-depth understanding of the issues surrounding both the means and the extent of the changes they had accomplished.

All of the respondents to this study felt that they needed to increase the amount of security content in their IT programs. While all of the respondents described their efforts as works in progress, only two had added new courses. Respondents were equally unanimous in feeling that security content needed to be spread across many courses rather than isolated in one course.

Results from interviews conducted during interest area meetings with RIT faculty indicate the following:

- While all of the interest areas indicated the need to modify their curriculum to enhance the security content in it, each of the interest areas had a very different conception of how this should be accomplished.
- Only the networking group saw the need to add additional courses to the existing curriculum.

Permission to make digital or hard copies of all or part of this work for personal or classroom use is granted without fee provided that copies are not made or distributed for profit or commercial advantage and that copies bear this notice and the full citation on the first page. To copy otherwise, or republish, to post on servers or to redistribute to lists, requires prior specific permission and/or a fee.

*CITC4'03*, October 16–18, 2003, Lafayette, Indiana, USA.  
Copyright 2003 ACM 1-58113-770-2/03/0010...\$5.00.

- The database group felt that adding new security modules to existing courses was the best way to enhance the security content in their interest area.
- The programming group interpreted the need to enhance students' awareness of security as a need to enhance students' awareness of good programming techniques and structures.

## Categories & Subject Descriptors: K.3.2

Computer Science Education

**General Terms:** Human Factors

## INTRODUCTION

The IT field is still relatively young and rapidly evolving. The IT curriculum was designed by individuals in response to a felt need for a computing curriculum that was different from the technology centric Computer Science curriculum. What courses and topics make up the IT curriculum is still a very open question that we as an IT community continue to wrestle with. Since its inception there have been many changes in the world that could have exerted a powerful force for change within the IT curriculum; the burst of the dot.com bubble, the recession, the boom and bust of the telecommunications companies. But none of these evoked such a visceral reaction as the terrorist attacks of 9/11. While watching the Twin Towers burn and ultimately fall it was very clear that bad people were out to attack us and we all had to change our lives to do something about it. In the IT community it was easy to extrapolate this into a need for a greater security component within the IT curriculum.

As IT educators we have been asked to bring an increased awareness of information security into our classrooms and to help our students to gain a better awareness of the security implications of many of the things that they do. IT is not, however, a monolithic field, rather it is a discipline made up of several fairly well defined interest areas each of which have their own pedagogical concerns and issues, only some of which are in the area of security. This study is designed to gain a better understanding of the extent to which IT programs and the interest areas within them have changed to include a greater security component, and the means by which this has been accomplished (e.g. through the addition of new courses or the modification of existing courses).

Data to support this area of inquiry has been drawn from several sources. Surveys were sent to attendees of CITC3 that directed them to a web form that gathered information about their

perceptions of the need to change their programs and the means by which they had carried out the changes. Interviews were conducted with RIT teaching faculty during bi-monthly interest area meetings and a sample of survey respondents to gain a more in-depth understanding of the issues surrounding both the means and the extent of the changes they had accomplished.

All of the respondents to this study felt that they needed to increase the amount of security content in their IT programs. While all of the respondents described their efforts as works in progress, only two had added new courses. Respondents were equally unanimous in feeling that security content needed to be spread across many courses rather than isolated in one course.

Results from interviews conducted during interest area meetings with RIT faculty indicate the following:

- While all of the interest areas indicated the need to modify their curriculum to enhance the security content in it, each of the interest areas had a very different conception of how this should be accomplished.
- Only the networking group saw the need to add additional courses to the existing curriculum.
- The database group felt that adding new security modules to existing courses was the best way to enhance the security content in their interest area.
- The programming group interpreted the need to enhance students' awareness of security as a need to enhance students' awareness of good programming techniques and structures.

## INTEREST GROUP ANALYSIS

At the time this study was conducted<sup>1</sup> the Information Technology program at the Rochester Institute of Technology (RIT) was informally divided into the following curricular groupings: Networking and System Administration, Multimedia, Programming, E-Commerce, and Human Computer Interaction (HCI). All of these groups except for the Networking and System Administration group (the lead author is a member of this group) was interviewed as part of their bi-monthly interest group meetings to gain a better understanding of the following questions: what "security" meant to the group, did the group feel that they needed to enhance the security component of their curriculum, what are the essential elements of security that needed to be included in the curriculum, and what was the best approach to be followed if the security component of their curriculum needed to be enhanced. Each of the groups was very deliberative in their answers and provided very important insights into security education in the IT curriculum.

## Groups and perspectives

### Multimedia:

The Multimedia group was very interested in the topic of security and felt that not enough security content was covered in their curriculum or in the IT core. While little security content is

explicitly contained in any of the syllabi for Multimedia courses all of the faculty felt that including more security content was essential. They felt that security content should not be collapsed into one special "Multimedia Security" course, rather security for them was an all-pervasive topic and as such should be spread across all the courses both in Multimedia and the entire IT core.

For this group of faculty security as a topic had two essential aspects, it involves protecting data coming to a site as well as data residing at a site, and it involved making students aware of how to "handle" data. The first aspect was most easily included in their curriculum through the inclusion of such topics as the interplay between network transport and server technologies, the second aspect they felt was much more difficult to explicitly include. "It is hard to teach about security, but you can teach the right way to do things." Security from this perspective involved teaching students to take their time and pay attention to the ways in which they work with user data and to assume responsibility for the creation of applications that provide a secure environment for the collection and manipulation of user data.

They also pointed to the need to include more of a discussion of the ethical considerations revolving around multimedia and security. The following question was posed to illustrate this concept; "what constitutes hacking of a web server? A web server is an essentially open server that is designed to be interacted with by the world. At what point in that interaction does a user transgress from a legitimate interaction to an illegitimate hacker?"

### Programming:

The Programming group was very concerned that their students were not being given enough security content in their courses. The IT curriculum is built around a three course Java sequence that is designed to give all students a basic introduction to object oriented programming and problem solving through the use of Java. At several points in the current curriculum the Java security model is discussed in a comparative fashion to other programming languages (especially C, and C++). The current emphasis of the program is to solve problems using Java. While this emphasis is considered to be in alignment with the heart of the IT curriculum, it allows students and faculty to become complacent about the means by which those problems are solved. Good security practice, from the perspective of the Programming group, involves going a step beyond just solving the problem at hand, to finding the *correct* way to solve the problem. Security from this perspective is about understanding and following good programming practices.

The Programming group was also concerned that in their upper level classes they did not spend enough time on the following topics: Checking the validity of classes before they are loaded, working with certificates, and implementing different cryptography schemes. Security, as the programming group saw it, ultimately comes down to the programming that makes up the applications. And it was from this perspective that this group saw many of the problems that are currently plaguing the Internet, applications written without following good programming practices, and not using the existing security tools. "It isn't that good tools don't exist, it is that they are implemented poorly." While conceptualizing the implementation of existing tools as being one of the strengths of the IT curriculum, they felt that this should be one of their strengths.

---

<sup>1</sup> There have been several structural changes to the Information Technology Department. The RIT portion of this study was conducted largely before these changes took place. The changes have been more structural than substantive and have had little impact on the results of this study.

## E-Commerce

The E-Commerce group saw themselves as being second only to the networking group in responsibility for teaching good security practices. The applications that their students will be developing are the primary points of contact for most people with that portion of the Internet where security is of primary concern.

In the curriculum as it currently stands security content is limited to a discussion of basic login procedures, simple password rules, the use of the secure shell, SSL, and HTTPS.

From the E-Commerce perspective security has a two-part focus. On one hand security is about technologies and the use of those technologies to prevent users from doing unauthorized things. On the other hand security is about human computer interactions and finding ways to build trust among users and a sense of community. On the technical side the E-Commerce people want to enhance the amount of time spent in their curriculum on such technologies as file security and tightening the permissions on files, user authentication, developing applications that utilize payment gateways, web sever administration, and securing user data at the database level. On the social side the E-Commerce people want to include more discussion and projects relating to building trust through communities, privacy policies, and satisfaction guarantees.

The consensus opinion among the E-Commerce group is that although the curriculum needs to be changed to include more security content that change can be accomplished incrementally through the current course structure.

## Database:

The Database group felt that they were largely beholden to the Data Base Management Systems (DBMS) that they use in their classes for security (Oracle, db2, SQL Server, and Mysql). They did not perceive that they had much control over security except at the design level, especially in their Three Tier Design course. Most database applications operate only in the top two layers of the OSI Model and therefore the role of the DBA, and by extension, the Database group is to make sure that students understand and implement the security controls that are part of the DBMS. This was frustrating for them and they were very interested in finding a way to include more security content in their curriculum especially regarding topics related to LDAP. The problem, they felt was that there was little available time in their existing course structure.

## Networking and System Administration:

Following the paradigm that much of security is keeping the bad guys out at the perimeter the Networking and System Administration group has taken the need to include more security content into their curriculum to heart. This section of this paper will not attempt to catalog all of the efforts that the Networking and System Administration group has accomplished rather it will point to some of the more relevant and interesting topics.

Changes to the Networking and System Administration curriculum have been accomplished through both formal and informal methods.

## Formal

- Professional development: Several faculty members have attended workshops and industry based training programs in security.
- New Masters Degree: As a member of the B. Thomas Golisano College of Computing and Information Sciences along with Computer Science and Software Engineering the Networking and System Administration group has been part of forming a new Security Masters degree that will include courses taught by faculty members from the other departments.
- New course design: New courses have been designed in for both the undergraduate and graduate curricula.
- Facilities: In order to conduct labs in which students explore exploits that might disrupt the normal networking activity of the college we have developed a new lab that can easily be disconnected from the University's network.

## Informal

- Professional development: Informal professional development in the area of security has taken the form of readings and conversations among faculty regarding security related topics.
- Increased security content throughout the curriculum: While few of our syllabi have been changed, we have increased the amount of security content in all of our courses. This has been done either through formal lecture modules or readings related to security or more informal portions of lectures or labs.

## SURVEY RESEARCH

### Introduction:

In an effort to better understand how other institutions are approaching the inclusion of security content in their curriculum a survey was sent out to all the attendees of CITC3 in Rochester, NY during the Fall of 2003 who listed their home institution as being an academic institution (their were several attendees from places such as the ACM, and IEEE) and other than RIT (we had tried to gather information from the RIT attendees as part of the previous portion of the study). The survey took the form of an e-mail message outlining the project and a URL directing the respondent to a form housed on an RIT webserver, respondents were then invited to volunteer to participate in a phone interview to be completed by the researchers<sup>2</sup>. The idea behind the survey structure was to attempt to gather information from people interested in the IT curriculum regarding both, the need for, and mechanics behind, their inclusion of more security content in their IT curriculum. The researchers recognized that this information would be based on the perceptions of the respondents of the need to change their curriculum and would thus have both qualitative and quantitative dimensions. Both the survey form and the phone interview were designed to touch on both dimensions.

---

<sup>2</sup> See appendix A and B for copies of both the original e-mail and the form.

## Survey Analysis:

Response to the survey was not good, the survey was originally sent to sixty potential respondents on 5/30/03. Six people responded for a ten percent response rate. The survey was sent out again on 6/11/03 to the same sixty potential respondents, three additional people responded for a total of thirteen respondents. Of these, six people volunteered to participate in the telephone interview and two people were successfully contacted. Although it was impossible to tell from the actual forms (the CGI script that was used to collect results from the form and e-mail them to the researchers did not gather any information about the respondent) the results seem to indicate that at least two of the respondents might have come from the same institution. While this is not bad (the survey was designed to collect empirical as well as perceptual information) it could lead to one institution's perspective having a greater dominance than it should in the results. Results from the survey are summarized below.

The first section of the survey was designed to gain an idea of the areas of specialization of the respondents and a general idea as to the size of their institution and their IT program.

### Survey Results

#### Personal area of specialization

Multimedia	0
Programming	2
Networking	1
Database	1
Human Computer Interface	1
Other	2

#### Number of students currently enrolled in the institution

Less than 2,000	1
2,000 to 8,000	0
8,000 to 15,000	3
More than 15,000	3

#### Number of students currently enrolled in IT.

Less than 100	1
100 to 300	4
300 to 600	2
More than 600	0

#### Are undergraduate specialization tracks in IT offered?

Yes	7
No	0

Web Development  
Networking/Security

Networks  
Programming  
Web Related  
Systems

Software Development  
Database  
Mainframe  
Web & E-Commerce

Before asking respondents about the ways in which they had responded through their curriculum to the increasing interest in security we wanted to gain a better understanding of the importance of the terrorist attacks of 9/11/2001 on their individual perspectives of the security component in their curriculum. The terrorist attacks were only important to changing the perspective of one of the respondents. This respondent felt that the attacks proved the immediacy of the threat; "people are out there actively and carefully planning to harm and/or destroy us in any way they think that they can." Another respondent simply replied that 9/11 had no impact on their perspective and that more security content was needed prior to 9/11 and the problem is still the same.

Using 9/11/2001, as a starting date, the next question asked respondents if they had implemented any changes to their curriculum to enhance student's awareness of computer security. Responses to this question were mixed but clearly showed that most respondents either have changed their curriculum (four respondents) or are planning to change their curriculum (one respondent). Only two respondents said that they had not changed their curriculum since 9/11.

The next four questions related to the mechanics behind changing the curriculum to include more security content. Our idea in developing these questions was that there are only a few ways in which a curriculum can be changed; by adding new courses to it, by adding new, discrete modules to existing courses, by adding content throughout an existing course, or by completely reevaluating an existing course to include more or different content (the main difference between the last two options is more a matter of scope than substance). The idea behind these questions was to ask those respondents who volunteered that they had changed their curriculum, how they had done it.

Only three respondents answered the question related to the addition of new courses to their curriculum. Each respondent listed one new course and gave the following as course titles; Data Security and Encryption, Cryptography and Compression, and Information Warfare and Defense.

Three respondents answered the next question about the inclusion of new modules in existing classes. One said that they had not added any new modules, another said that they had added a basic security module to an Introduction to Computing general education course, and the third said that they had added a basics of encryption to their Digital Communications course.

Two respondents answered our question relating to the addition of security content throughout existing courses. One replied negatively, and the other replied that the content already existed.

Only two respondents answered our question relating to the comprehensive reevaluation of existing course content and both responded negatively.

The position could be taken that there would be little problem with security if one could protect the periphery of most networks and not allow the bad guys in. This approach would place most of the onus for security, and by extension most of the onus for changing the IT curriculum, on the networking people. Our next question solicited our respondent's ideas on this subject. It posed the

question: “Do you see security awareness as being the purview of any one particular specialization within the IT curriculum, or does it belong to many or all specializations?” Six respondents answered this question and all of them said that security was a concern for all the disciplines. Three respondents added some comments to their answer. One pointed out that the ethics of maintaining the confidentiality of data was an important aspect of security that needed to be taught to students. Two others pointed to the potential development of a new specialization in the IT field dealing with security and one of them gave a name to it, “Security and Audit”.

Our next question sought to gain a better understanding of how respondents felt about the changes they had made to their curriculum. The idea was to attempt to solicit the respondents perspectives not only on the exact changes they felt needed to be made to their curriculum, but their general impressions on whether they were done with modifying their curriculum or if any changes had yet to be made. Six of seven respondents answered this question, only two of the respondents felt that they were even done for the moment with changes, the rest all felt that they had to continue to modify their curriculum. Two felt that they needed to develop either a focus track or a concentration on security or IT Audit, Security and Control. One felt that they needed to develop a new course in Computer Security and reevaluate their entire curriculum to include more security content. One felt that they needed to continue to evolve to meet increasing demand for security content, another felt that they needed to continue to change but was not specific as to how and the last felt that they needed to continue evolving, but were unsure where and how.

As a new discipline in a quickly changing field we are constantly being asked to change. Security is one area in which we have been asked to change, but may not be that different from other areas in which similar pressure has been placed on us. The next question sought to find out the perceptions of the respondents as to how long it took from the inception of the idea for change to the implementation of those changes. Four respondents answered this question. One respondent said that it took about one year from the inception of the idea to its implementation, another said one term. Another said that they had just developed a networking focus track and that it would take about two years to fully implement the new courses. The last respondent pointed to the need to enhance their faculty’s expertise as the main stumbling block and that as that was enhanced more changes would occur.

The modification of the curriculum can be viewed as a discrete act that one does and then is done with. Or it can be viewed as an ongoing process which is never completed, but is always a work in progress. Our next question posed this idea to our respondents and all four of those who answered this question felt that the enhancement of the security component of their curriculum was a work in progress (there were no comments listed in this question).

The evolution of a curriculum can be a very labor intensive endeavor that can be facilitated by the administration of a college or university in a number of ways (course reductions for new course development, financial incentives for new facilities, administrative assistance, etc.). Our next question sought to find out if the respondents had received any assistance from their administration to facilitate the evolution of their curriculum to include more security content. Of the four respondents who responded to this question only one replied affirmatively. The rest replied that they had received no assistance outside of their department.

## **TELEPHONE INTERVIEW ANALYSIS**

One of the topics that this study tried to better understand was the evolution of programs over time. This is an extremely important topic for the future of higher education and receives little attention in the literature. Like most topics that must be studied longitudinally the adaptation of any curriculum over time is difficult to do for many reasons. One of the reasons is that it is difficult to find a common starting line, one action that precipitates a response by many institutions. We saw the tragic events of 9/11 as a particularly stunning catalyst for change and we wanted to see whether or not it had influenced different institutions to enhance the security component of their IT curriculum two and a half years later to this change and if it had, how had they responded.

Attempts were made to contact all the respondents who volunteered for the telephone interview at the phone number they listed. Six of the seven respondents to the survey volunteered to participate in the telephone interview of these two were successfully contacted.

The two respondents to the telephone interviews were from very different institutions. The first respondent explained that at his institution the administrative style is very hierarchical and that they are unable to respond very effectively to changes in student demand. They have created one new course in Cryptography and Compression, but feel very constrained in their attempts to evolve their curriculum by their inability to convince the upper administration to let the IT program grow into new areas of specialization. This problem is compounded by the fact that there are five computing majors spread across three separate colleges. Having been unsuccessful in convincing the upper administration to allow them to hire new faculty the question for them becomes, “what can we confidently teach with the faculty that are currently on staff.” They bring more security content into their curriculum primarily through bringing in seminar speakers from outside the university with expertise in security issues

The second respondent came from a very different institution. At this institution they feel much more free to evolve their IT program in many different areas but are fearful of constructing artificial “picket fences” (like the engineering field is used to) around different areas of the curriculum when they see security as an essential part of many curricular issues. They see security as most closely allied with networking, but want to avoid developing a separate degree in security. They are also very intrigued by the importance of human factors in security and are in the process of developing a senior level course dealing with security policy and implementation issues.

The two separate respondents approached the inclusion of more security content in their curricula in very different ways largely based on their local circumstances.

## **CONCLUSIONS**

This study has attempted to gain a better understanding of the extent to which IT programs and the interest areas within them have changed to include a greater security component, and the means by which this has been accomplished. This has been accomplished by conceptualizing this issue as having both quantitative and qualitative dimensions and has used research methods appropriate for both dimensions of the issue. The results of this study include the following:

The most important result from this study is that enhancing the security education content within the IT curriculum is an important topic that people in the IT community are interested in. Although the topics to be included and the mechanics of inclusion vary from institution to institution, and across interest groups, security education is an important concept.

The different interest areas within the RIT IT program are all interested in increasing the amount of security content in their programs, but as of this writing only the Networking and System Administration group has developed new courses specifically related to security. The other interest areas have taken an approach that includes adding security content to existing courses either as formal lecture modules or as a subject that pervades one or several existing courses. The faculty are not entirely happy with this approach and consider this a work in progress.

Although the general methodology of this study was valid given the questions we sought to address it was implemented at the wrong time of the year (early summer) and this resulted in a very poor response rate.

## Appendix A: Survey E-Mail

Dear CITC3 attendee:

If you have already completed the form we are using to collect information for our CITC4 presentation please delete this and I am very sorry for the inconvenience. This is a new way of collecting survey data for us and Murphy's law seems to have come down rather hard on us.

As IT educators we have been asked to bring an increased awareness of information security into our classrooms and to help our students to gain a better awareness of the security implications of many of the things that they do. IT is not, however, a monolithic field, rather it is a discipline made up of several fairly well defined interest areas each of which have their own pedagogical concerns, and issues, only some of which are in the area of security. This study is designed to gain a better

understanding of the extent to which IT programs, and the interest areas within them, have changed to include a greater security component, and the means by which this has been accomplished (e.g. through the addition of new courses or the modification of existing courses). We plan to present the results of this study at CITC4 to be hosted by Purdue University in Lafayette, IN and hope to see you there.

As an attendee of CITC3 in Rochester, NY we would like you to take a few minutes to answer several questions about the role that information security plays in your curriculum and if and how you have adapted your program to enhance the security component.

We would like to follow the survey portion of this study up with a more in-depth discussion of some of the qualitative aspects of these issues with a select group of participants. If you are interested in participating in this portion of the study please so indicate at the bottom of this form. You will be contacted as close as possible to the date that you indicate by either Charles Border or Ed Holden. The entire interview will take less than twenty minutes.

Please go to the following link to complete our survey, the entire survey will only take about fifteen minutes to complete:  
<http://www.it.rit.edu/~cbb/seced1.htm>

Charles Border, Ph.D.  
Assistant Professor  
Golisano College of Computing and Information Sciences  
Department of Information Technology  
Rochester Institute of Technology  
102 Lomb Memorial Drive  
Office 70-2269  
Rochester, NY 14623-5608  
(585) 475-7946  
[cborder@it.rit.edu](mailto:cborder@it.rit.edu)

## Appendix B: Web Form

### Security Education Within the IT Curriculum

Thank you for participating in this study. We are hopeful that it will help all of us to gain a better understanding of how other programs are addressing this very important issue.

Your response to this form will be anonymous. Should you desire to submit an e-mail directly to the authors with greater detail or seeking further information, that would be great, we look forward to hearing from you. Once again, we would like to follow these questions up with a short telephone interview. If you would like to participate in the telephone portion of the study please let us know when and how to contact you at the end of the form. Please take your time answering these questions.

Thank you very much for taking the time to help us out. We look forward to seeing you at Purdue!

Sincerely,

Charles Border

Ed Holden

1. What is your personal area of specialization?

- Multimedia  Programming  Networking  Database  Human Computer Interface  
 Other:

2. How many students are currently enrolled in your institution?

- Less than 2,000  Between 2,000 and 8,000  Between 8,000 and 15,000  More than 15,000

3. How many students are currently enrolled in your IT curriculum?

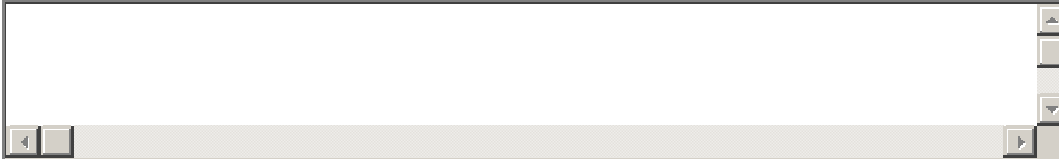
- Less than 100  Between 100 and 300  Between 300 and 600  More than 600

4. Do you offer specialization tracks within your undergraduate IT program?

- Yes  No If yes, what are they?

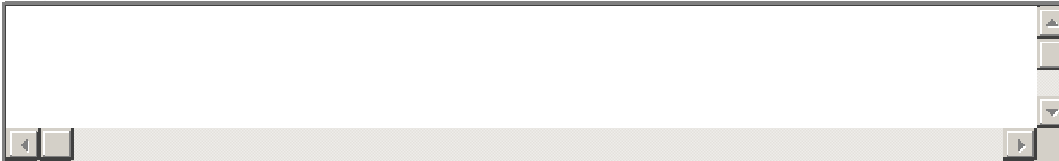
5. Has your perspective regarding the importance of a security component in the IT curriculum changed as a result of 9/11, if so how?

6. Have you implemented any changes to your curriculum designed to enhance your student's awareness of computer security since 9/11?

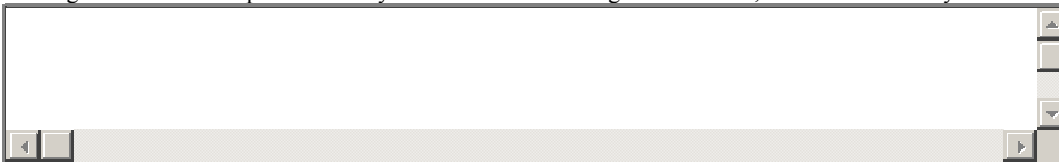


7. If yes, how did you enhance the security component of your curriculum? -Through the addition of new course/s?

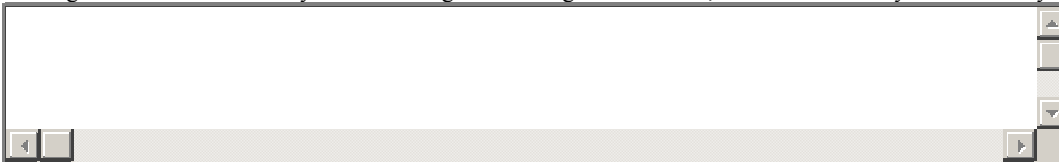
If so, what are the titles of the course/s?



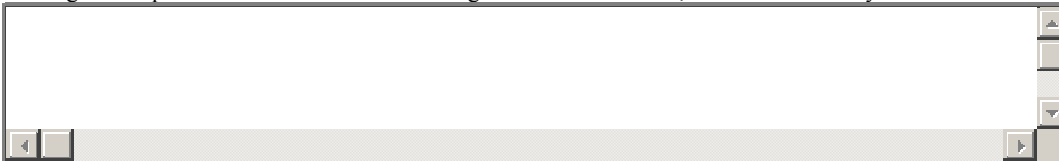
-Through the addition of specific security modules within existing courses? If so, What modules did you add to which courses?



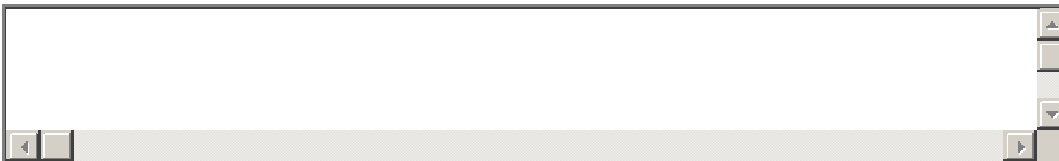
-Through the addition of security content throughout existing courses? If so, which courses did you add security content to?



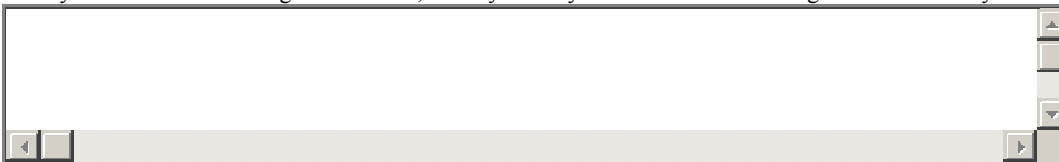
-Through a comprehensive reevaluation of existing course content? If so, which courses did you reevaluate to include more security content?



8. Do you see security awareness as being the purview of any one particular specialization within the IT curriculum, or does it belong to many or all specializations? If one, which one?



9. Do you feel that more changes are needed, or are you fairly comfortable with the degree and extent of your modifications?



10. If you modified your curriculum in any way to include more security content, how long did it take you between the inception of the idea for change and the implementation of the changes?

11. If you modified your curriculum to include more security content, do you see the enhancement of the security component of your curriculum as a work in progress, or a completed activity?

12. If you modified your curriculum to include more security content, did you receive any assistance or encouragement from your administration to facilitate your modifications?

We would very much like to follow up on your responses to these questions with a short phone interview regarding your perceptions of the qualitative issues brought up by the idea of bringing more security content into your IT curriculum. If you would like to participate in this portion of our study please indicate a phone number and the best dates and times for one of us to contact you. We will e-mail you with a date and time as close as possible to the time that you offer below and then call you at that time.

Thank you very much for participating in this study, we look forward to seeing you at CITC4 in Lafayette, IN.

I would like to participate in the qualitative portion of this study. Please contact me at the date and time listed below:

Name:  Institution:

Date or dates:  Best time or times to reach me:

Telephone number with area code: