CERIAS
The Center for Education and Research in Information Assurance and Security

Security Business Intelligence (SBI) Curriculum - *Blazing the Trail*

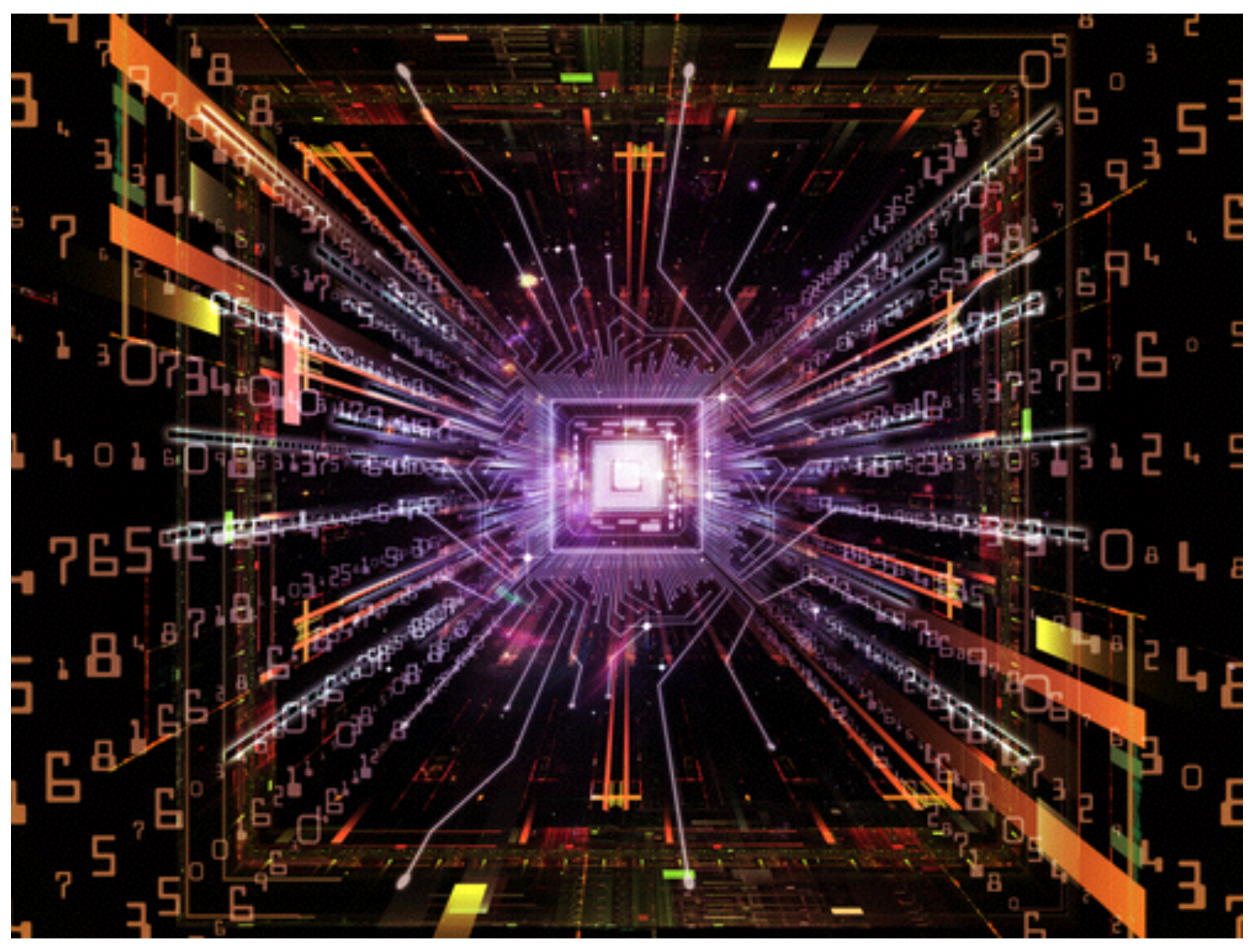
Kelley Misata, Ph.D Student, CERIAS Interdisciplinary Program in Information Security
Supervised by Dr. Marcus K. Rogers

The vision for this project was to create an undergraduate, multi-disciplinary security business intelligence (SBI) curriculum aimed at preparing students for the future of security business intelligence in enterprises. Students will navigate through basic processes, life cycles and data gathering and analysis tools in alignment with SBI critical in an organizational setting. Learning for this course will be conducted through lectures, lab based homework assignments, examinations and a presentation project.

intel Education

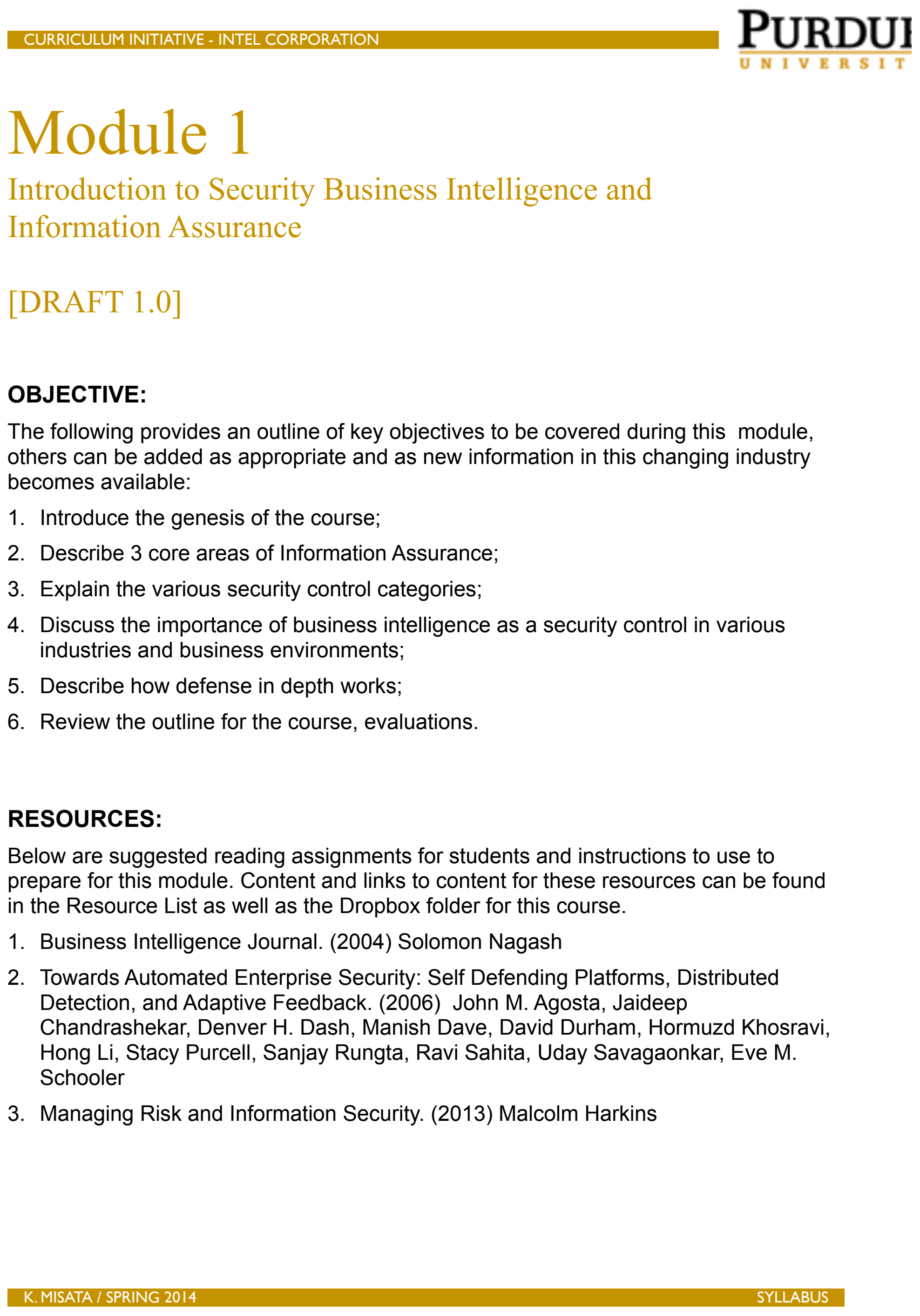
Course Objectives:

- Discuss the current context of Security and Business Intelligence
- Describe the basic process of Security and Business Intelligence
- Explain the Security Intelligence Life Cycle
- Review critical components to SBI including Visualization tools, detective controls, logs, events and alerts
- Discuss key correlations and connections to the business environment including presenting finding to management and other business units;
- Discuss where does privacy and other human factors impact SBI
- Look into the future of SBI



Content in Review:

☑ Complete Course Syllabus
☑ 10 Learning Modules
☑ Key Terminology
☑ Reading List with over 45 references
☑ 6 Additional Course Offerings



PURDUE UNIVERSITY

Module 1

Introduction to Security Business Intelligence and Information Assurance

[DRAFT 1.0]

OBJECTIVE:

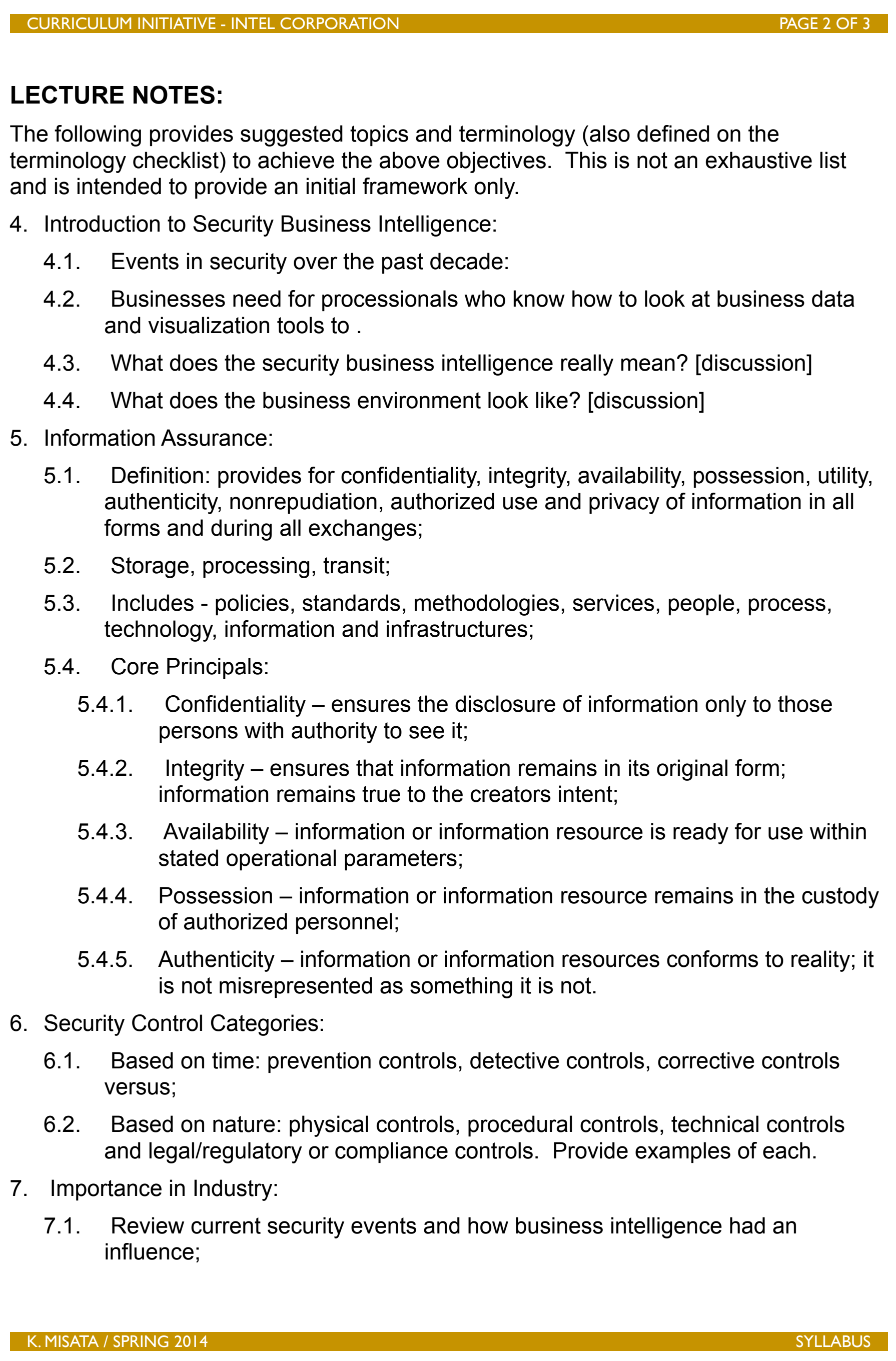
The following provides an outline of key objectives to be covered during this module, others can be added as appropriate and as new information in this changing industry becomes available:

1. Introduce the genesis of the course;
2. Describe 3 core areas of Information Assurance;
3. Explain the various security control categories;
4. Discuss the importance of business intelligence as a security control in various industries and business environments;
5. Describe how defense in depth works;
6. Review the outline for the course, evaluations.

RESOURCES:

Below are suggested reading assignments for students and instructions to use to prepare for this module. Content and links to content for these resources can be found in the Resource List as well as the Dropbox folder for this course.

1. Business Intelligence Journal. (2004) Solomon Nagash
2. Towards Automated Enterprise Security: Self Defending Platforms, Distributed Detection, and Adaptive Feedback. (2006) John M. Agosta, Jaideep Chandrashekar, Denver H. Dash, Manish Dave, David Durham, Hormuzd Khosravi, Hong Li, Stacy Purcell, Sanjay Rungta, Ravi Sahita, Uday Savagaonkar, Eve M. Schooler
3. Managing Risk and Information Security. (2013) Malcolm Harkins



LECTURE NOTES:

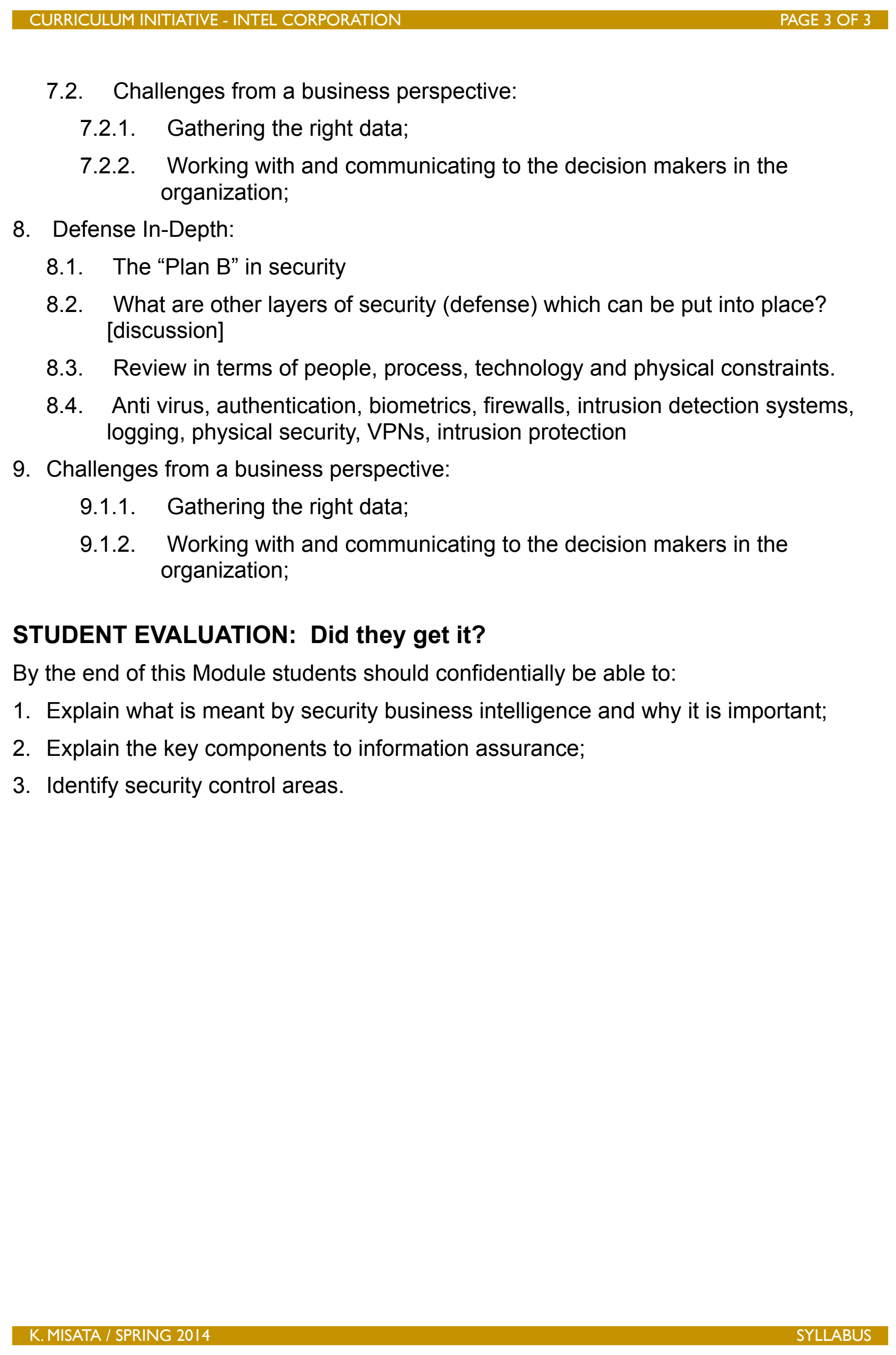
The following provides suggested topics and terminology (also defined on the terminology checklist) to achieve the above objectives. This is not an exhaustive list and is intended to provide an initial framework only.

4. Introduction to Security Business Intelligence:
  4.1. Events in security over the past decade:
  4.2. Businesses need for processionals who know how to look at business data and visualization tools to .
  4.3. What does the security business intelligence really mean? [discussion]
  4.4. What does the business environment look like? [discussion]

5. Information Assurance:
  5.1. Definition: provides for confidentiality, integrity, availability, possession, utility, authenticity, nonrepudiation, authorized use and privacy of information in all forms and during all exchanges;
  5.2. Storage, processing, transit;
  5.3. Includes - policies, standards, methodologies, services, people, process, technology, information and infrastructures;
  5.4. Core Principals:
    5.4.1. Confidentiality – ensures the disclosure of information only to those persons with authority to see it;
    5.4.2. Integrity – ensures that information remains in its original form; information remains true to the creators intent;
    5.4.3. Availability – information or information resource is ready for use within stated operational parameters;
    5.4.4. Possession – information or information resource remains in the custody of authorized personnel;
    5.4.5. Authenticity – information or information resources conforms to reality; it is not misrepresented as something it is not.

6. Security Control Categories:
  6.1. Based on time: prevention controls, detective controls, corrective controls versus;
  6.2. Based on nature: physical controls, procedural controls, technical controls and legal/regulatory or compliance controls. Provide examples of each.

7. Importance in Industry:
  7.1. Review current security events and how business intelligence had an influence;



  7.2. Challenges from a business perspective:
    7.2.1. Gathering the right data;
    7.2.2. Working with and communicating to the decision makers in the organization;

8. Defense In-Depth:
  8.1. The “Plan B” in security
  8.2. What are other layers of security (defense) which can be put into place? [discussion]
  8.3. Review in terms of people, process, technology and physical constraints.
  8.4. Anti virus, authentication, biometrics, firewalls, intrusion detection systems, logging, physical security, VPNs, intrusion protection

9. Challenges from a business perspective:
    9.1.1. Gathering the right data;
    9.1.2. Working with and communicating to the decision makers in the organization;

STUDENT EVALUATION: Did they get it?

By the end of this Module students should confidentially be able to:

1. Explain what is meant by security business intelligence and why it is important;
2. Explain the key components to information assurance;
3. Identify security control areas.

RECOMMENDED ADDITIONAL COURSE OFFERINGS

Getting the Message Across - Reporting and Presenting Results

Predictive Analytics

Extract, Transform, Load

Business Intelligence 200+

Looking thru the Crystal Ball

SBI Team Event

CERIAS

PURDUE UNIVERSITY