IDC 6601
Behavioral Aspects of Cybersecurity
"Situation Awareness"

Bruce Caulkins, Ph.D.

Institute for Simulation and Training
University of Central Florida

AGENDA

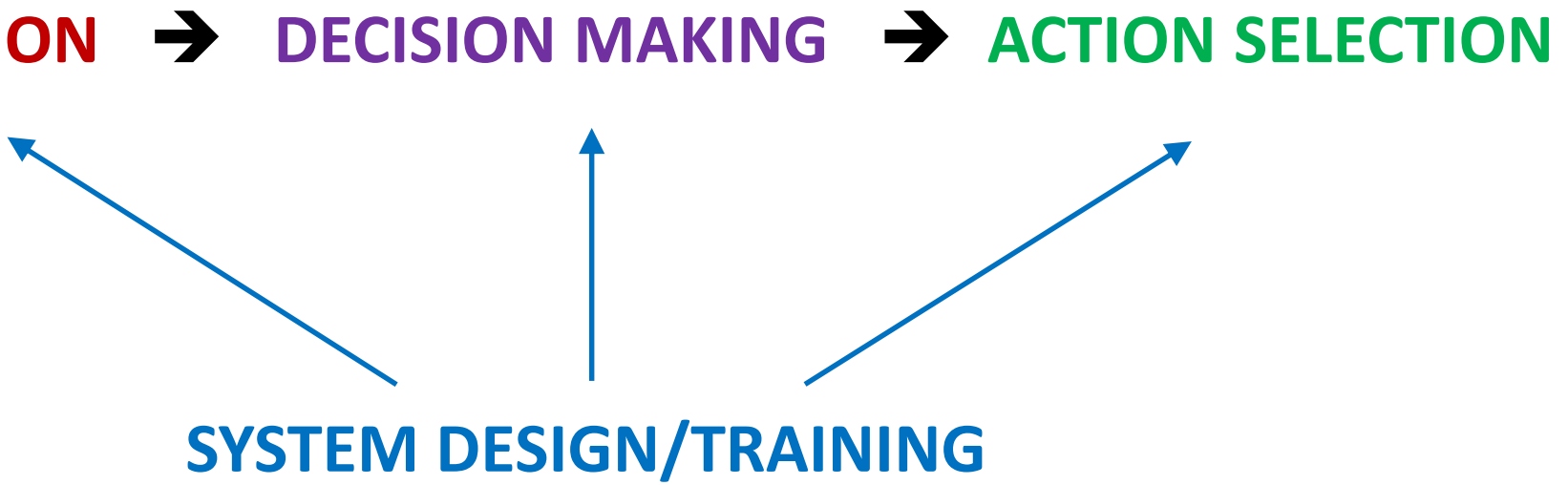
Awareness

- Situation Awareness
- Threats
- Security Awareness

HUMAN FACTORS & CYBERSECURITY

1. What has Human Factors got to do with Cybersecurity?

   Scientific principles of ***perception***, ***decision making***, ***action selection***, and ***training*** that have been developed in basic and applied cognitive research can provide a principled basis for analyzing the factors affecting security-related human decisions and choices.



HUMAN FACTORS & CYBERSECURITY

PERCEPTION

- Perception of information
- Views on security, risk perception (bias, heuristics)

DECISION MAKING

- Individual Differences
- Expert vs. novice decision making
- Decision making under stress, over/underload, fatigue
- Bias and heuristics that affect decision making
- Factors that contribute to vulnerability (weapons of influence, social engineering etc.)

ACTION SELECTION

- Ease of implementing response required

AWARENESS & TRAINING

- Situational Factors
- Situation Awareness
- Organizational factors

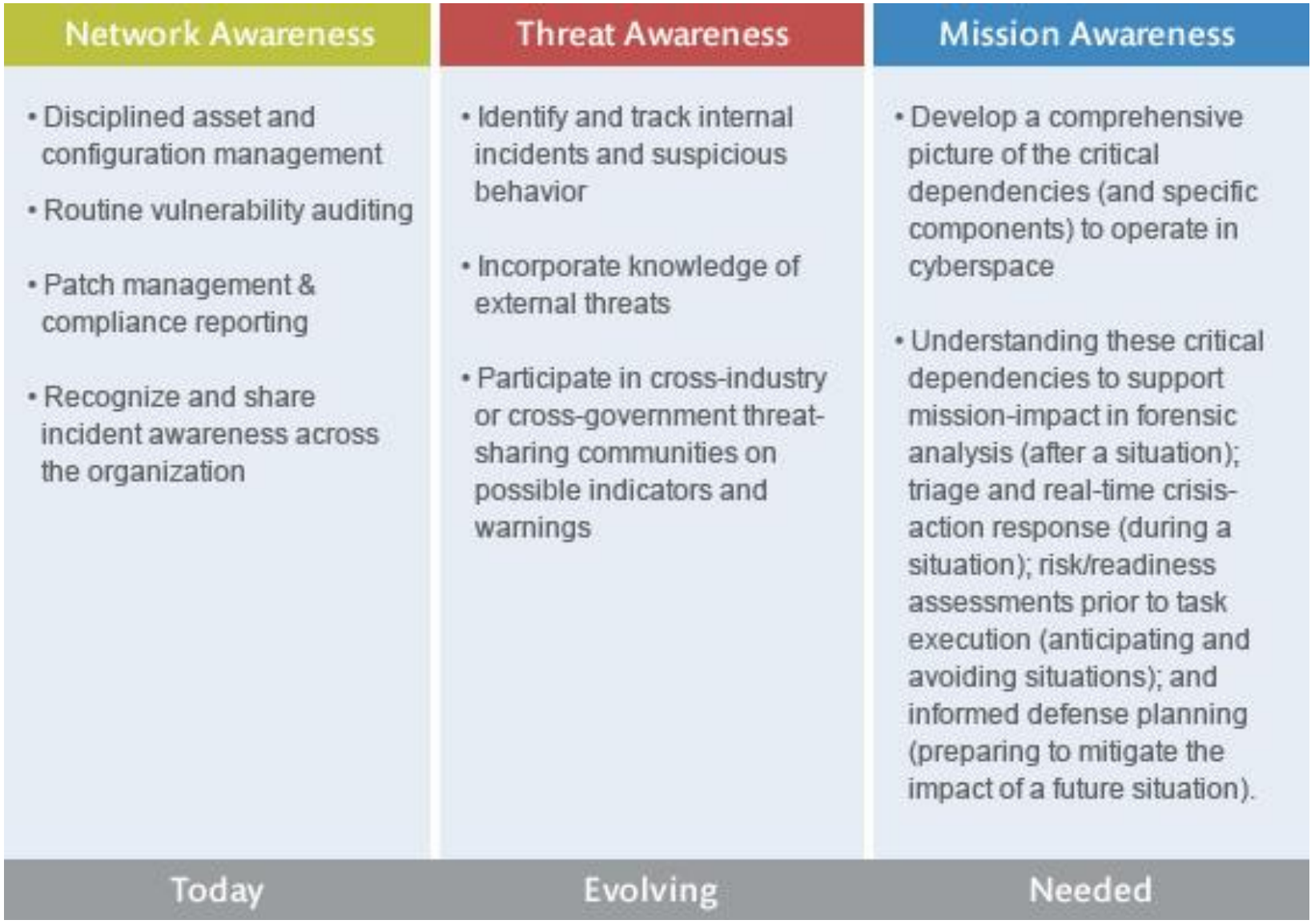
SYSTEM DESIGN

- Features of task, website etc

Situation Awareness - Cybersecurity

- Situation Awareness (SA): Understanding the environment to accurately predict and respond to threats and potential problems that might occur.
- Three key areas of comprehensive cyber SA
  - ✓Computing & Network
  - ✓Threat Information
  - ✓Mission Dependencies

Situation Awareness



Situation Awareness – Some of the Leading Threats

- Viruses
  - ✓ Software programs designed to invade computers, interfere with its operation, and to copy, corrupt or delete data.
- Worms
  - ✓ Smart viruses that replicate automatically and send themselves to other computers
- Trojan Horses / Logic Bombs
  - ✓ Malware that destroys data when certain conditions are met. Looks to be doing one thing while actually doing another
- Social Engineering Tactics
  - ✓ Lies, impersonation, tricks, bribes, blackmail, and threats
- Rootkits
  - ✓ A collection of programs that a hacker uses to mask intrusion and obtain administrator-level access to a computer or computer network.
- Botnets / Zombies
  - ✓ A collection of compromised computers or **zombies**, used to send out spam, viruses or distributed denial of service attacks.

Situation Awareness – Security Gaps

- Security technology is essential
  - ✓ Firewalls, anti-virus, intrusion detection, encryption etc.
- Technology is not enough
  - ✓ Gartner: 80% of downtime is due to people and processes
- Tighter the security controls, the harder they are to break and the target becomes the user
  - ✓ Technology can make it difficult to forge IDs but can't stop people getting real IDs under fake names
- Technology can never stop social engineering
  - ✓ People are still tricked into disclosing their passwords

Situation Awareness – Organizational Level

Information Security Program: Designed to prepare and protect information

- Policy and Procedures
  - ✓To support business objectives while considering security requirements
- Informing users of their responsibilities
  - ✓Employees must know policies, understand their obligations, and actively comply
- Monitoring and review of program
  - ✓Measuring how well employees maintain awareness and follow protocols

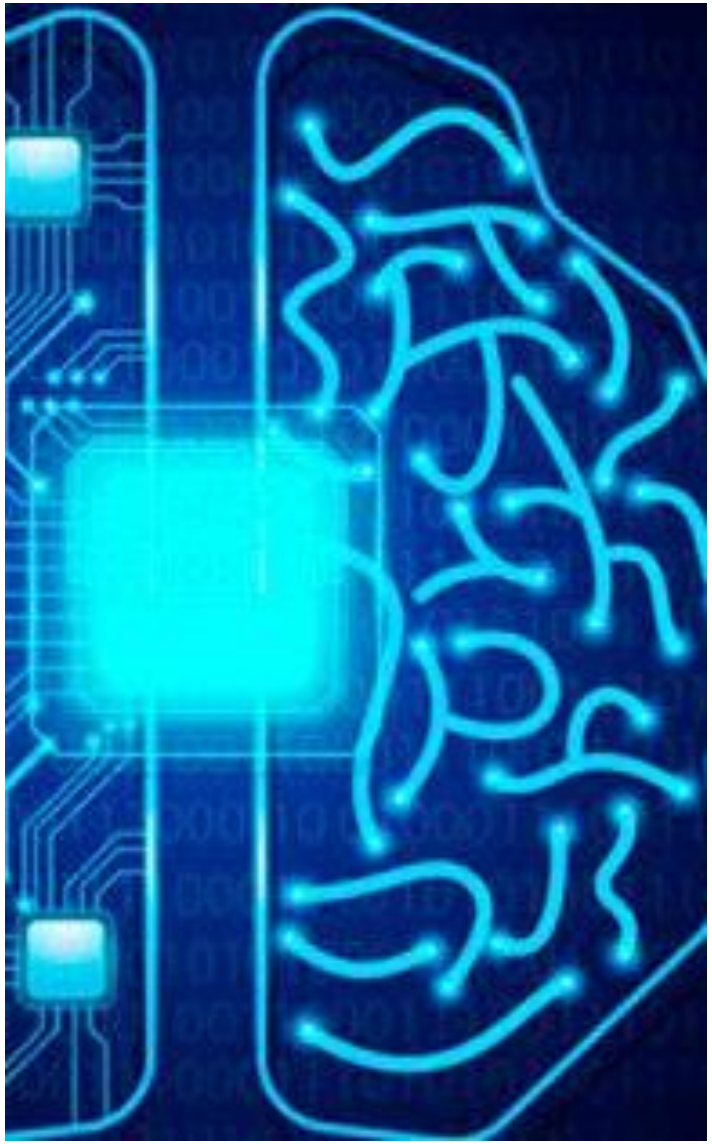
Situation Awareness – Information Security Waves

- Technical Wave
  - ✓Authentication and access control
- Management Wave
  - ✓Policies, procedures
  - ✓CISO and separate security staff
- Institutionalization Wave
  - ✓Information Security Awareness
  - ✓Information Security Culture
    - Standardization, certification and measurement
    - Human Aspects

Von Solms (2000)

Situation Awareness – Humans & Technology

- Security controls deal with known risk
- People spot irregularities
- Employees that are security conscious and correctly trained
  - ✓Develop a “feeling” for what is “normal” behavior
  - ✓Recognize unusual, unexpected behavior
- Employees need to
  - ✓Adapt to new scenarios
  - ✓Report and act on incidents



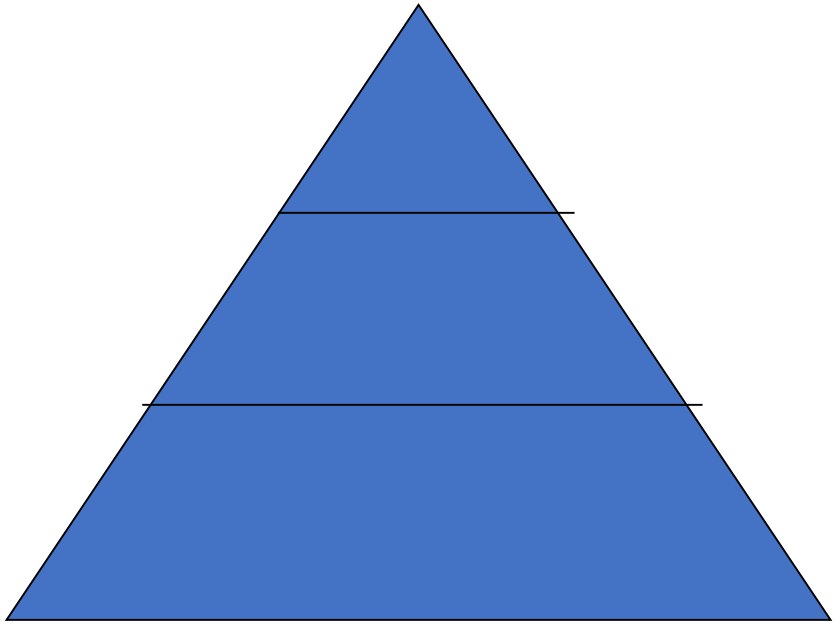
Situation Awareness – The Human Element

Information and Information Systems Security:

Products

Processes

People



H/W and S/W

Management
Operational

Users
Administrators

Situation Awareness – The Human Element

NIST SP 800-53

- "An effective information security program should include … security awareness training to inform personnel of the information security risks associated with their activities and responsibilities in complying with organizational policies and procedures designed to reduce these risks"

NIST SP 800-50

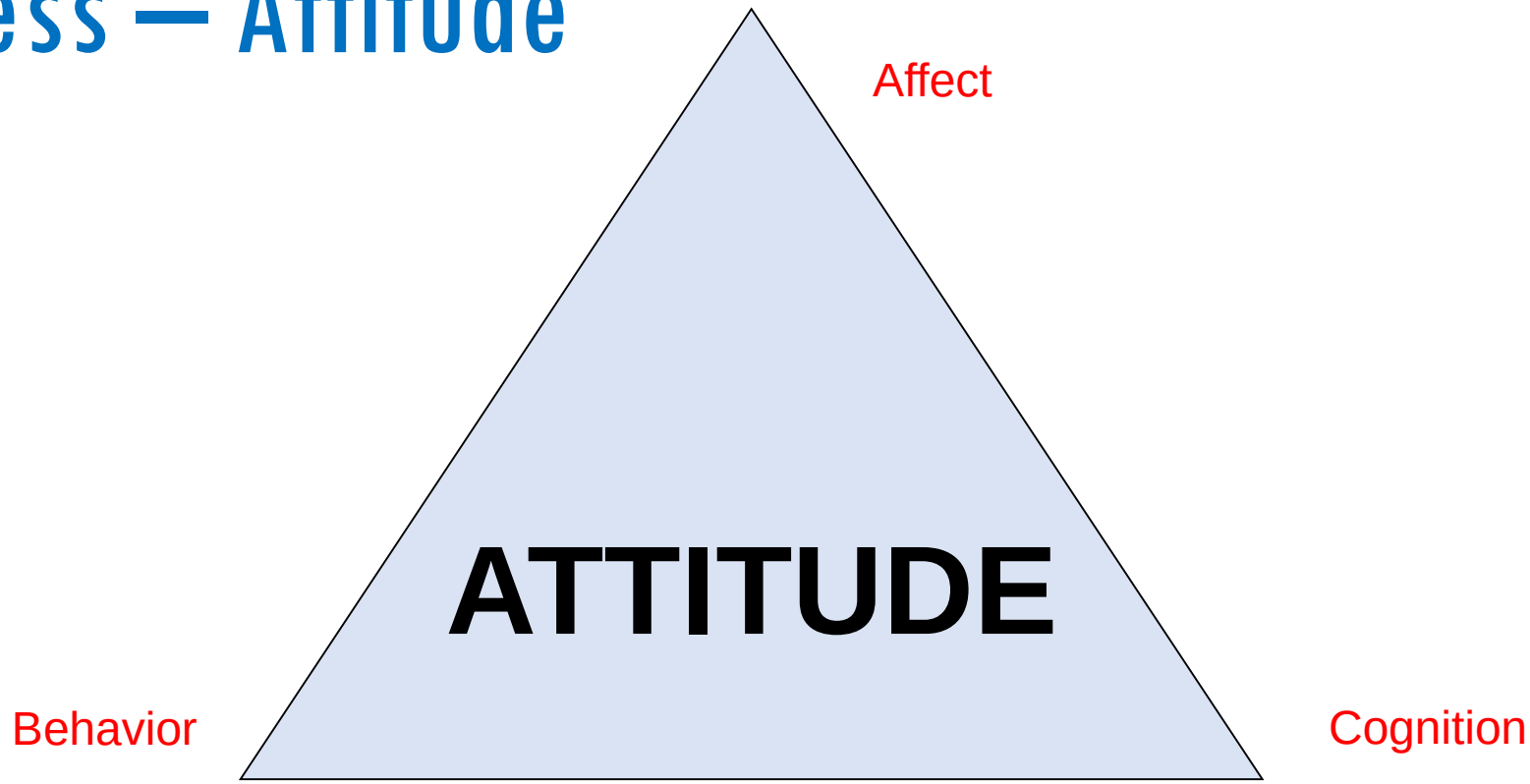
- "Awareness involves guiding and motivating people on appropriate behaviors"

NIST SP 800-16

- The fundamental value of security awareness is to create "a change in attitudes which change the organizational culture"

Situation Awareness – Attitude

- Attitude is important
  - ✓Predictor of Behavior
  - ✓Motivator of Behavior
  - ✓Source of Risk
  - ✓Irrational behavior



Influencing Behavior and Decision-Making

Sam Chum, CISSP: *Change that Attitude: The ABCs of a Persuasive Awareness Program*

Awareness, Training & Education

Comparative Framework			
	Awareness	**Training**	**Education**
Attribute	What	How	Why
Level	Information	Knowledge	Insight
Learning Objective	Recognition & Retention	Skill	Understanding
Example Teaching Method	*Media* -Videos -Newsletters -Posters	*Practical Instruction* -Lecture and/or demo -Case study -Hands-on practice	*Theoretical Instruction* -Seminar and discussion -Reading and study -Research
Test Measure	True/False Multiple Choice (identify learning)	Problem Solving Recognition & Resolution (apply learning)	Essay (interpret learning)
Impact Timeframe	Short-Term	Intermediate	Long-Term

"The Human Factor in Training Strategies" by Dorothea de Zafra, Nov. 1991 as quoted in NIST SP 800-16

Situation Awareness: Challenges

- Keep current on new threats, vulnerabilities and solutions
- Educate general users and senior management of threats and exploits. Show them why cyber security is needed and what they can do to protect information
- Instill in all employees a feeling of shared responsibility
- Sell information security

Situation Awareness – In the Workplace

Implement a Security Awareness Program to:

- Communicate security requirements
  - ✓ Policy, rules of behavior
- Communicate Roles and Responsibilities
- Improve understanding of proper security procedures
  - ✓ At work and at home
- Serve as basis for monitoring and sanctions program

Situation Awareness – WHO?

- Every system user!
  - Needs some form of SA

- NIST defines 5 roles
  - ✓Executives
  - ✓Security Personnel
  - ✓Systems Owners
  - ✓Systems Admin and IT Support
  - ✓Operational Managers and System Users

Improving SA in the Workplace: WHAT?

Security Awareness personnel need to:

Understand

- Security threats
- Business objectives
- Line managers' concerns, problems
- Individual and group issues

Possess

- IT Background and security knowledge
- Communication Skills

Improving SA in the Workplace: HOW?

- Mandatory annual awareness presentation for all
  - ✓General
  - ✓Real world examples
  - ✓Lots in the Press about Identity Theft
- Home PC Security
  - ✓Bring the message home
- Other sessions tailored for particular groups
  - ✓Targeted messages and examples
- Involve people in awareness to overcome their resistance to change

Improving SA in the Workplace: WHEN & WHERE?

- Prior to being granted privileges
  - ✓No access without awareness
- Periodically
  - ✓Mandatory Annual Awareness
  - ✓Classes or On-line
- Interim, short communiqués
  - ✓E-mails, broadcasts, “Tip of the Day”
  - ✓In response to new threats, vulnerabilities and policies
- Small group sessions
- Less formal events
  - ✓Fairs, Awareness Days
  - ✓Games – Security Jeopardy

Situation Awareness: After Training

Cyber Personnel:

- Are aware of the threats, vulnerabilities and consequences of exploits
- Recognize and report suspicious activity
- Can discuss why controls are necessary
- Take an active role in protecting information

Situation Awareness Benefits of Program

Trained employees lead to:

- Fewer Audit Findings
- Fewer material weaknesses
- Fewer violations
- Less severe incidents
- Less repetition of errors
- Less damage
- Reduced cost of compliance

Situation Awareness Recap

- Cyber experts can be better prepared through SA
- Important to maintain cyber situation awareness
- Organizational commitment to SA preparation is necessary in the workplace

IDC 6601
Behavioral Aspects of Cybersecurity
"Situation Awareness"

Bruce Caulkins, Ph.D.

Institute for Simulation and Training
University of Central Florida