**Exploring the Foundation of My Information Science and Security Education**

The journey toward a career in information science and cybersecurity requires a solid foundation in both technical and theoretical knowledge. My academic coursework has provided me with the tools necessary to understand core information systems, analyze digital behaviors, protect data, and design ethical security policies. These courses, spanning disciplines such as computer information systems and library and information science, are not only vital for building technical competency but also for developing a deeper understanding of how information is used, accessed, and protected in today’s digital world. Below is a summary of each course and its significance to my future career in cybersecurity and information management.

**Core Information and IT Foundations**

* **LIS 3261 Introduction to Information Science**  
  This course introduces the study of information, its organization, use, and role in society. It emphasizes information technologies and their applications in different contexts.
* **LIS 3353 IT Concepts for Information Professionals**  
  Covers foundational IT knowledge such as hardware, software, data, and internet applications, tailored for professionals managing information resources.

These courses provided the groundwork for understanding how information is processed, stored, and used. As someone aiming for a career in cybersecurity or IT policy, having a deep understanding of information behavior and system architecture is essential. They set the stage for more advanced coursework in security, networking, and policy.

**Security and Systems Architecture**

* **CIS 3360 Principles of Information Security**  
  Explores basic security concepts including risk management, cryptography, and network security.
* **CIS 3367 Architecting Operating Systems Security**  
  Focuses on securing operating systems through access control, user permissions, and system-level defenses.
* **CIS 4204 Ethical Hacking**  
  Teaches penetration testing, vulnerability assessment, and ethical considerations in offensive security.
* **CIS 4361 Information Security Management for IT**  
  Covers risk assessment, incident response, and the development of organizational security policies.
* **CIS 4365 Computer Security Policies**  
  Examines the design, implementation, and evaluation of policies that support information security within organizations.

These courses are related to my career aspirations in cybersecurity. They provided practical skills in ethical hacking and penetration testing, as well as strategic thinking around security management and policy development. Together, they prepared me for roles such as security analyst, systems auditor, or IT compliance officer.

**Information Behavior, Ethics, and Communication**

* **LIS 4204 Information Behaviors**  
  Studies how individuals seek, access, and use information across different environments.
* **LIS 4414 Information Policy and Ethics**  
  Focuses on the legal, ethical, and regulatory frameworks that guide information use and privacy.
* **LIS 4482 Networks and Communication**  
  Introduces concepts in network architecture, protocols, and data communication.

Understanding user behavior and ethical considerations is critical in cybersecurity, especially when dealing with privacy, surveillance, and user consent. These courses helped me see the human side of information science, making me more capable of crafting ethical policies and secure systems that serve users effectively.

**Health Information and Capstone Experience**

* **LIS 4930 Health Information Sources**  
  Explores the organization and evaluation of health-related information for various user groups.
* **LIS 4934 BSIS Senior Capstone**  
  A culminating project that integrates knowledge gained throughout the degree program, often involving research, presentation, and applied problem-solving.

These final courses refined my research skills and allowed me to apply everything I have learned in a practical, often interdisciplinary setting. Understanding health information is especially relevant if I choose to work in health IT, a field that requires strong privacy and ethical considerations.

**Conclusion**

Altogether, the courses I have taken have equipped me with a strong blend of technical knowledge, ethical awareness, and practical skills that align with my career goals in cybersecurity and information systems. From understanding system vulnerabilities to crafting responsible data policies, each course has built upon the last to prepare me for a dynamic and impactful career. The interdisciplinary approach of my education ensures that I can not only protect information but also understand its value and role in society.