

CyberSecurity Awareness @ Fordham University

Katherine Egan

New Jersey Institute of Technology

MSPTC Project Final Report

24 April 2007

Kse3@njit.edu

Table of Contents

Introduction.....	3
Site Description.....	5
<i>My Role</i>	5
Project Description.....	6
<i>Audiences</i>	6
<i>Purpose</i>	7
<i>Aims or Goals</i>	8
<i>Medium for Delivery</i>	8
Problem Description.....	8
<i>Solving the Problem</i>	9
Project Timeline.....	10
Literature review.....	11
Theory.....	13
Methodology.....	14
Lessons Learned.....	19
Conclusion.....	20
Works Cited.....	21
Appendix A – CyberSecurity Survey Results.....	23

Introduction

In September of 2003, Fordham University spent close to \$200,000 cleaning and updating computers due to the Blaster virus. This was an unforeseen event for which we could not have budgeted. But, to ensure network access for our students, faculty and staff, we had to find the money. We hired extra resources to work (ten-hour days) over Labor Day Weekend to assist in the clean-up as students moved into the residence halls. A month later, machines were still being cleaned, and we weren't alone. Considering the following chart from the Chronicle of Higher Education, Fordham was lucky.

WHAT ONE WORM COST				
During five weeks last summer, when the Blaster worm hit the Internet, colleges devoted hundreds of hours to fixing infected computers. Here are the costs reported by four universities during that period.				
	Number of computers infected	Percentage of computers infected	Hours spent to repair	Total cost
Stanford U.	6,000	30%	18,420	\$806,000
U. of Chicago	1,600	18%	9,000	\$377,000
U. of Colorado at Boulder	265	3%	465	\$9,000
U. of Michigan at Ann Arbor	2,600	7%	16,100	\$543,000
Source: Gregory A. Jackson, U. of Chicago				

Cyber-security is a global issue that industries as well as individuals must be concerned with if they are to survive in the technological age. Unfortunately, as technology grows and becomes more widespread so does the pool of would-be hackers who thrive on finding loopholes and exploiting weaknesses in software. Any organization or individual who uses the Internet or has an email address is a potential target for hackers, computer viruses, identity theft, phishing schemes and other kinds of electronic fraud.

And, the world of Academia has a rather unique perspective. “Providing secure information technology (IT) services to colleges and universities is a special challenge, given the public nature of higher education and an academic culture that values open access to information and the free flow of ideas” (Caruso 1). How do you balance the need for a secure computing environment with the ideal of academic freedom? How do you protect the confidentiality and integrity of institutional and individual data in an environment where the free exchange of ideas is paramount?

One answer is training and awareness. Many colleges and universities have developed programs for cyber security awareness, designed to education their respective communities on these critical issues. In fact, the EDUCAUSE Center for Applied Research found in its “2006 Study on Information Technology Security in Higher Education” that those institutions where IT security was part of the institutional employee culture had higher confidence in their IT security programs (11). In other words, if there was IT security awareness throughout the community – then the school had a better chance of keeping its institutional data secure.

Technology solutions alone won’t work. “Education and awareness of the individual, whether in the largest multinational corporation, small business or the home user, is critical. Security is more than just installing a piece of software, it is using best practices, updating your antivirus, and practicing safe and secure computing” (Wong 2).

To facilitate Cyber Security Awareness at Fordham University, I proposed to develop a website (initially delivered on a CD-Rom) to include information on a variety of electronic security topics. Only by making the Fordham community aware of electronic security issues can we ensure a safe and reliable computing environment, and, hopefully avoid unforeseen costs. It

is my hope that this is only the first step towards a comprehensive Cyber Security Awareness Program.

This document describes the project in detail and includes the following topics:

- Project site description: including Fordham University and my role
- Project Description: including audience(s), purpose, aims or goals, and medium for delivery
- Problem description and resolution
- Project Timeline
- Literature review
- Theory
- Methodology
- Lessons Learned
- Conclusion

Site Description

Fordham University, the Jesuit University of New York, is a mid-sized Doctoral/Research-extensive school, located on three campuses in the New York metropolitan area, (Rose Hill in the Bronx, Lincoln Center in Manhattan, and Marymount in Tarrytown, Westchester). Fordham is an independent, not-for-profit University, which enrolls approximately 16,000 students in 5 undergraduate colleges, 4 graduate and 2 professional schools, (approximately 8,500 graduate students and 7,500 undergraduates).

My Role

I work for the Vice President for Information Technology and CIO at Fordham, focusing on IT Strategy and Planning. My responsibilities include various forms of communications and

reports to the Fordham community, including Annual and Quarterly reports to the President and Board of Trustees. I am also responsible for writing and editing technical documentation and other media as well as maintaining fresh and relevant content for two major websites within www.fordham.edu.

Additionally, as of January 2007, I have been asked to assume the responsibilities of communications for the Fordham IT division. Among other things, this includes providing communication for all major technology projects and creating processes and procedures to improve IT communications with the University community.

As the content of this proposed project will eventually be incorporated into the Fordham IT website and this is within my area of responsibility, my role in this project was to develop the look and feel as well as the navigation for the deliverable. I also wrote, edited, and organized the content for presentation.

Project Description

The project described in this document is a comprehensive CD on the Topic of CyberSecurity Awareness @ Fordham. The CD is informational for the most part, including best practices, How To's, What To Do's, links to external resources, such as articles, other websites, videos, podcasts and an interactive 'password checker' where you can type in a password to verify how secure it is.

Audiences

The primary audience for the project – the CyberSecurity Awareness @ Fordham CD and eventual website – consists of the students, faculty and staff of Fordham University. Their needs include the CD/website content with useful and timely information such that they feel informed and aware of threats and preventative measures while online, to ensure safe computing, both at

Fordham and at home. Also in the primary audience category are the Academic Reviewers and Gatekeeper. Needs for this group include all relevant materials for the project, (i.e., the deliverable, this final report and presentation materials), displaying mastery of MSPTC core competencies.

An additional primary audience member is my external reviewer, Mr. Jason Benedict, Fordham University's new University Information Security Officer. In this role, Jason is responsible for the overall direction of information security functions relating to Fordham University, specifically: IT risk management, security policies, security awareness, and security architecture. We will be working closely over the next few months to develop an InfoSec website for Fordham, to include much of what has been developed in this project.

The secondary audience consists of the staff members in the Faculty Technology Centers (FTC) and Student Technology Centers (STC). They must be familiar with the content to be able to answer and anticipate potential questions in support of the Fordham community. Tertiary audiences include various technology groups who support both the FTCs and STCs as well as the community at large.

Purpose

The purpose of this project was to determine what electronic security information is most relevant to the Fordham Community and in what media the community would like this information presented. The ultimate purpose was to raise awareness about Cyber Security and the adverse consequences of its failures, in order to better prepare the University community to follow safe computing guidelines.

Aims or Goals

The overall goal for this project is a community at Fordham University that is aware of cyber-security risks and threats and that is proactive in securing our network, our institutional data and individual data. Making security a habit so that it becomes second nature to our community is essential to protecting the confidentiality, integrity, and availability of our institutional data, as well as our personal data.

Medium for Delivery

CyberSecurity Awareness @ Fordham was developed as a website and will eventually be incorporated into the Fordham University website. Initially, the delivery mechanism is a CD. The reasons for a different initial delivery mechanism were two-fold. First, a separate and distinct CD on Cyber-Security awareness highlights how critical this topic is in and of itself. Second, we are in the process of reorganizing, restructuring and redesigning the Fordham IT website and it would be somewhat complicated to incorporate an entirely new CyberSecurity section into the reorganization process.

Problem Description

The problem to be resolved by a CyberSecurity Awareness website is essentially a lack of awareness regarding electronic (or cyber) security. Since the Blaster virus incident in 2003, Fordham has undertaken some measures to ensure a secure and reliable network. For example, in the Residence Halls and on the wireless network, the University instituted a security protocol whereby computers attempting to access the network are scanned to verify that they are up-to-date with operating system patches and anti-virus signatures. Only computers who are certified in this manner may access the University network. Unfortunately, lack of awareness and understanding about why we undertook these measures and the intended purpose, left many

community members frustrated. It seems that many computers had never been updated with operating system patches. One can imagine that it took sometimes hours for computers to be updated.

Solving the Problem

The above is just one example of the University's need for an awareness program in the realm of electronic security. Fordham's current website lacks a cohesive and comprehensive set of information about this topic. This CyberSecurity Awareness CD is the first step towards promoting awareness throughout the University which will aid in keeping our institutional data secure.

Topics include:

- Safe Computing (essentials, preventative measures)
 - Including general online safety tips, appropriate password setting, firewalls, getting Operating System Updates, Anti-virus protection, etc.
- Threats
 - Including spam, phishing, pharming, viruses, worms, spyware, and identity theft.
- IT Policies
 - Anti-spam, E-mail, Mass Mailings, Peer-to-Peer, Web Hosting and Wireless.
- Fordham's Network
 - Including the specifics required for access, (installed and up-to-date Anti-Virus protection and up-to-date operating system patches), and Fordham approved anti-virus software options.

- Resources
 - Including articles, podcasts, external websites, flyers, etc.

Project Timeline

Table 1 below presents the timeline and associated tasks for this project.

ID	Task Name	Duration	Start	Finish	Mar '07					Apr '07				May '07				
					2/25	3/4	3/11	3/18	3/25	4/1	4/8	4/15	4/22	4/29	5/6			
1	Begin Project	5 days	Mon 3/5/07	Fri 3/9/07														
2	Peer & Aspirant research	5 days	Mon 3/5/07	Fri 3/9/07														
3	Survey	22 days	Thu 3/8/07	Thu 3/29/07														
4	Identify Survey Participants	2 days	Mon 3/12/07	Tue 3/13/07														
5	Develop survey	2 days	Thu 3/8/07	Fri 3/9/07														
6	Deliver survey	1 day	Mon 3/19/07	Mon 3/19/07														
7	Collect Data & rank interest	10 days	Tue 3/20/07	Thu 3/29/07														
8	Podcasts	12 days	Mon 4/16/07	Fri 4/27/07														
9	Coordinate development & production	12 days	Mon 4/16/07	Fri 4/27/07														
10	CD / Website	55 days?	Tue 3/6/07	Sun 4/29/07														
11	Design & Develop website template	4 days	Tue 3/6/07	Fri 3/9/07														
12	Develop website content	20 days	Thu 3/8/07	Tue 3/27/07														
13	Present website for Prelim review	1 day?	Mon 4/2/07	Mon 4/2/07														
14	Revise website	22 days	Fri 4/6/07	Fri 4/27/07														
15	Add podcasts to CD/website	2 days	Sat 4/28/07	Sun 4/29/07														
16	Deliverables	23 days?	Tue 4/10/07	Wed 5/2/07														
17	Develop prototype CD	1 day?	Mon 4/30/07	Mon 4/30/07														
18	Develop Ppt for presentation	6 days	Sun 4/22/07	Fri 4/27/07														
19	Develop Final Report	15 days	Tue 4/10/07	Tue 4/24/07														
20	Develop project materials (package)	3 days	Mon 4/30/07	Wed 5/2/07														
21	Present Project	0 days	Wed 5/2/07	Wed 5/2/07														

Table 1 – Project Timeline

Details of timeline:

1. Performed Grounded Theory research to identify core categories of electronic security.
2. Identified participants for survey, got names and email addresses.
3. Developed and refined questions, created and delivered survey.
4. Collected data as responses were received. Identified the topics of highest interest to survey respondents.
5. Collaborated on and coordinated podcast development and production for 2 of the highest interest topics.
6. Designed and developed the website look & feel (template), and navigation.

7. Developed and refined content for website.
8. Presented website to University Information Security Officer.
9. Revised website based on feedback.
10. Developed CD cover for prototype.
11. Developed Powerpoint slides for presentation.
12. Developed final report.
13. Developed project materials, (package for program requirements).
14. Presented project.

Literature review

A literature review did not yield much in the area of electronic security awareness or in building components of a CyberSecurity Awareness program. However, it did find some interesting and relevant articles. For example, an article in the January 2007 issue of Communication News states that online fraud is steadily increasing and becoming more sophisticated. In fact, “Symantec has observed more than seven million total phishing attempts each day” in 2006 (PHISHING 6).

Business Communications Review from May 2005 included an article by Arthur Wong, a vice president at Symantec, Corporation. He agrees that security threats from the Internet are becoming more sophisticated and more aggressive. Wong also asserts that “we are starting to see the use of viruses and worms to attack newer applications, such as instant messaging and peer-to-peer networking” (Wong 1). This is critical to know as more students arrive on campus each year with increasing numbers of technological devices, which include these types of applications.

An article in the American Marketing Association, by Keith B. Anderson, quoted John W. Snow, (United States Secretary of the Treasury 2003 – 2006), “The greatest threat to

consumers today is the growing menace of identity theft. Identity theft is far more insidious and harmful to our national welfare than many realize. It attacks the trust and confidence that nurture our open economy, even as it destroys individual lives” (160). Snow was an advocate for the accuracy and security of individuals’ financial information. He spoke on behalf of United States citizens and proposed programs to improve national standards while holding this post.

Even something as simple and seemingly innocuous as a CVS loyalty card can be compromised. “The 50-million-strong Extra-Care program, the nation's largest retail-loyalty-card operation, has a potential security hole that allows anyone with a member's card number, zip code and last name to obtain via e-mail a potentially embarrassing and invasive list of that person's over-the-counter drug and family-planning purchases” (Neff 1). This was proven when a privacy advocate, Katherine Albrecht performed a test for Advertising Age in which she was given an account number of a reporter. She was able to obtain a list of the reporters’ purchases – with only a last name, the card number and a zip code.

An interesting article found in Business Communications Review noted that some consumers have actually gone as far as to move their financial accounts to a different bank to avoid the threat of identity theft. “As consumers become more aware of the risks posed by identity theft, almost 6 percent have switched banks to avoid the problem,” according to a survey performed by Financial Insights, a research and advisory firm (Some Switch 1).

Additionally, the “EDUCAUSE Core Data Service Fiscal Year 2005 Summary Report” shows that all colleges and university respondents indicate increased network security measures. In fact, “fewer than 1% of ALL respondents have no firewalls” (EDUCAUSE 45). And, almost 100% of respondents have both anti-spam and anti-virus tools.

Although I found nothing specific to CyberSecurity Awareness per se, these articles uncovered the most prominent electronic security core categories and validated the topics I had in mind for the project.

Theory

The relevant theory for discussion here is hypertext theory, which George P. Landow, Professor of English and Art History, Brown University defines as “the convergence of contemporary critical theory and technology” (Landow 1). How does the integration of critical theory and technology present itself? How does this impact the ways in which people communicate?

The term hypertext was coined by Theodor H. Nelson, who explains it as “non-sequential writing -- text that branches and allows choices to the reader, best read at an interactive screen” (Landow). Unlike reading a book, in which the reader turns page by page in sequence, hypertext allows the reader to click a link to jump to a different part of the text. The link may be sequential, it may be chronological, it may appear alphabetical, and it may even be random. In effect, the reader is taking part in the writing of the text as she clicks each new link. Raley describes it thus, “the reader is in charge of ordering the information in front of her on the screen in a manner quantitatively and qualitatively distinct from the page and in a manner that constitutes authorship in its own right” (3). Each reading experience is different. This requires different skills than reading a traditional book. It also requires additional skills to write in this new medium.

All of which leads to a new concept, one of Information and Communication Literacy, which might be considered as essential today as the traditional version of ‘literacy’ was considered many years ago. *The Report of the 21st Century Literacy Summit* defines this updated literacy as “the set of abilities and skills where aural, visual and digital literacy overlap. These

include the ability to understand the power of images and sounds, to recognize and use that power, to manipulate and transform digital media, to distribute them pervasively, and to easily adapt them to new forms” (New Media 2).

One might consider this new form of literacy to be essential in order to survive in this new world of global networks. We can communicate today, almost instantly, with anyone anywhere in the world via e-mail, instant messaging and social networking on the Internet. These media are becoming more and more visual and aural and less text-based. And the bad citizens of the world are becoming more and more creative in the ways they go about their fraudulent activities.

It is my opinion that CyberSecurity awareness is part and parcel of this new form of literacy. It requires citizens to be aware, for example, of how they interact on the Internet, of where and when and how they supply personal information, of understanding how to spot the differences between legitimate websites and fraudulent ones, which at a glance may appear very similar, and of how they secure their work environment. Institutes of Higher Education are unique in the sense that they often must secure more information in terms of breadth than other types of institutions. For example, a financial institution might house personal (biographic and demographic) information as well as financial information for their customers. A university houses personal, academic, health and financial information about its students, personal and financial information about its employees, and personal and financial information about parents of applicants (who may never attend the school), enrolled students and alumni.

Methodology

Research was conducted in three phases via two different methodologies. The literature review served as the initial phase, in which I combined previous knowledge and experience with

results from the literature review. In this phase I began the continual cycle of data collection, note-taking and coding of Grounded Theory. The literature review phase uncovered the most relevant cyber security topics, which were coded into 13 categories and then used in the following phases of my research.

The second phase continued and validated my grounded theory approach. I used the topics uncovered in the literature review as search-terms and attempted to find them on the websites of Fordham's peer and aspirant schools. By researching peer and aspirant schools, we become cognizant of past experience and best practices in the realm of CyberSecurity awareness – specifically for Institutes of Higher Education. Using the Grounded Theory methodology I was able to refine my coding and develop core categories, which were then used in phase three of my research.

Fordham's peer schools are Boston University, George Washington University, Santa Clara University, Villanova University and Syracuse University, and the aspirant schools are Boston College, Georgetown University, Columbia University, New York University and Notre Dame. Most of the ten schools had a variety of information regarding these topics.

In my initial research attempt, I scored a zero if I did not find a topic and 1 if I did. After completing my search of the 13 categories for all ten schools, I realized that it might be useful to be more granular in my scoring methodology. I then decided to review all ten schools' websites again and score them as follows:

0. if I could not find information on the topic
1. if the topic was mentioned but did not have a page specifically dedicated to the topic
2. if the topic had a dedicated page, but I had to search for it [i.e., I could not navigate to the page]

3. if the topic was present on its own page and was easy to navigate to

My results shown in Figure 1, indicate that other than a General PC Protection section and Policies, which all schools had, the topics of Anti-Virus, Passwords and Spam seemed the most popular. Interestingly, these were almost identical to my first website search using a simple one and zero), except in that first search, Spyware came out as one of the top five instead of Passwords.

Topics	Aspirant Schools					Peer Schools					Total#
	Boston College	Georgetown University	Columbia University	Notre Dame	New York University	Boston University	George Washington University	Santa Clara University	Villanova University	Syracuse	
General PC protection/ Security / Safe Computing	3	3	3	3	3	1	3	3	3	3	28
Anti-Virus	3	3	3	1	3	3	3	1	1	2	23
Phishing	1	3	3	0	1	3	3	0	1	1	16
Spyware	3	3	3	3	1	3	1	0	1	1	19
Worms	0	3	0	0	1	0	1	0	1	1	7
Getting OS updates	3	1	3	0	1	1	1	1	1	1	13
Identity Theft	2	3	1	3	1	3	1	0	0	0	14
File sharing - Peer-to-Peer	2	0	3	0	1	0	1	0	1	1	9
Passwords	3	3	3	3	3	1	3	0	0	3	22
Policies	3	3	3	3	3	1	3	3	3	3	28
Firewalls	1	3	3	2	1	1	3	1	1	0	16
Backing up Data	2	1	3	2	1	0	0	1	1	1	12
Spam	2	3	3	3	1	3	3	1	1	2	22

Figure 1 - Peer & Aspirant Research Results

The third phase of my research took the form of a structured interview. Bernard defines structured interviewing as “people responding to a set of nearly identical stimuli” (191). The stimuli in this case were survey questions. Thirty-five students were chosen to participate in this survey, which was launched just after students returned from Spring Break. These students were selected specifically because they have been employed in the past by Fordham IT to assist residents with technology issues during move-in weekend in the fall semester. These students are unofficial technology advisors among their peers.

For the survey, I developed three questions, each of which was presented in a five-point Likert scale. The first question was not necessary for my research purposes per se, but was included for my own curiosity and as a warm-up for the students. The second question asked

students to identify their level of interest or concern for each of the 12 core categories of CyberSecurity. I eliminated the lowest-scored category (worms) from the selection as this topic is typically found in combination with viruses. The third question asked students to identify their interest level for a variety of delivery mechanisms for technology-related information.

Each question was scored in a similar manner, by taking the number of respondents for each core category and multiplying by the number corresponding to their interest level (i.e., 1 through 5). Each item was analyzed separately and then summed to a get total score. The item total scores were then ranked to identify: 1) which CyberSecurity topics (i.e., core categories) students have the most expertise or knowledge in, 2) which CyberSecurity topics are of highest interest or concern to the student survey participants, and 3) preferred delivery mechanisms for technology-related information.

Analysis of results for the question regarding level of interest or concern indicates the topics of General PC Protection, Identity Theft, Anti-Virus, and Backing up your data scored the highest, with Firewalls and Getting OS Updates tying for 5th place (see Appendix A – **CyberSecurity Survey Results** on page 23). This is somewhat contradictory to my grounded theory research results. In fact, there are only two topics that came out in the top 5 – in both research methods – General PC protection and Anti-Virus. This caused a slight dilemma. When it came time to select the topics for the proposed podcasts, which results are the most relevant? The highest-scoring topics from the website review of Fordham’s peer and aspirant schools? Or the topics indicated by students as the most concerning? I felt it better to lean toward the student interests rather than the CyberSecurity topics published on the websites of Fordham’s Peer and Aspirant schools, as I cannot be sure how other schools selected these topics.

Analysis of results for the question regarding level of interest in delivery mechanism indicates that Website, USB Flash Drive, CD-Rom and podcast scored the highest, in that order. Given that USB Flash Drives are not feasible at this time, I focused on the other three. The information was developed as a website for initial delivery on CD-Rom, and includes two podcasts, which were selected based on the scores of student-indicated interest or concern.

The highest scored topic was General PC Protection/Safe Computing. A podcast was not created for this topic, as it is the general subject area of the entire website and two videos were included covering this general topic.

Other high-scoring categories were Identity Theft, Anti-Virus, and Backing Up Your Data, in that order, with Firewalls and Getting OS Updates tied for 5th place. Since Backing Up Your Data and Getting OS Updates were two of the three highest scored categories for the question regarding student level of knowledge or expertise, these were not chosen either. Two podcasts were created, one for Anti-Virus (developed and recorded by Gerard Cariffe, Ph.D., Executive Director of Enterprise Technology Services, Fordham University) and one for Firewalls (developed and recorded by Mark McNeil, Director of Network Engineering and Operations, Fordham University). Since Identity Theft is such a broad and important topic, it was decided to include links to a variety of Identity Theft related podcasts rather than creating a new one. After a brief search through many sites, I found the following three podcasts – specifically relating to University Identity Security on Podcast.Net. These are perfect for inclusion in a CyberSecurity Awareness website for a mid-sized University of approximately 16,000 students and 5,000 faculty and staff members.

7. University Identity Security- Part 3 Rebroadcast 
 Part Three of three parts exploring Identity Security at our Nation's™ Universities. File Download (16:40 min / 7.7 MB)
 Podcast Date: Sep 15, 2006 20:34:00

8. University Identity Security- Part 2 Rebroadcast 
 University of Idaho, and University of Alabama, Birmingham representatives posted sensitive information online about their students in excel files. Join Aaron Titus to review these case studies, and I...

9. University Identity Security- Part 1 Rebroadcast 
 Universities maintain very private records about students'™ finances, health records, location, SSN, and other personal data, often for decades after the students attend. Yet every week, about 60,000...

Podcast Date: Aug 15, 2006 20:07:00

Figure 2 –University Identity Security Podcasts

The CyberSecurity Awareness website also includes three short videos, the first on Superhighway Safety, the second on the topic of backing up your data and the third on general computer security. These videos represent winning entries in the Security Awareness Video Contest sponsored by the EDUCAUSE/Internet2 Computer and Network Security Task Force and the National Cyber Security Alliance. During the summer months I will transfer this CyberSecurity information to either the Fordham IT website or to the new InfoSec website.

Lessons Learned

Communicate early and often. This is something already known, but the experience of developing the CyberSecurity Awareness website reinforced this concept. I learned to talk to everyone and anyone who might have expertise, ideas or merely suggestions on the topic of CyberSecurity. As a result I found new ways to present the information and I was introduced to resources I never would have found on my own.

Research can be fun. Initially I was nervous about the research part of this process, however once I began my interest grew. I actually had fun developing two different research strategies and then analyzing and comparing the results of the two approaches.

Learn to leverage. Use one thing for more than one purpose. I was fortunate that Fordham IT was evaluating new survey software right around the same time I needed to develop and launch a survey. The software fit my needs as well as the needs of the division. Additionally, the content I developed for this CyberSecurity Awareness website will be used to seed the University's larger InfoSec website.

You don't need to recreate the wheel. There are resources available that might fit your needs perfectly. I was unable to have a video created in the timeframe of this semester, however I found award winning videos available for educational noncommercial use provided that they are identified and credited appropriately – that fit my topic perfectly.

Develop a project plan. Only by outlining all the necessary steps in your particular process will you be able to stay on track. By listing all the tasks I needed to complete, identifying the items that could overlap and be accomplished concurrently and those with required predecessors, I was able to schedule my time and stick to the plan. Had I not identified the tasks that had to be completed in sequence I could would not have been able to remain on schedule.

Have fun. Do something that holds your interest and that you have some passion for. If you truly enjoy what you are doing your end product will all that much better.

Conclusion

“IT security will remain a problem that can't be solved, only managed. IT executives are not optimistic that security risks will go away, and only one in ten believes technology can solve IT security problems. Instead, most envision a future where identity theft and virus attacks will just get worse” (Alter 2). This is disturbing information and it is my hope that an electronic security awareness program is a step in the right direction towards protecting Fordham University community members as well as our institutional data.

Works Cited

- “A Global Imperative, The Report of the 21st Century Literacy Summit” The New Media Consortium. 2005. 09 November 2006.
- Alter, Allen E. “The Future of I.T.: What’s on Tap for 2007.” CIO Insight. 16 Jan. 2007. Ziff Davis Media, Inc. <http://www.cioinsight.com/print_article2/0,1217,a=198697,00.asp>
- Anderson, Keith B. "Who Are the Victims of Identity Theft? The Effect of Demographics." Journal of Public Policy & Marketing 25.2 (2006): 160-171. Communication & Mass Media Complete. 8 February 2007. <<http://search.ebscohost.com>>
- “EDUCAUSE Core Data Service Fiscal Year 2005 Summary Report.” EDUCAUSE Core Data Service (2007) EDUCAUSE 8 February 2007.
<<http://www.educause.edu/apps/coredata/reports/2005/>>
- Foster, Andrea L. “Colleges Brace for the Next Worm.” The Chronicle of Higher Education. 50.28 March 2004. A29. <<http://chronicle.com/weekly/v50/i28/28a02901.htm>>
- Howard, Philip N., Steve Jones, ed. Society Online: The Internet in Context. Thousand Oaks: Sage, 2004.
- Landow, George P. “The Definition of Hypertext and Its History as a Concept.” 01 Mar. 2007. <<http://scholars.nus.edu.sg/cpace/ht/jhup/history.html#1>>
- Neff, Jack. “Is your CVS loyalty card a privacy threat?” Advertising Age 76.25 (2005): 3-36. Communication & Mass Media Complete. 8 February 2007.
<<http://search.ebscohost.com>>
- “PHISHING IS CATCHING ON.” Communications News 44.1 (2007): 6-6. Communication & Mass Media Complete. 8 February 2007. <<http://search.ebscohost.com>>

Raley, Rita. "Reveal Codes: Hypertext and Performance" Postmodern Culture. 12.1 Sep. 2001.

<http://muse.jhu.edu/journals/postmodern_culture/v012/12.1ralely.html>

"Some Switch Banks To Avoid ID Theft." Business Communications Review 35.5 (2005): 6-6.

Communication & Mass Media Complete. 8 February 2007.

<<http://search.ebscohost.com>.>

"The Privacy Podcast." Podcast Networks. 2006. 23 Apr. 2007.

<<http://www.podcast.net/show/15618>>

Wong, Arthur. "Prescription for protection." Communications News 41.1 (2004): 7-8.

Communication & Mass Media Complete. 8 February 2007.

<<http://search.ebscohost.com>.>

Appendix A – CyberSecurity Survey Results

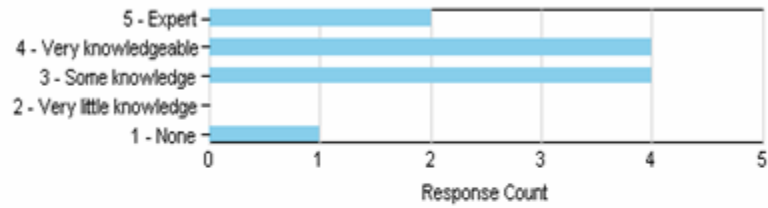
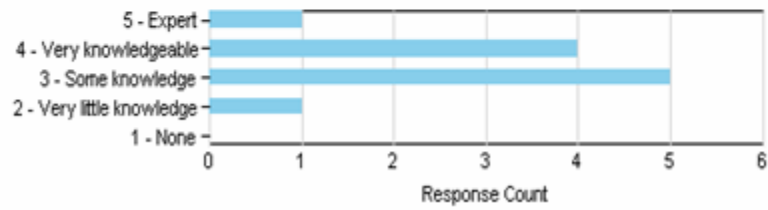
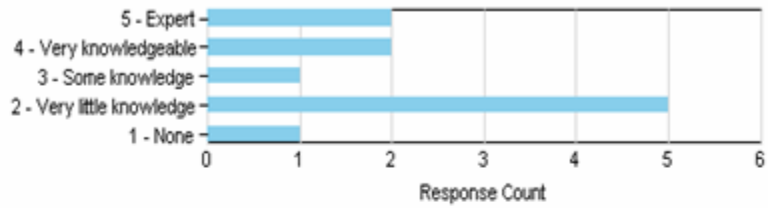
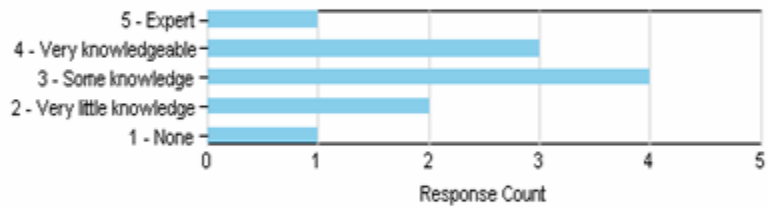
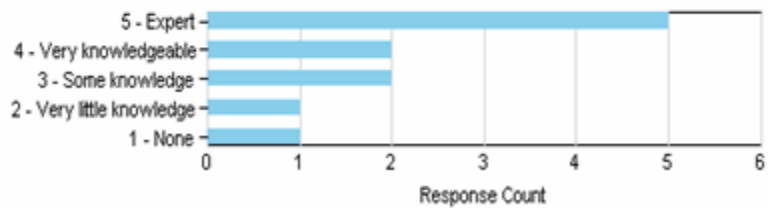
Question 1 Responses

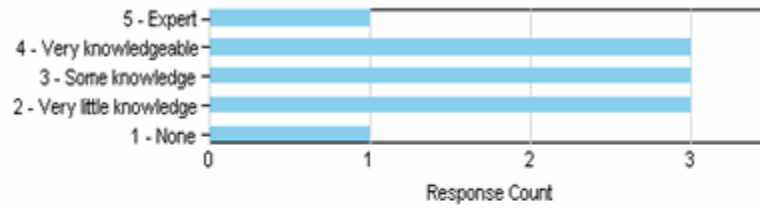
1. Please indicate your level of knowledge or experience for each of the following topics:						
	1 - None	2 - Very little knowledge	3 - Some knowledge	4 - Very knowledgeable	5 - Expert	Response Total
General PC protection	9.1% (1)	0.0% (0)	36.4% (4)	36.4% (4)	18.2% (2)	11
Anti-Virus	0.0% (0)	9.1% (1)	45.5% (5)	36.4% (4)	9.1% (1)	11
Phishing	9.1% (1)	45.5% (5)	9.1% (1)	18.2% (2)	18.2% (2)	11
Spyware	9.1% (1)	18.2% (2)	36.4% (4)	27.3% (3)	9.1% (1)	11
Getting OS Updates	9.1% (1)	9.1% (1)	18.2% (2)	18.2% (2)	45.5% (5)	11
Identity Theft	9.1% (1)	27.3% (3)	27.3% (3)	27.3% (3)	9.1% (1)	11
Peer-to-Peer file sharing	9.1% (1)	9.1% (1)	36.4% (4)	18.2% (2)	27.3% (3)	11
Password Setting	9.1% (1)	0.0% (0)	18.2% (2)	36.4% (4)	36.4% (4)	11
Policies	18.2% (2)	9.1% (1)	45.5% (5)	9.1% (1)	18.2% (2)	11
Firewalls	0.0% (0)	18.2% (2)	27.3% (3)	27.3% (3)	27.3% (3)	11
Backing up your data	0.0% (0)	0.0% (0)	36.4% (4)	36.4% (4)	27.3% (3)	11
Spam	9.1% (1)	18.2% (2)	18.2% (2)	36.4% (4)	18.2% (2)	11
Totals:	10	18	39	36	29	

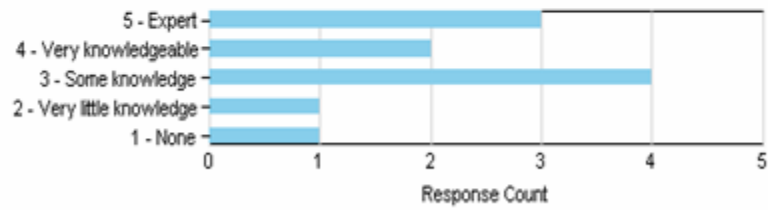
Question 1 Scores

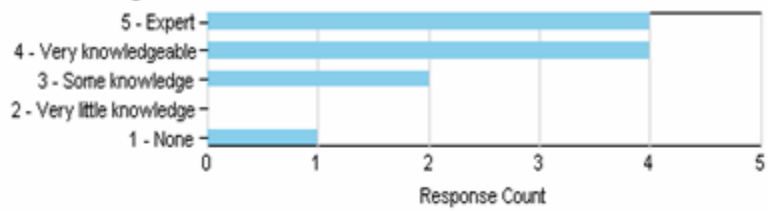
Scores for Question 1:						
	1 - None	2 - Very little knowledge	3 - Some knowledge	4 - Very knowledgeable	5 - Expert	Score Total
General PC protection	1	0	12	16	10	39
Anti-Virus	0	2	15	16	5	38
Phishing	1	10	3	8	10	32
Spyware	1	4	12	12	5	34
Getting OS Updates	1	2	6	8	25	42
Identity Theft	1	6	9	12	5	33
Peer-to-Peer file sharing	1	2	12	8	15	38
Password Setting	1	0	6	16	20	43
Policies	2	2	15	4	10	33
Firewalls	0	4	9	12	15	40
Backing up your data	0	0	12	16	15	43
Spam	1	4	6	16	10	37

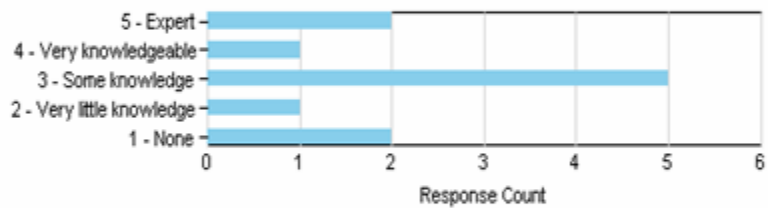
Question 1 Details

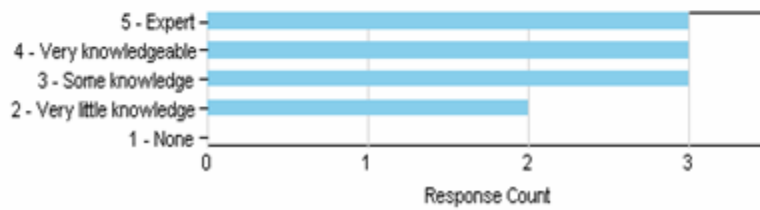
General PC protection**Anti-Virus****Phishing****Spyware****Getting OS Updates**

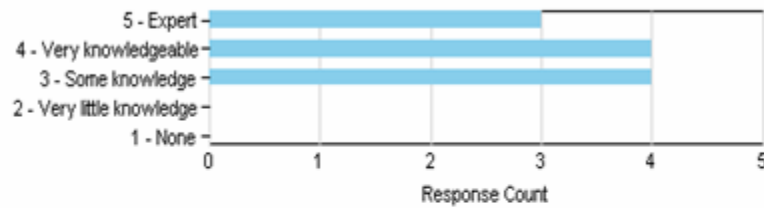
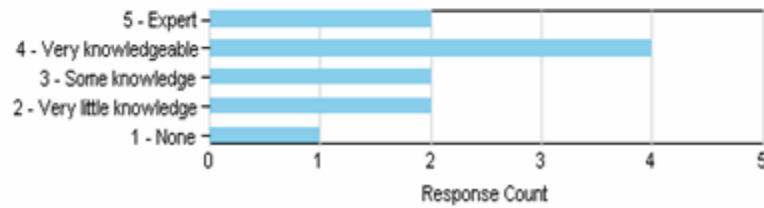
Identity Theft

Peer-to-Peer file sharing

Password Setting

Policies

Firewalls

Backing up your data**Spam***Question 2 Responses*

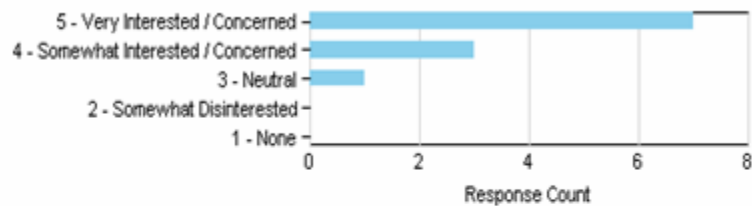
2. Please indicate your level of interest or concern for each of the following topics:						
	1 - None	2 - Somewhat Disinterested	3 - Neutral	4 - Somewhat Interested / Concerned	5 - Very Interested / Concerned	Response Total
General PC protection	0.0% (0)	0.0% (0)	9.1% (1)	27.3% (3)	63.6% (7)	11
Anti-Virus	0.0% (0)	0.0% (0)	18.2% (2)	36.4% (4)	45.5% (5)	11
Phishing	0.0% (0)	18.2% (2)	27.3% (3)	36.4% (4)	18.2% (2)	11
Spyware	0.0% (0)	9.1% (1)	18.2% (2)	36.4% (4)	36.4% (4)	11
Getting OS Updates	0.0% (0)	9.1% (1)	9.1% (1)	45.5% (5)	36.4% (4)	11
Identity Theft	0.0% (0)	9.1% (1)	0.0% (0)	36.4% (4)	54.5% (6)	11
Peer-to-peer file sharing	0.0% (0)	9.1% (1)	18.2% (2)	45.5% (5)	27.3% (3)	11
Password Setting	0.0% (0)	9.1% (1)	45.5% (5)	27.3% (3)	18.2% (2)	11
Policies	9.1% (1)	9.1% (1)	45.5% (5)	18.2% (2)	18.2% (2)	11
Firewalls	0.0% (0)	9.1% (1)	18.2% (2)	27.3% (3)	45.5% (5)	11
Backing up your data	0.0% (0)	9.1% (1)	0.0% (0)	45.5% (5)	45.5% (5)	11
Spam	0.0% (0)	9.1% (1)	18.2% (2)	63.6% (7)	9.1% (1)	11
Totals:	1	11	25	49	46	

Question 2 Scores

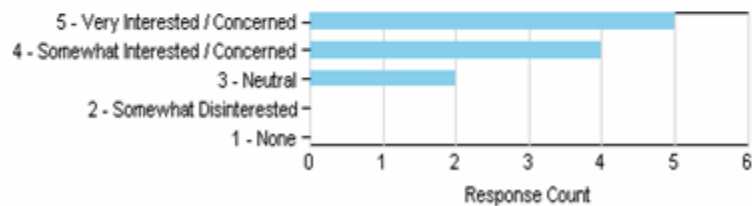
Scores for Question 2:						
	1 - None	2 - Somewhat Disinterested	3 - Neutral	4 - Somewhat Interested / Concerned	5 - Very Interested / Concerned	Score Total
General PC protection	0	0	3	12	35	50
Anti-Virus	0	0	6	16	25	47
Phishing	0	4	9	16	10	39
Spyware	0	2	6	16	20	44
Getting OS Updates	0	2	3	20	20	45
Identity Theft	0	2	0	16	30	48
Peer-to-Peer file sharing	0	2	6	20	15	43
Password Setting	0	2	15	12	10	39
Policies	1	2	15	8	10	36
Firewalls	0	2	6	12	25	45
Backing up your data	0	2	0	20	25	47
Spam	0	2	6	28	5	41

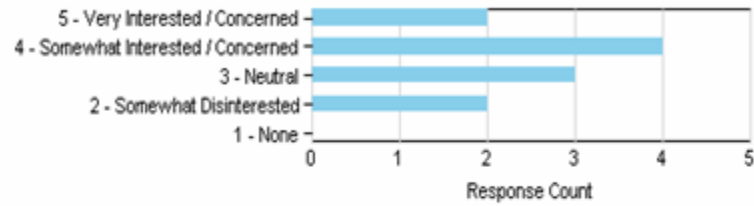
Question 2 Details

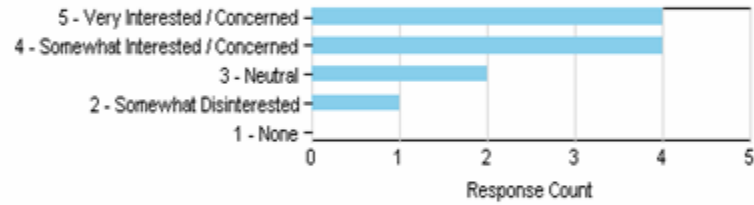
General PC protection

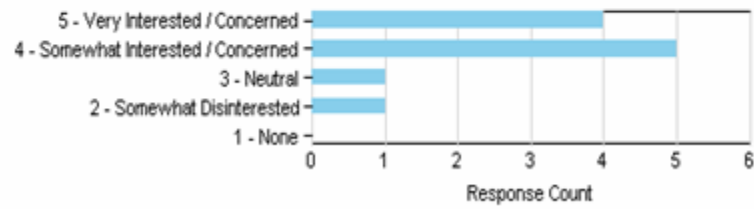


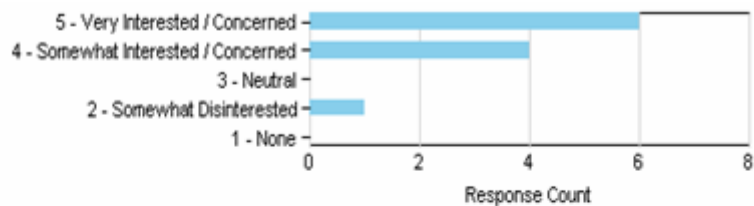
Anti-Virus

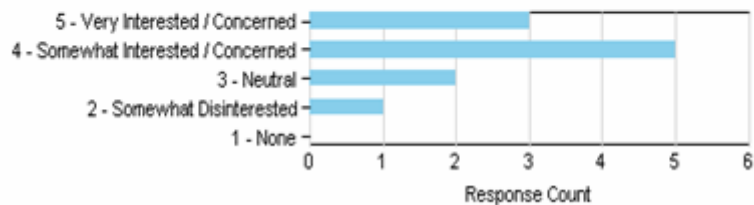


Phishing

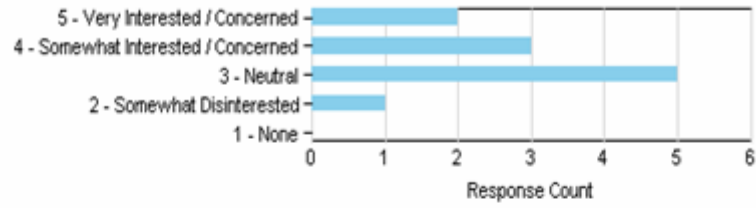
Spyware

Getting OS Updates

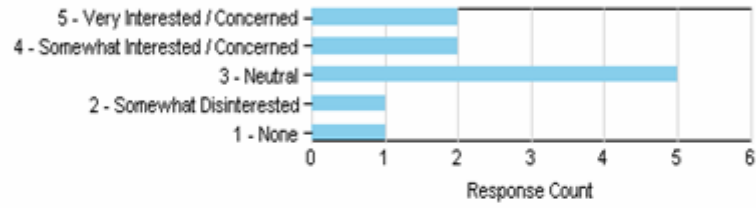
Identity Theft

Peer-to-peer file sharing

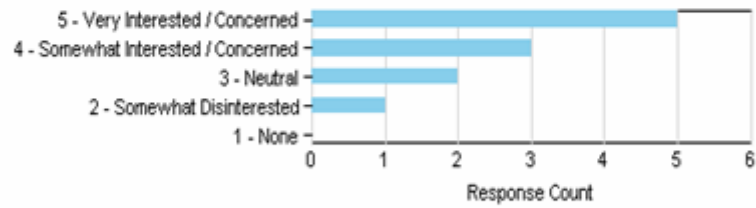
Password Setting



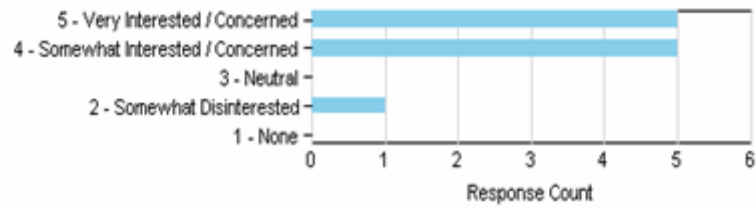
Policies



Firewalls



Backing up your data



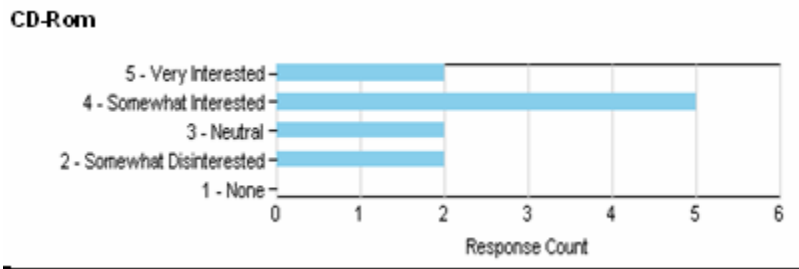
Question 3 Responses

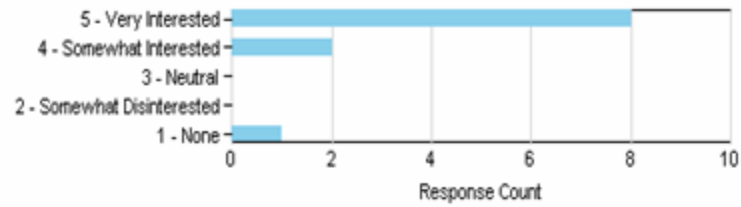
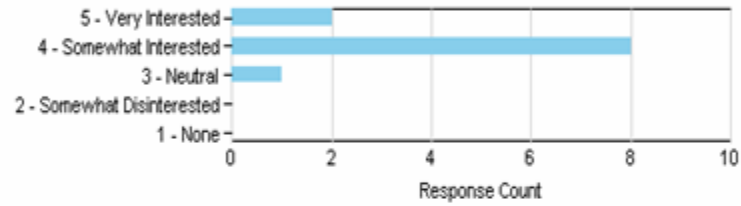
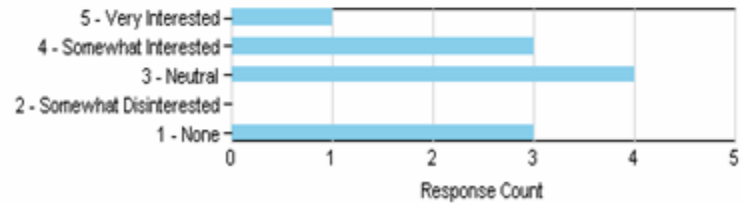
3. Please indicate your interest level for each of the following delivery mechanisms for technology related information:						
	1 - None	2 - Somewhat Disinterested	3 - Neutral	4 - Somewhat Interested	5 - Very Interested	Response Total
CD-Rom	0.0% (0)	18.2% (2)	18.2% (2)	45.5% (5)	18.2% (2)	11
Website	9.1% (1)	0.0% (0)	0.0% (0)	18.2% (2)	72.7% (8)	11
USB Flash Drive	0.0% (0)	0.0% (0)	9.1% (1)	72.7% (8)	18.2% (2)	11
Podcast	27.3% (3)	0.0% (0)	27.3% (3)	27.3% (3)	18.2% (2)	11
Vodcast	27.3% (3)	0.0% (0)	36.4% (4)	27.3% (3)	9.1% (1)	11
Podcast w/ Powerpoint Combined	27.3% (3)	9.1% (1)	18.2% (2)	36.4% (4)	9.1% (1)	11
Totals:	10	3	12	25	16	

Question 3 Scores

Scores for Question 3:						
	1 - None	2 - Somewhat Disinterested	3 - Neutral	4 - Somewhat Interested	5 - Very Interested	Score Total
CD-Rom	0	4	6	20	10	40
Website	1	0	0	8	40	49
USB Flash Drive	0	0	3	32	10	45
Podcast	3	0	9	12	10	34
Vodcast	3	0	12	12	5	32
Podcast w/ Powerpoint Combined	3	2	6	16	5	32

Question 3 Details



Website**USB Flash Drive****Podcast****Vodcast****Podcast w/ Powerpoint Combined**