

ISACA Curriculum

<http://www.isaca.org/Knowledge-Center/Academia/Pages/Educational-Materials-for-Professors-and-Teachers.aspx>

infosysclub@uncc.edu



CYBERSECURITY FUNDAMENTALS CAREER STARTER

BE PART OF BUILDING A STRONGER CYBER SECURITY WORKFORCE

How to Download the Academic Package

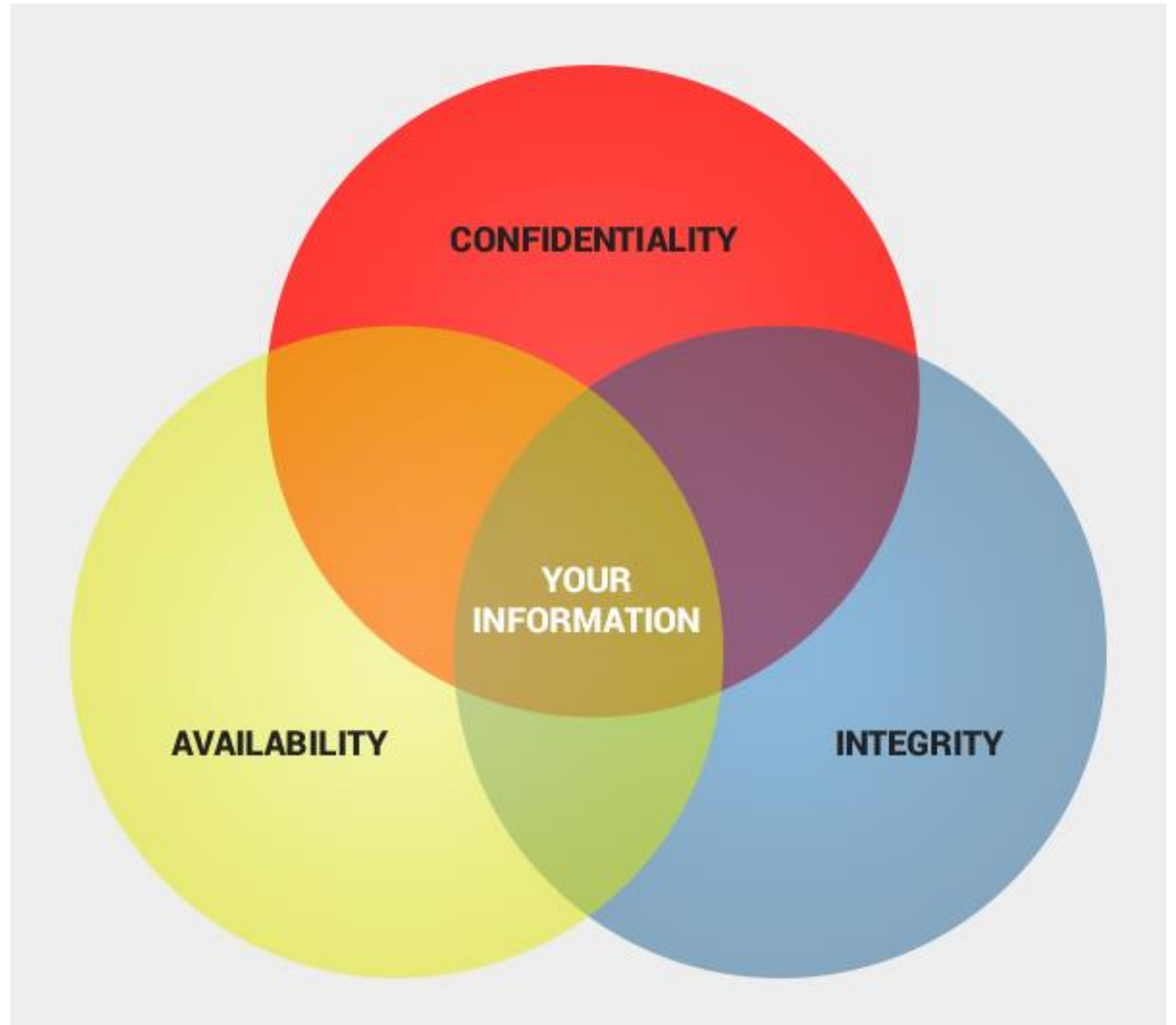
Introduction to Cybersecurity

Section 1 – Topic 1

1. Cybersecurity definition
2. Objectives of cybersecurity
3. Key business and technology factors

Cybersecurity Triad

- **Confidentiality**
protection from unauthorized access
- **Integrity**
protection from unauthorized modification
- **Availability**
protection from disruptions in access



Information Security vs. Cybersecurity

- Cybersecurity is a part of information security
- Marketing, vendors & analysts use the term “cyber” too broadly
- Cybersecurity is anything intended to protect enterprises and individuals from intentional attacks

Definition of cybersecurity: the protection of information assets by addressing threats to information processed, stored and transported by internetworked information systems

True or False?

Cybersecurity professionals must demonstrate a high degree of *situational awareness*

True.

Central to this awareness is an understanding of key business and technology factors that affect information security, including

- Business plans and business environment
- Available information technology, security process or systems in particular

Technological Factors that Impact Security

- Platforms and tools used
- Network connectivity (internal, third-party, public)
- Level of IT complexity
- Operational support for security
- User community and capabilities
- New or emerging security tools

Business Factors that Impact Security

- Nature of business
- Risk tolerance
- Security profile
- Industry trends for security
- Mergers, acquisitions and partnerships
 - Consider type, frequency and resulting level of integration
- Outsourcing services or providers

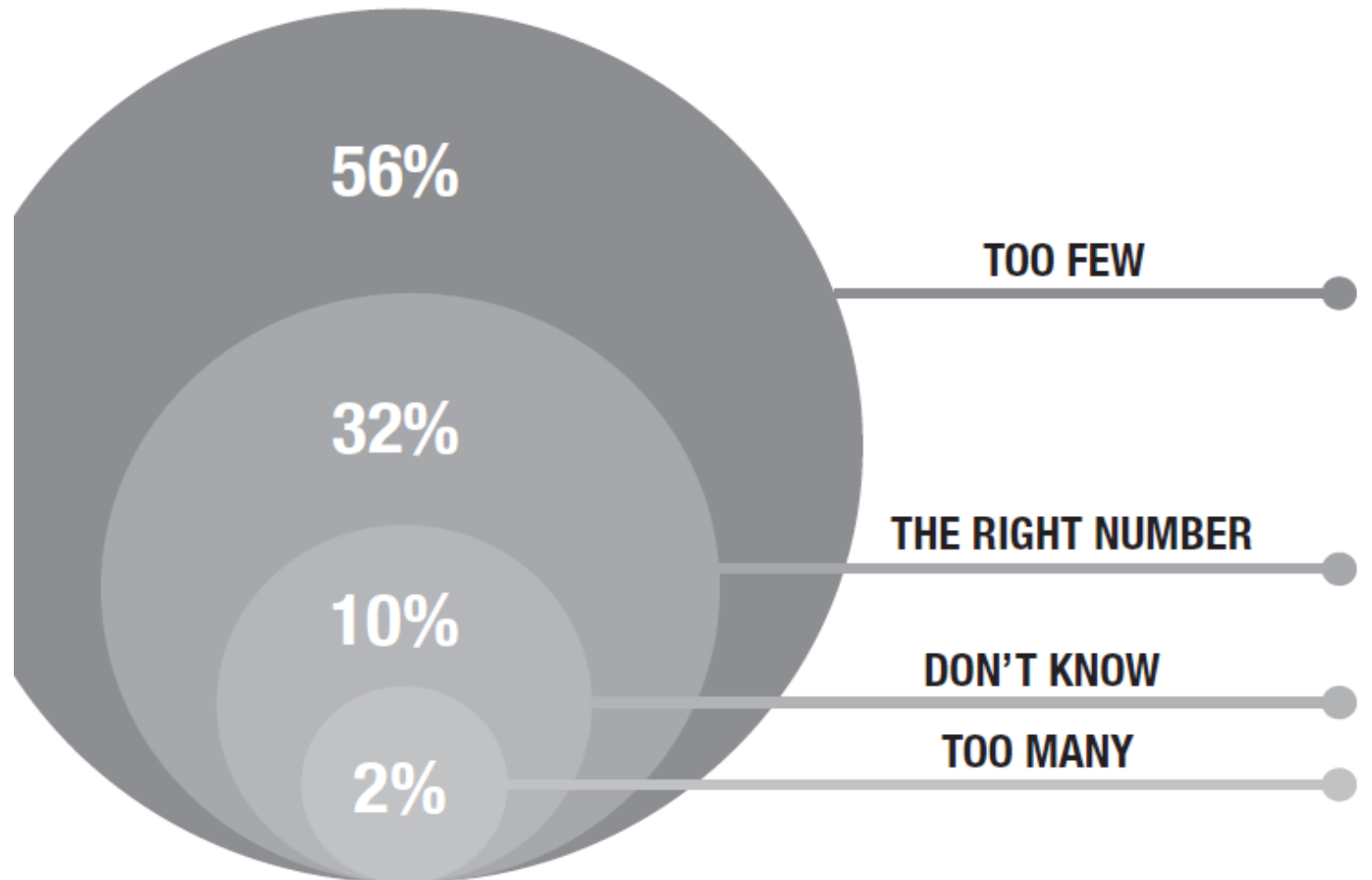
The Cybersecurity Skills Gap

- Constant changes in technology
- Advanced threat vectors
- Endless regulations

Professionals need to be skilled in

- Business
- Technology
- Leadership
- Communication

Exhibit 1.2: Information Security Workforce Outlook



e: Frost & Sullivan, Booz Allen Hamilton, (ISC)², 2013 (ISC)² Global Information Security Workforce Study, 2014

The Cybersecurity Skills Gap

- By 2018 jobs requiring information security professionals will increase by 53% from 2015
- The shortage of skilled professionals is leading to more frequent, costly data breaches
- Skills gaps exist in technical and business aspects of security

James Mickens

*Not Even Close: The State of
Computer Security*

- Galactic Viceroy of Research Excellence
- Harvard University, Authority on all Things & Associate Professor of Computer Science

<https://vimeo.com/135347162>