

DOCUMENT INDEX:

(Clickable)

The Challenges Of It Security	2.
Industry Overview	2.
Projected Job Growth	3.
What Employers Want	4.
Benefits to Employers	4.
Fast Track Your Way to a New Career	4.
About the Institute and Univ of Tulsa	5.
Now Designed for Working Adults	6.
Faculty and Graduates	6.
Module Descriptions	8.
Ceis 4013	8.
Ceis 4413	8.
Ceis 4313	8.
Ceis 4113	9.
Ceis 4213	10.
Vet Benefits	11.
Registration Requirements	11.
Tuition and Application Info	12.
Financial Aid & Payment Plans	12.
Contact Info	13.

DID YOU KNOW?

- 221 billion dollars a year are lost by businesses all over the world due to identity theft.*
- Between 200 and 300 computer viruses are created each month
- 99.67% of companies surveyed experienced at least one virus encounter, 51% claimed they had at least one “virus” disaster during the 12 month period before they were surveyed including hard and soft dollar figures, the true cost of virus disasters is between \$100,000 and \$ 1 Million per company.
- Reuters reported that over \$ 12 billion in damage was ww-caused by computer viruses in the first 6 months of the year 2000 alone.
- According to “Tippet’s Law of Malicious Code,” the virus problem doubles about every 14 months.”

Source: www.comptia.org/research/security.aspx

Computer Crime & Security Survey Computer Security Institute, March 12, 2001

www.tudce.org to learn more



Contact Us!

THE CHALLENGE OF IT SECURITY:

IT security remains a major concern of IT professionals around the world according to CompTIA's 7th Annual Trends in Information Security: an Analysis of IT Security and the Workforce study.

As information technology's role within an organization continues to expand, so does the potential for security breaches.

In 2008, the average number of security breaches increased slightly from previous years. Although the number of security breaches remained moderate over the last few years, the data indicates the severity levels have increased. This suggests many organizations have made significant progress

in dealing with security issues, but the number and types of threats have increased in step.

The most significant costs of security breaches remains the overall impact on employee productivity. About one-third of U.S. respondents cite lost productivity as the top consequence of a breach, followed by a disruption of revenue-generating activities. The primary cause for the most severe security breaches remains unintentional in nature and typically caused by human error. This demonstrates a need for more employee training and a deeper knowledge of technology functions.

INFORMATION SECURITY INDUSTRY OVERVIEW:

"The need for highly trained IT security professionals is higher than ever," and continues to grow. This is due largely to the ever increasing attacks and intrusions by malicious hackers and criminals. There are so many threats ranging from attacking and shutting down our most necessary resources, to causing huge problems in business networks and compromising criti-



Contact Us!

cal data stored on company servers and machines. With the fear of a major terrorist attack increasing every day, many companies are left vulnerable to these types of problems. The best way to combat and prevent these types of intrusions is to hire or contract certified professionals that have the skills and know how to protect against them.

If you are considering a career in Information Technology, you will soon realize that there are many career options and good jobs available. You will also discover that IT careers offer the flexibility to work in a variety of different industries. Just look around you and see how much we rely on this technology every day. Then imagine being part of this exciting, growing, and fast changing industry.

The Information Technology Association of America (ITAA) reports that 92% of all IT workers are in non-IT companies, 80% of which are small companies. Even if the career you are currently in or are hoping to work in does not focus

solely on IT, the job will likely involve the use of computers and technology to accomplish tasks and process information.

Source: www.trainace.com

PROJECTED JOB GROWTH

The United States Department of Labor's Bureau of Labor Statistics predicts that between 2001 and 2012, the number of computer security specialists is expected to increase much faster than the average. Companies and other organizations will continue to adopt and integrate new computer driven technologies, making the computer system design and related services industry one of the fastest growing industries in the U.S. economy.

The federal government and the Department of Homeland Security have made information protection a matter of national security, and that is not limited to just the government information. Access to private data and sensitive business details could create security problems. Therefore, despite any downturns in the information technology economy, the market for



Contact Us!

information security and other computer security personnel is likely to remain strong.

WHAT DO EMPLOYERS WANT?

At the June 2005 Colloquium on Information Systems Security Education (CISSE) held at Georgia Technical University, many industry speakers emphasized the value of management perspectives, experience and vocabulary in their information assurance staff. They repeatedly stressed the importance of intellectual flexibility, the ability to learn new skills, and the capacity to communicate effectively with non-technical colleagues.

BENEFITS TO EMPLOYERS

GRADUATES OF THE CERTIFICATE IN INFORMATION

SECURITY WILL BE ABLE TO:

- Create systems designed to protect data from misuse by people who are either inside or outside your business or organization

- Design computer networks and infrastructure that will allow you to accomplish your goals while protecting core information
- Create intrusion and detection systems that inspect all inbound and outbound network activity to identify suspicious patterns that may indicate someone is attempting to break into or compromise a computer system
- Create a system that provides user authorization and authentication. Authorization allows the user access to various resources based upon proof of the user's identity. Authentication makes certain that users are who they claim to be.
- Maintain the integrity of your business or organizations data and develop a recovery backup system
- Create a security policy for your business or organization and make sure that this is adhered to by people within the organization.
- Familiarity with national and state laws that regulate privacy concerns and electronic commerce

FAST TRACK YOUR WAY TO A NEW CAREER

The Certificate in Information Security is designed to equip students with marketable skills and knowledge for adaptation to specific tasks and industry recognized standards associated with network security, information and data security, and information assurance. The fifteen credit certificate



Contact Us!

program is endorsed by the U.S. Federal Government's Committee on National Security Systems (CNSS).

STUDENTS WHO SUCCESSFULLY COMPLETE THE PROGRAM ARE ELIGIBLE FOR BOTH THE NSTISSI 4011 INFORMATION SECURITY PROFESSIONAL CERTIFICATION AS WELL AS THE CNSSI 4012 SENIOR SYSTEM MANAGER'S CERTIFICATION.

These are standard credentials for information systems security personnel employed as:

- Senior Systems Managers
- System Administrators
- Information Systems Security officers
- System Certifiers
- Risk Analysts

In addition to obtaining the 4011 and 4012 Certifications, you will have made significant progress towards the remaining 4013, 4014, 4015 and 4016 Certifications.

OBTAIN YOUR 4011 AND 4012 CERTIFICATION PLUS 15 UNDERGRADUATE CREDITS IN JUST 40 WEEKS!

ABOUT THE INSTITUTE FOR INFORMATION SECURITY AT THE UNIVERSITY OF TULSA

The University of Tulsa's (TU's) Institute for Information Security (iSec) is a multidisciplinary program of study and research tackling cyber security issues on a global scale. TU has already established itself as one of the leading schools in the country for information security research and education with more than a decade of experience in the field.

The excellence of iSec's committed faculty and students has earned the recognition of several government and industry partners. TU has been designated as a NSA Center of Academic Excellence in Information Assurance Education, and boasts an array of educational opportunities for undergraduates, graduate students and professionals alike. The information assurance curriculum at TU offers certifications for all six federal



Contact Us!

information security standards endorsed by the Committee on National Security Systems.

TU is also a NSA Center of Excellence in Information Assurance Research. In research, iSec has core concentrations in critical infrastructure protection, security engineering, enterprise security and digital forensics. iSec faculty and students work closely with two congressionally-funded centers: the Memorial Institute for the Prevention of Terrorism in Oklahoma City and the Institute for Security Technology Studies at Dartmouth College. In addition, the Institute participates in the I3P Consortium, headquartered at Dartmouth College.

Now Designed For the Convenience of Working Adults

The traditional INFOSEC Certificate Program is now offered in the evening to meet the needs of busy working professionals like you, who are either looking to enter the field of information security or looking to advance in your current

career. The courses are offered in three-hour blocks two nights a week for eight weeks. iSec requires all applicants to have a minimum of 60 college level credits.

FACULTY



DR. JOHN HALE

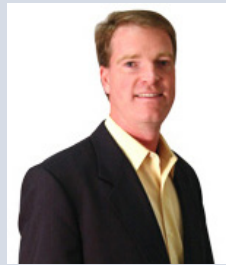
**DIRECTOR, ASSOCIATE PROFESSOR OF
COMPUTER SCIENCE**

Dr. John Hale, Director of the Institute for Information Security, received his Bachelor

of Science in 1990, Master of Science in 1992 and doctorate degree in 1997, all in computer science from TU. As director of the Institute, Hale has overseen the development of the premier information assurance curriculum in the nation. In 2000, he earned a prestigious National Science Foundation CAREER award for his education and research initiatives at iSec. His research interests include cyber attack modeling, analysis and visualization, enterprise security management, secure operat-



ing systems, distributed system verification and policy coordination.



DAVID GREER
EXECUTIVE DIRECTOR OF THE INSTITUTE FOR INFORMATION SECURITY

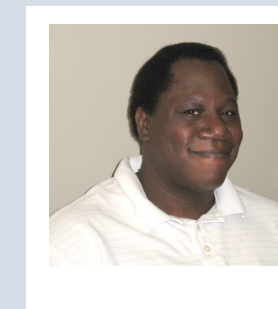
David Greer brings more than 10 years of combined experience to iSec, including time as an information security and digital forensics consultant, information security coordinator, e-learning coordinator and software compliance specialist. As executive director of iSec, Greer is charged with the development, implementation and supervision of the Institute's mission to produce exceptional graduates and technical discoveries in the information security field. He also serves as the liaison between iSec and industry, government, academic partnerships and alumni. In addition, Greer's duties extend to seeking research funding for classified, unclassified, public and private projects.

Contact Us!



JIM MORRIS
INSTRUCTOR INFORMATION SECURITY PROGRAM

Jim Morris has a B.S. in Business and Information Systems and an M.S. in Computer Science specializing in Information Assurance and Digital Forensics from the University of Tulsa. He holds numerous IT certifications and frequently attends conferences and workshops where he presents on various data security and digital forensic topics.



WILLIAM REDDING
GRADUATED STUDENT - 2008

"I have spent my adult career within the information technology field. While enrolled in the Certificate in Information Security Program, I learned best practices and other techniques I never knew existed. This information has been a vital asset to my career and employer. I was able to utilize what I had learned within a few weeks back at my workplace."

-IS Student 2008

Contact Us!

MODULE DESCRIPTIONS

**ALL CLASSES ARE OFFERED AT THE ADVANCED
4000 LEVEL**

CEIS 4013 INTRO TO COMPUTER SECURITY (3 CREDITS)

AUG 24 – OCT 14 2010

COURSE GOALS AND OBJECTIVES

To develop the student's basic understanding of computer security and proficiency with related technologies. To promote the student's appreciation for the threats to computer systems, the data residing on those systems and the measures that can be taken to mitigate the threats and to protect systems data.

MAJOR TOPICS COVERED IN THE COURSE

- Attacks, Computer Criminals, Methods of Defense
- Symmetric/Asymmetric Encryptions Systems, Data Encryption Standard, Public Key Encryption
- Secure Programs, Nonmalicious Program Errors, Viruses and Other Malicious Code
- Memory and Address Protection, File Protection Mechanisms, User Authentication

- Security Policies, Models of Security, Assurance in Trusted Operating Systems
- Security Requirements, Reliability and Integrity, Sensitive Data, Inference, Multilevel Databases, Data Mining
- Network Concepts, Threats in Networks, Network Security Controls, Firewalls, IDS, Secure E-mail
- Security Planning, Risk Analysis, Physical Security
- Quantifying Security, Modeling Cyber Security
- Privacy Principles and Policies, Authentication and Privacy, Privacy on the Web
- Information and the Law, Rights of Employees and Employers, Ethical Issues





Contact Us!

CEIS 4413 PROTECTING NETWORKS AND AUTOMATED INFORMATION SYSTEMS (3 CREDITS)

OCT 19 – DEC 16 2010

COURSE GOALS / OBJECTIVES

To develop the student's basic understanding of threats to networks and automated information systems. To promote the students understanding for methods to protect networks and automated information systems through defense in depth and the implementation of hardware and software firewalls, intrusion detection systems, access control devices, etc.

MAJOR TOPICS COVERED IN THE COURSE:

- Firewalls
- Security Policy
- Virtual Private Networks
- Network Intrusion Prevention/Detection
- Host Hardening
- Secure Perimeter Design
- Separating Resources

CEIS 4313 IT SECURITY RISK MANAGEMENT (3 CREDITS)

JAN 11 – MAR 3 2011

COURSE GOALS / OBJECTIVES:

To develop the student's basic understanding of an effective risk management process and that risk management's principle goal is to protect the organization and its ability to perform the organization's mission, not just its IT assets.

MAJOR TOPICS COVERED IN THE COURSE:

- System Characterization
- Threat Identification
- Vulnerability Identification
- Control Analysis
- Likelihood Determination
- Impact Analysis
- Risk Determination
- Control Recommendations
- Results Documentation



Contact Us!

CEIS 4113 SECURE ELECTRONIC COMMERCE

(3 CREDITS)

MARCH 8 – MAY 5 2011

COURSE GOALS/OBJECTIVES:

To develop the student's basic understanding of secure electronic commerce architectures, proficiency with related technologies. To promote the student's appreciation for legislative and regulatory issues of electronic commerce and the role of public policy in shaping a global digital economy.

MAJOR TOPICS COVERED IN THE COURSE:

- Paper-based Commerce vs. Electronic Commerce, Electronic Risks
- Internet Applications, the Internet Community, Electronic Data Interchange (EDI) on the Internet
- Business/Legal Principles, Binding Electronic Transactions, Legislation/Regulation, Business Models
- Electronic commerce technologies, Shopping Carts, Agents, Electronic Cash
- Cryptography (DES,RSA), Digital Signatures, Key Management, Authentication
- Network Protocol Security, Firewalls, Message Secrecy, Web

Security, EDI Security, SET Protocol

- Certificates, Public-Private Key Management, Certificate Distribution, X.509, Certification Practices
- Public-Key Infrastructures (PKI), Hierarchical Models, PGP, Progressive Constraint Trust
- Principles of Non-repudiation, Trusted Third Parties, Dispute Resolution

CEIS 4213 ENTERPRISE SECURITY MANAGEMENT

(3 CREDITS)

MAY 10 – JUNE 30 2011

COURSE GOALS/OBJECTIVES:

To develop the student's basic understanding of threats to the data infrastructure of an enterprise. To promote the student's appreciation for the threats to enterprise computing systems, the data residing on those systems, the means to identify and quantify threats, measures to mitigate threats and protect systems and data essential to the enterprise, and to proactively



Contact Us!

deal with incidents that may occur in an enterprise infrastructure.

MAJOR TOPICS COVERED IN THE COURSE:

- Risk Management and Analysis
- Vulnerability Analysis
- Legal Aspects of ESM
- Security Metrics
- Contingency Planning
- Disaster Recovery
- Incident Handling

VET BENEFITS:

Are you a United States Military Veteran?

This program has been approved for education benefits by the U.S. Department of Veterans Affairs, Oklahoma State Accrediting Agency.

For further information on how to apply for educational benefits contact the University of Tulsa School Certifying Officer, Cindy Watts, at: Cindy-watts@utulsa.edu or phone: (918) 631-3985

PROGRAM REGISTRATION REQUIREMENTS:

- Applicants must be twenty-five years old or older;
- Must have been out of full-time education for a minimum of two years;
- Required minimum of sixty college credits;
- Some certificate programs may have additional admission requirements

PLEASE NOTE: STUDENTS CURRENTLY SEEKING A DEGREE FROM THE UNIVERSITY OF TULSA WILL NOT BE ELIGIBLE FOR CERTIFICATE PROGRAMS OFFERED BY THE DIVISION OF CONTINUING EDUCATION.



Contact Us!

TUITION AND APPLICATION INFORMATION

Students seeking admission into the credit certificate programs, like all other students seeking academic credit from the University, must first be admitted to the University of Tulsa. Certificate applicants complete a convenient, short application form and provide supporting documentation to the Division of Continuing Education.

TUITION INFORMATION:

The University of Tulsa offers a significant reduction in the credit hour rate for credit classes taken through the Division of Continuing Education. The 2010 Division of Continuing Education credit hour rate is \$545. Tuition for each of 3 credit hour class \$1,635.

THERE IS A NON-REFUNDABLE APPLICATION FEE OF \$30.

STUDENTS ARE REQUIRED TO ENROLL FOR CLASSES EACH SEMESTER.

FINANCIAL AID: AVAILABLE THROUGH OFFICE OF STUDENT FIN. SERV: (918) 631-2527

MONTHLY PAYMENT PLANS:

Monthly payment plans are available through FACTS Tuition Management.

Phone: 1-800-609-8056 or 1-800-609-8056

Or visit: www.factsmgt.com.

TUITION REIMBURSEMENT:

Many companies in the Tulsa area pay all or part of their employees' tuition. The Company Deferment Form will be included in your registration packet.

Contact Us!

FOR MORE INFORMATION AND AN ADMISSIONS PACKET,
CONTACT US AT:

PHONE: (918) 631-2524

EMAIL: DEANNA-SAPLIN@UTULSA.EDU

WEB: WWW.CONTED.UTULSA.EDU

FAX: (918) 631-3367

MAIL: THE UNIVERSITY OF TULSA

DIVISION OF CONTINUING EDUCATION

JOHN ZINK HALL

800 S. TUCKER DRIVE

TULSA, OK 74104