

INFORMATION SYSTEMS EDUCATION JOURNAL

In this issue:

- 4. Where do Student Outcomes Begin? Developing Professional and Personal Management Skills as a Strategy for Student Success in the First Computing Course and Beyond**
Sean Humpherys, West Texas A&M University
Jeffrey Babb, West Texas A&M University
Amjad Abdullat, West Texas A&M University
- 27. The Information Systems Core: A Study from the Perspective of IS Core Curricula in the U.S.**
Drew Hwang, Cal Poly Pomona
Zhongming Ma, Cal Poly Pomona
Ming Wang, California State University, Los Angeles
- 35. A Project Management Approach to Applying Best Practices to Online CS/MIS Experiential Learning Projects**
Dana Schwieger, Southeast Missouri State University
Ken Surendran, Southeast Missouri State University
- 43. Assessing Cyberbullying in Higher Education**
Ali Kamali, Missouri Western University
- 54. A Match in the Making: How Emergent Changes in the Marketing Discipline Present Opportunities for Information Systems Programs**
Maureen Carley, Virginia Commonwealth University
Jeffrey Babb, West Texas A&M University
- 68. Adding Value: Online Student Engagement**
Donna R. Everett, Morehead State University
- 77. A Systems Analysis and Design Case Study for a Business Modeling Learning Experience for a Capstone CIS/IS Systems Development Class**
Jack Russell, Northwestern State University
Barbara Russell, Northwestern State University
- 97. A Model for Establishing a Cybersecurity Center of Excellence**
Edward, J. Moskal, Saint Peter's University
- 109. Course Redesign Based On the Quality Matters Program: Examples of Before and After**
Jennifer Kreie, New Mexico State University
Susan Bussmann, New Mexico State University

The **Information Systems Education Journal** (ISEDJ) is a double-blind peer-reviewed academic journal published by **EDSIG**, the Education Special Interest Group of AITP, the Association of Information Technology Professionals (Chicago, Illinois). Publishing frequency is six times per year. The first year of publication is 2003.

ISEDJ is published online (<http://isedj.org>). Our sister publication, the Proceedings of EDSIG (<http://www.edsigcon.org>) features all papers, panels, workshops, and presentations from the conference.

The journal acceptance review process involves a minimum of three double-blind peer reviews, where both the reviewer is not aware of the identities of the authors and the authors are not aware of the identities of the reviewers. The initial reviews happen before the conference. At that point papers are divided into award papers (top 15%), other journal papers (top 30%), unsettled papers, and non-journal papers. The unsettled papers are subjected to a second round of blind peer review to establish whether they will be accepted to the journal or not. Those papers that are deemed of sufficient quality are accepted for publication in the ISEDJ journal. Currently the target acceptance rate for the journal is under 40%.

Information Systems Education Journal is pleased to be listed in the 1st Edition of Cabell's Directory of Publishing Opportunities in Educational Technology and Library Science, in both the electronic and printed editions. Questions should be addressed to the editor at editor@isedj.org or the publisher at publisher@isedj.org.

2015 AITP Education Special Interest Group (EDSIG) Board of Directors

Scott Hunsinger
Appalachian State Univ
President

Jeffry Babb
West Texas A&M
Vice President

Wendy Ceccucci
Quinnipiac University
President – 2013-2014

Eric Breimer
Siena College
Director

Nita Brooks
Middle Tennessee State Univ
Director

Tom Janicki
U North Carolina Wilmington
Director

Muhammed Miah
Southern Univ New Orleans
Director

James Pomykalski
Susquehanna University
Director

Anthony Serapiglia
St. Vincent College
Director

Leslie J. Waguespack Jr
Bentley University
Director

Peter Wu
Robert Morris University
Director

Lee Freeman
Univ. of Michigan - Dearborn
JISE Editor

Copyright © 2015 by the Education Special Interest Group (EDSIG) of the Association of Information Technology Professionals (AITP). Permission to make digital or hard copies of all or part of this journal for personal or classroom use is granted without fee provided that the copies are not made or distributed for profit or commercial use. All copies must bear this notice and full citation. Permission from the Editor is required to post to servers, redistribute to lists, or utilize in a for-profit or commercial use. Permission requests should be sent to Nita Brooks, Editor, editor@isedj.org.

INFORMATION SYSTEMS EDUCATION JOURNAL

Editors

Nita Brooks
Senior Editor
Middle Tennessee State Univ

Thomas Janicki
Publisher
U of North Carolina Wilmington

Donald Colton
Emeritus Editor
Brigham Young University Hawaii

Jeffry Babb
Associate Editor
West Texas A&M University

Wendy Ceccucci
Associate Editor
Quinnipiac University

Melinda Korzaan
Associate Editor
Middle Tennessee State Univ

Guido Lang
Associate Editor
Quinnipiac University

George Nezek
Associate Editor
Univ of Wisconsin - Milwaukee

Samuel Sambasivam
Associate Editor
Azusa Pacific University

Anthony Serapiglia
Teaching Cases Co-Editor
St. Vincent College

Cameron Lawrence
Teaching Cases Co-Editor
The University of Montana

ISEDJ Editorial Board

Samuel Abraham
Siena Heights University

Mark Jones
Lock Haven University

Alan Pyslak
Penn State University

Teko Jan Bekkering
Northeastern State University

James Lawler
Pace University

Doncho Petkov
Eastern Connecticut State Univ

Ulku Clark
U of North Carolina Wilmington

Paul Leidig
Grand Valley State University

James Pomykalski
Susquehanna University

Jamie Cotler
Siena College

Michelle Louch
Duquesne University

Franklyn Prescod
Ryerson University

Jeffrey Cummings
U of North Carolina Wilmington

Cynthia Martincic
Saint Vincent College

Bruce Saulnier
Quinnipiac University

Christopher Davis
U of South Florida St Petersburg

Fortune Mhlanga
Lipscomb University

Li-Jen Shannon
Sam Houston State University

Gerald DeHondt

Muhammed Miah
Southern Univ at New Orleans

Karthikeyan Umapathy
University of North Florida

Audrey Griffin
Chowan University

Edward Moskal
Saint Peter's University

Leslie Waguespack
Bentley University

Janet Helwig
Dominican University

Monica Parzinger
St. Mary's University

Bruce White
Quinnipiac University

Scott Hunsinger
Appalachian State University

Peter Y. Wu
Robert Morris University

A Model for Establishing a Cybersecurity Center of Excellence

Edward J. Moskal
emoskal@saintpeters.edu
Computer & Information Sciences Department
Saint Peter's University
Jersey City, New Jersey 07306

Abstract

In order to effectively ensure our continued technical advantage and future cybersecurity, we need a technologically skilled and cyber savvy workforce and an effective pipeline of future employees. Our Government has identified Cybersecurity as one of the most serious economic and national security challenges we face as a nation and has ear-marked cybersecurity education as a major part of its Comprehensive National Cybersecurity Initiative. By establishing a Cybersecurity Center of Excellence as part of our Computer Science - Cybersecurity curriculum, Saint Peter's University will be well positioned to train and educate students on this very important National initiative. In addition, we will be providing our students with the skill-sets necessary to become a member of the cybersecurity workforce that is expected to increase from global revenues of \$95 billion in 2014 to \$155 billion in 2019.

Keywords: Cybersecurity, Center of Excellence, Security, Information Technology

1. INTRODUCTION

The need for information security has been increasing in all industry sectors, including energy, healthcare, financial services, manufacturing, transportation, and homeland security. Associated with this need for information security, is the demand for professionals with knowledge in the areas of computer security and information risk and assurance.

In February 2012, the Commerce Department's National Institute of Standards and Technology (NIST) established a National Cybersecurity Center of Excellence. According to NIST, the Center is to operate as a public - private collaboration for accelerating the widespread adoption of integrated cybersecurity tools and technologies (National Institute of Standards and Technology, 2014). The National Cybersecurity Center of Excellence (NCCoE), located in Rockville, Maryland, provides businesses with real-world cybersecurity

solutions, based on commercially available technologies. The center brings together experts from industry, government and academia to demonstrate integrated cybersecurity that is cost-effective, repeatable and scalable (National Cybersecurity Center of Excellence, 2014).

During the design of our Cybersecurity Center of Excellence Model, the NCCoE has been our advisor and has provided us with cybersecurity educational information. They have also introduced us to cybersecurity technology vendors and business partners. This advisor capacity role has played an important part in the design of our Cybersecurity Center of Excellence.

2. WHAT IS CYBERSECURITY?

Cybersecurity refers generally to the ability to control access to networked systems and the information they contain. Where cyber security controls are effective, cyberspace is considered a reliable, resilient, and trustworthy digital infrastructure. Where cyber security controls are

absent, incomplete, or poorly designed, cyberspace is considered the wild west of the digital age

(Bayuk, Healey, Rohmeyer, Sachs, Marcus, Schmidt, Weiss, 2013). Given the rapid global diffusion of Internet and social networking technologies, the degree to which societies around the world are increasingly linked is on the rise. With each new participant in the information age added to the network, the possibilities for threats and opportunities increase exponentially. Today, due to the Internet and the access it provides to file servers containing databases throughout the world, information has become available at virtually no cost to anyone who has a computer and Internet connectivity (Johnson, 2014).

3. CYBERCRIME COSTS & STATISTICS

According to an industry study by McAfee, cybercrimes cost the global economy up to US\$500 billion annually. The study also found that cybercrimes can potentially result in the loss of 500,000 jobs in the United States (McAfee, 2013). Ponemon Institute's 2013 Cost of Cyber Crime study finds the average company in the U.S. experiences more than 100 successful cyber-attacks each year at a cost of \$11.6M. That's an increase of 26% from 2012. The study also shows that companies who implement enabling security technologies reduced losses by nearly \$4M, and those employing good security governance practices reduced costs by an average of \$1.5M (Ponemon Institute, 2013). A study by Norton found that about 556 million adults are victims of cybercrime each year, which equates to 1.5 million victims per day and 18 victims per second (Norton, 2012). A good website that collects information on global cybersecurity attacks and reports statistics on the attacks is Hackmageddon.com. To illustrate, Figure 1 shows attacks based on country distribution, Figure 2 shows motivations behind attacks, and Figure 3 shows distribution of attack techniques. All illustrations are from the Hackmageddon.com (2013), web site and are for a snapshot in time, the month of August 2013. As illustrated in Figures 1-3, cyber-attacks are global. They are classified into 4 main areas of motivation: cybercrime, hacktivism, cyber warfare, and cyber espionage. Leading in the type of attack techniques that are known are DDoS with 17.8% and account hijacking with 16.8%. Out of all attack techniques, 24.3% are categorized as Unknown. Despite the estimated loss of money and information and known threats from adversaries, the precise impact of cybercrime is

unknown because it is not always detected and reported.

Figure 1

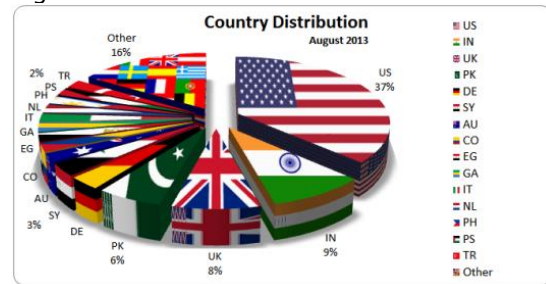


Figure 2

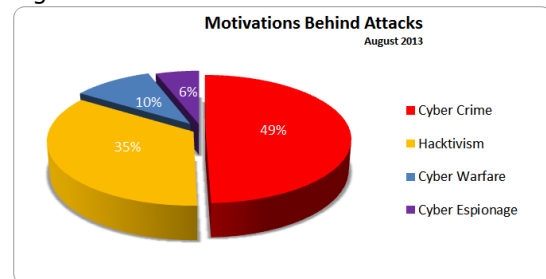
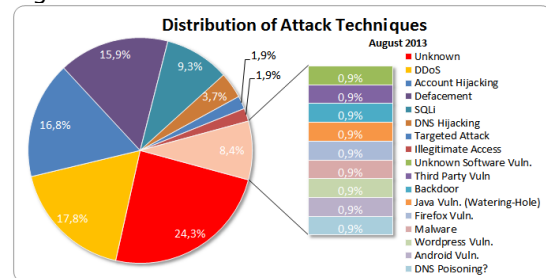


Figure 3



As a result of sophisticated technology and computers linked to information systems and databases, which are networked via lightning fast telecommunications links, we are in an era where the information revolution has changed the way organizations conduct business. Cyber-attacks continue to proliferate as vulnerabilities in computer systems and threats from hackers have increased every year. Malicious software threats, attacks, and botnets make front page news displaying the infamous success of hackers stealing data, crippling companies, and spying on corporations and governments.

Appropriate cybersecurity controls and tools need to be in place with a cybersecurity-savvy workforce that can combat the many risks and vulnerabilities faced in today's global society.

Our Government has identified Cybersecurity as one of the most serious economic and national security challenges we face as a nation. As a result, a Government project has been initiated to review the federal efforts to defend the United States information and communications infrastructure and the development of a comprehensive approach to secure America's digital infrastructure. One of the tenants of the comprehensive approach is to encourage institutions/organizations to provide education programs and training in Cybersecurity (The White House, 2014).

4. RESEARCH METHODOLOGY

During the 2013/2014 Academic Year, the Computer Science Department received approval to implement a new undergraduate concentration in Cybersecurity. Appendix A identifies the Cybersecurity curriculum concentration. We wanted to implement a Cybersecurity Center of Excellence as part of the curriculum to provide a value-added computing and learning environment for our students. Therefore, we conducted a study to determine what other United States colleges and universities were doing with Cybersecurity Labs in connection with their undergraduate and graduate Cybersecurity curriculums. The study would help us in designing the Model of our Cybersecurity COE. A total of 100 colleges and universities were studied. The schools that were part of the study were identified from literature searches on the Internet and from selecting schools around the country that have computer science degree offerings.

Table 1: Geographic Breakdown of Cybersecurity Degrees

North East	17
Mid Atlantic	8
South East	1
Mid West	5
South	2
South West	0
North West	0
West	2
Online	3

Total 38

Appendix B identifies schools studied that offer Cybersecurity undergraduate and graduate degrees including schools that have Cybersecurity Labs. From the 100 colleges and

universities studied, thirty-eight schools offer Cybersecurity degrees and seventeen of those schools have Cybersecurity Labs.

Appendix C identifies schools studied that do not offer Cybersecurity degrees. There are sixty-two schools that do not offer Cybersecurity degrees. Twenty-four of the schools have Cybersecurity Labs.

Table 1 shows the geographic breakdown of schools offering Cybersecurity degrees. Of the 38 schools that offer Cybersecurity degrees:

- 27 have undergraduate programs
- 20 have graduate programs
- 9 have both undergraduate and graduate programs
- 3 are Online
- 17 have a Cybersecurity Lab

Adding the schools that have a Cybersecurity Lab from Appendix B and C, we come up with 41 schools that have a Cybersecurity Lab.

5. CYBERSECURITY CENTER OF EXCELLENCE MODEL

A detailed review of the 41 colleges and university Cybersecurity Labs led to the model that we developed for the Saint Peter's University Cybersecurity Center of Excellence. Implementation is planned for the start of the fall 2015 Term. Appendix D is an illustration of the Cybersecurity Center of Excellence (COE) Model. The Cybersecurity COE will consist of (1) a physical 24/7 state-of-the art computer network facility consisting of hardware platforms and operating systems, network, and security software/tools and (2) a 24/7 virtual web portal that consists of Cybersecurity documents, products, tools, and an eLearning repository that can be accessed anywhere around the world.

In reviewing the 41 colleges and universities that have Cybersecurity Labs, while they had good hardware and software infrastructures and ongoing research projects, none of them included other academic departments as part of their Cybersecurity Lab. To help differentiate the Saint Peter's University Cybersecurity COE from other colleges and universities Cybersecurity Labs, we are including in our Cybersecurity COE, two academic departments: (1) Criminal Justice, and (2) Business Administration. We are also including our Guarini Institute for Government and Leadership. The two departments and the Guarini Institute will be participants and have a role in the COE. They will include their students

in educational related activities/events and also emphasize cybersecurity technical, legal, and ethical issues during course lectures, assignments, and seminars.

Technology and equipment for the COE will be made possible from vendor donations, grants, and University funding. It will include large computer screens that provide real-time information on Cyber-attack timelines, world-wide geographic locations, cyber threats and vulnerabilities, metrics, and computer dashboards from SANS (SysAdmin, Audit, Network and Security, 2014), the CERTStation (CERTStation, 2014), and the Arbor Networks Attacks Source Map (Arbor Networks, 2014).

6. CYBERSECURITY COE CONTENTS

The Cybersecurity COE will consist of a network of Windows and Linux computers. The network is currently in the design stage and will include:

- Software:
 - Microsoft SQL Server R2
 - Microsoft .NET Framework 4.0
 - IBM Security AppScan: Security Vulnerability Program
 - HP WebInspect: Security Vulnerability Program
 - LogRhythm: Log Event and Management Analysis
 - CISCO Network Simulator
 - Department of Homeland Security Cyber Security Evaluation Tool
 - Network Sniffers and Intrusion Detection Software
- Virtual Machines:
 - NETinVM: VMWare Virtual Machine Image that contains a series of User-Mode Linux Virtual Machines
 - CISCO Virtual Lab
- Vendor Testing Sites:
 - IBM Altoromutual
 - HP Freebank
 - CrackMeBank

As illustrated in Appendix D, The Cybersecurity COE, consists of four domains: Education, Leadership, Communication, and Innovation. The domains constitute the major tenants on which we designed our Cybersecurity COE. Following is what each domain will consist of/provide for:

Education:

- Programs
- Internships
- Workshops
- Tools
- Test Beds
- Physical Labs
- Virtual Labs
- Cyber Club
- Ethical Hacking Contest

Leadership:

- Subject Matter Experts
- Coordination of Resources
- Vendor Relations
- Business Relations
- Government Relations
- Liaison with other Universities

Communications:

- Increase University Awareness
- Increase Public Awareness
- Newsletters
- Multi-Media
- Threat/Vulnerability Dashboards

Innovation:

- Research
- Collaborations
- Case Studies
- Publications

In the Appendix D illustration at the top of the domains is also labeled: the National Cybersecurity Center of Excellence. We will continue to work with the NCCoE to get new ideas and incorporate state-of-the-art technology and software tools into our Cybersecurity COE. They are the overarching umbrella of our Cybersecurity COE that will help guide our future direction.

7. CYBERSECURITY COE OPERATIONS

The Cybersecurity COE, will operate in the Computer & Information Sciences Department of the University. It will be managed by a Director. The Director will be responsible for the day-to-day activities and growth of the COE. Student interns will provide technical support, work on projects, and conduct research in collaboration with University professors. We will create a Cybersecurity COE Board which will consist of Subject Matter Experts, by industry, from local businesses that will report to the Cybersecurity COE Director. This Board will meet to discuss the direction and technology/software to be deployed in the Cybersecurity COE and work to help promote the COE to the community and public. Our Cybersecurity COE will go live at the start of the fall 2015 Term.

8. RESEARCH AND WORKSHOP OPPORTUNITIES

Research will be conducted at the Cybersecurity COE that has a complex cybersecurity challenge that requires an integrated solution that has benefits for one or more industry sectors. Some examples of research could be in the area of cloud computing, mobile and wireless computing, and military information protection. The research conducted will lead to journal publications and conference presentations and papers. Workshops and seminars will be conducted by Computer Science Department subject matter experts. These workshops and seminars will be open to students, faculty and the public to educate the community, promote the Center and showcase the research activities that we are engaged in.

9. SUMMARY

Establishing a Cybersecurity COE at a college/university will provide an environment where students can learn, collaborate, conduct research, and have hands-on training to the latest technology providing a rich and dynamic learning experience. Students could participate in internships in the Cybersecurity field to allow them to further excel intellectually. By establishing a Cybersecurity COE, colleges/universities will be well positioned to train/educate their students on the very important National Cybersecurity initiative earmarked by our Government on cyber-security education. In addition, students can be provided with the skill-sets necessary to become a member of the cybersecurity workforce that is estimated to grow from \$95.60 billion in 2014 to \$155.74 billion by 2019, at a Compound Annual Growth Rate of 10.3% from 2014 to 2019 (MarketsandMarkets, 2014).

During Academic Year 2014/2015, our University we will be putting in place the Cybersecurity COE. More details on our Cybersecurity Model including implementation progress and our collaboration efforts with the NCCoE will be discussed at the 2014 ISECON Conference.

10. REFERENCES

Arbor Networks. (2014). *Digital Attack Map - Global DDoS Attack Visualization*. Retrieved June 1, 2014, from: <http://www.arbornetworks.com/>

Bayuk, Jennifer, L., Healey, J., Rohmeyer, P., Sachs, Marcus, H., Schmidt, J., Weiss, J., (2012). *Cyber Security Policy Guidebook*. Hoboken, NJ: John Wiley & Sons, Inc.

CERTStation. (2014). *CertStation's Cyber Security Dashboard*. Retrieved June 1, 2014, from: <http://www.certstation.com/>

Hackmageddon.com. (2013). *2013 Cyber Attacks Statistics*. Retrieved June 1, 2014, from: <http://hackmageddon.com/2013-cyber-attacks-statistics/>

Johnson, Thomas, A., (2012). *Power, National Security, and Transformational Global Events*. Boca Raton, FL: CRC Press.

MarketsandMarkets. (2014). *Cyber Security Market worth \$155.74 Billion by 2019*. Retrieved June 1, 2014, from: <http://www.marketsandmarkets.com/PressReleases/cyber-security.asp>

McAfee - Center for Strategic and International Studies. (2013). *The Economic Impact of CyberCrime and Cyber Espionage*. Retrieved June 1, 2014, from: <http://www.mcafee.com/sg/resources/reports/rp-economic-impact-cybercrime.pdf?cid=BHP016>

National Cybersecurity Center of Excellence. (2014). *The Center*. Retrieved June 1, 2014, from: <http://nccoe.nist.gov/?q=content/about>

National Initiative for Cybersecurity Education. (2014). *National Cybersecurity Workforce Framework*. Retrieved June 1, 2014, from: <http://csrc.nist.gov/nice/framework/>

National Institute of Standards and Technology. (2014). *Cybersecurity Framework*. Retrieved June 1, 2014, from: <http://www.nist.gov/cyberframework/index.cfm>

Norton. (2012). *Cybercrime Report 2012*. Retrieved June 1, 2014, from: <http://nowstatic.norton.com/now/en/pu/images/Promotions/2012/>

- cybercrimeReport/2012_Norton_Cybercrime_Report_Master_FINAL_050912.pdf
Ponemon Institute. (2013). *2013 Cost of Cyber Crime Study Reports*. Retrieved June 1, 2014, from: <http://www.hpenterprisesecurity.com/ponemon-2013-cost-of-cyber-crime-study-reports>
- SysAdmin, Audit, Network and Security (SANS). (2014). *Programs*. Retrieved June 1, 2014, from: <http://www.sans.org/programs/>
- The White House. (2014). *Comprehensive National Cybersecurity Initiative*. Retrieved June 1, 2014, from: <http://www.whitehouse.gov/issues/foreign-policy/cybersecurity/national-initiative>

Editor's Note:

This paper was selected for inclusion in the journal as an ISECON 2014 Meritorious Paper. The acceptance rate is typically 15% for this category of paper based on blind reviews from six or more peers including three or more former best papers authors who did not submit a paper in 2014.

APPENDIX A

Requirements for Computer Science Major - Cybersecurity Concentration.

This option is designed for those who want to learn the technology that is necessary to secure and defend information systems and networks. Students will be able to:

- Protect an organization's vital information and assets
- Implement cybersecurity best practices and risk management
- Understand how to use software to minimize vulnerabilities
- Implement network monitoring and real-time security solutions
- Analyze persistent threats and implement counter measures
- Conduct risk assessments on information systems and networks
- Examine cybercrimes and support recovery of operations
- Create and communicate cybersecurity strategies
- Manage cybersecurity projects

COURSE	CREDITS
Elementary Calculus I	3
Elementary Calculus II	3
Fund Comp Prog: Html, JavaScript, C++	3
Introduction to C++	3
Advanced Programing Techniques Using C++	3
Information Technology Ethics	3
Data Structures	3
Computer Mathematics	3
Quantitative Methods for Business	3
Database Concepts	3
Information Technology Audit	3
Disaster Recovery	3
Cybersecurity and Risk Management	3
Telecommunications Networks	3
Cryptography	3
Cybersecurity Lab	3
Computer Science Major Capstone Course	3
	Total Credits 51

APPENDIX B

Colleges and Universities Offering Cybersecurity Degrees with associated Labs.

College/University	Undergrad	Graduate	Cyber Security Lab
Air Force Academy	Y		Y
Champlain University	Y		
Columbia		Y	Y
DePaul University	Y		
FDU	Y		
George Mason University	Y	Y	Y
George Washington University		Y	
Georgia Tech		Y	Y
Mercy College	Y	Y	
New England Institute of Technology	Y		
NJIT		Y	Y
NYU-Poly		Y	Y
Penn State (ONLINE)	Y		Y
Purdue	Y	Y	Y
Rasmussen College	Y		
RIT	Y	Y	Y
Robert Morris University	Y		
Sacred Heart University		Y	
Saint Peter's University	Y		
South East Missouri State University	Y		
Southern Methodist University	Y		Y
St. Johns University	Y	Y	
Stevens Institute of Technology	Y	Y	Y
Temple		Y	
University of Massachusetts Amherst	Y		Y
University of Dallas		Y	
University of Maryland	Y	Y	Y
University of Maryland Baltimore County		Y	Y
University of Maryland University College (ONLINE)	Y	Y	
University of Phoenix (ONLINE)	Y		
University of Notre Dame	Y		
University of Pittsburgh	Y		

US Military Academy	Y		Y
US Naval Academy	Y		Y
USC	Y	Y	Y
Villanova		Y	
Virginia College		Y	
West Chester University	Y		
TOTALS	27	20	17

APPENDIX C

College/University No Cybersecurity Degree – Has Cybersecurity Lab	College/University No Cybersecurity Degree – No Cybersecurity Lab
Boston University Carnegie Mellon Clemson Duke Indiana University Iowa State University James Madison University Kansas State LSU Mississippi State MIT North Carolina State Oklahoma State Oregon Pace University Penn State Santa Clara University Stanford Stony Brook UCLA University of California - Berkley University of Texas University of Washington Virginia Tech	Alabama Auburn Boston College Brigham Young Brown University Case Western Reserve Fairfield Florida International Georgetown Gonzaga University Harvard Manhattan College Memphis University Michigan Michigan State Northwestern University Ohio State Princeton Rutgers Saint Louis University Seton Hall Syracuse University of Chicago University of Cincinnati University of Florida University of Georgia University of Illinois University of Miami University of North Carolina University of Pennsylvania University of San Diego University of South Florida University of Wisconsin

	Virginia Wake Forest William & Mary Xavier Yale
--	-------------------------------------------------------------

APPENDIX D

Cybersecurity Center of Excellence – Model

