Instructional Resources for New IA Instructors

M. E. Kabay, PhD, CISSP-ISSMP
Professor of Computer Information Systems
School of Business & Management
Norwich University1

Abstract

New instructors starting to teach information assurance (IA) courses can face a major challenge, especially if no one has taught such courses in their institution. This paper reviews the Computer Security Handbook (CSH) designed for two undergraduate courses, Introduction to IA and Management of IA in a baccalaureate degree in information assurance2 or for the foundational courses of a Master’s degree in information assurance.3 Resources are freely available to all IA instructors from long-time IA teacher M. E. Kabay. Resources include

- Course descriptions
- Syllabuses
- Extensive PowerPoint slide sets
- Teaching platform design
- Sample memo-type exam questions
- Over 1500 multiple-choice questions
- Recommendations on use of Moodle and Facebook for teaching.

1 Email <mailto:mkabay@norwich.edu>; telephone 1.802.479.7937.
2 See for example <http://profschools.norwich.edu/business/csia/curriculum/>
3 See for example <http://online.norwich.edu/degree-programs/masters/master-science-information-security-assurance/overview>
# Table of Contents

Abstract ............................................................................................................................................ 1  
1 Introduction .................................................................................................................................. 3  
2 The Textbook ............................................................................................................................... 4  
  2.1 Volume I: Introduction to Information Assurance .............................................................. 4  
      2.1.1 Part I: Foundations of Computer Security ............................................................... 4  
  2.2 Part II: Threats and Vulnerabilities ....................................................................................... 4  
      2.2.1 Part III: Prevention: Technical Defenses ................................................................. 4  
  2.3 Volume II: Management of Information Assurance ........................................................... 5  
      2.3.1 Part IV: Prevention: Human Factors ........................................................................ 5  
      2.3.2 Part V: Detecting Security Breaches ........................................................................ 5  
      2.3.3 Part VI: Response and Remediation ........................................................................ 5  
      2.3.4 Part VII: Management’s Role in Security ................................................................. 5  
      2.3.5 Part VIII: Public Policy and Other Considerations ................................................... 5  
3 IS340, Introduction to Information Assurance ........................................................................ 6  
  3.1 Course Description ................................................................................................................ 6  
  3.2 Course Objectives ................................................................................................................ 6  
  3.3 Methods of Assessment ........................................................................................................ 6  
      3.3.1 Term Project: 20% of final grade .............................................................................. 6  
      3.3.2 Review Quizzes: 15% of final grade ......................................................................... 7  
      3.3.3 Mid-term Multiple-Choice Exam: 15% of final grade ............................................. 7  
      3.3.4 Final Memo Question Exam: 10% of final grade ...................................................... 7  
      3.3.5 Final Multiple-Choice Exam: 20% of final grade .................................................... 7  
      3.3.6 Term-Paper Presentation: 5% of final grade ........................................................... 7  
      3.3.7 Extra Work for Extra Points: .................................................................................. 7  
  3.4 Syllabus .................................................................................................................................. 8  
  3.5 Sample Memo-Exam Instructions and Questions .................................................................. 9  
      3.5.1 Mid-Term Exam Questions ...................................................................................... 9  
      3.5.2 Final-Exam Questions ............................................................................................ 10  
4 IS342 Management of Information Assurance ........................................................................ 12  
  4.1 Course Description ................................................................................................................ 12  
  4.2 Course Objectives ................................................................................................................ 12  
  4.3 Syllabus .................................................................................................................................. 13  
  4.4 Sample Memo-Exam Questions .......................................................................................... 14  
      4.4.1 Mid-Term Exam Questions ...................................................................................... 14  
      4.4.2 Final-Exam Questions ............................................................................................ 15  
5 NUoodle2 (variant of Moodle) Teaching Platform .................................................................. 17  
  5.1 Introductory Section .............................................................................................................. 17  
  5.2 Typical Weekly Section ........................................................................................................ 18  
6 Multiple-Choice Question Bank ............................................................................................... 19  
7 PowerPoint Slides ....................................................................................................................... 22  
8 General Resources ..................................................................................................................... 23  
9 Using Facebook as a Repository ............................................................................................... 24  
10 Concluding Remarks ............................................................................................................... 25  
11 Works Cited ............................................................................................................................... 26
1 Introduction

In 1999, I was asked by Wiley publishers to be the technical editor of the *Computer Security Handbook*, then in its third edition.\(^4\) I agreed provided I could restructure the fourth edition\(^5\) of the text to widen its scope and to serve as a teaching textbook. The work continued has with the fifth\(^6\) and sixth\(^7\) editions.

In 2001, I was hired by the School of Business and Management at Norwich University to create a baccalaureate program in information assurance. In 2002, I was asked to establish a master's program in information assurance in the School of Graduate and Continuing Education.

Over this decade and more of intensive work, I have created PowerPoint presentations for students in my information assurance courses, all of which are freely available to instructors for use as-is or as a basis for adaptation to their own needs. In addition, I have created 1500 multiple-choice questions suitable for use as weekly quizzes or exams using spreadsheets that can automatically create GIFT format questions for easy use with teaching platforms such as Moodle.

I've kept track of mid-term and final-exam questions that use memo format to provide practice for students in explaining security concepts and issues to non-technical managers. Many students have commented over the years that these exercises were of direct benefit when they entered the work force.

The associated term-paper guidelines, topic ideas, samples and grading standards may also be helpful to instructors.

---

\(^4\) (Hutt, Bosworth and Hoyt 1995)
\(^5\) (Bosworth and Kabay, Computer Security Handbook 2002)
\(^6\) (Bosworth, Kabay and Whyne, Computer Security Handbook 2009)
\(^7\) (Bosworth, Kabay and Whyne, Computer Security Handbook 2014)
2 The Textbook

2.1 Volume I: Introduction to Information Assurance

2.1.1 Part I: Foundations of Computer Security
1. Brief History and Mission of Information Systems Security
2. History of Computer Crime
3. Toward a New Framework for Information Security
4. Hardware Elements of Security
5. Data Communications and Information Security
6. Network Topologies, Protocols and Design
7. Encryption
8. Using a Common Language for Computer Security Incident Information
9. Mathematical Models of Computer Security
10. Understanding Studies and Surveys of Computer Crime
11. Fundamentals of Intellectual Property Law

2.2 Part II: Threats and Vulnerabilities
12. The Psychology of Computer Criminals
13. The Dangerous Information Technology Insider: Psychological Characteristics and Career Patterns
14. Information Warfare
15. Penetrating Computer Systems and Networks
16. Malicious Code
17. Mobile Code
18. Denial-of-Service Attacks
19. Social Engineering and Low-Tech Attacks
20. Spam, Phishing and Trojans: Attacks Meant to Fool
21. Web-Based Vulnerabilities
22. Physical Threats to the Information Infrastructure

2.2.1 Part III: Prevention: Technical Defenses
23. Protecting the Information Infrastructure
24. Operating Systems Security
25. Local Area Networks
26. Gateway Security Devices
27. Intrusion Detection and Intrusion Prevention Devices
28. Identification and Authentication
29. Biometric Authentication
30. E-Commerce and Web Server Safeguards
31. Web Monitoring and Content Filtering
32. Virtual Private Networks and Secure Remote Access
33. 802.11 Wireless LAN Security
34. Securing VoIP
35. Securing P2P, SMS and Collaboration Tools
36. Securing Stored Data
37. PKI and Certificate Authorities
38. Writing Secure Code
39. Software Development and Quality Assurance
40. Managing Software Patches and Vulnerabilities
41. Antivirus Technology
42. Protecting Digital Rights: Technical Approaches
2.3 Volume II: Management of Information Assurance

2.3.1 Part IV: Prevention: Human Factors

43. Ethical Decision Making and High Technology
44. Security Policy Guidelines
45. Employment Practices and Policies
46. Vulnerability Assessment
47. Operations Security and Production Controls
48. Email and Internet Use Policies
49. Implementing a Security-Awareness Program
50. Using Social Psychology to Implement Security Policies
51. Security Standards for Products

2.3.2 Part V: Detecting Security Breaches

52. Application Controls
53. Monitoring and Control Systems
54. Security Audits, Standards, and Inspections
55. Cyber Investigation

2.3.3 Part VI: Response and Remediation

56. Computer Security Incident Response Teams
57. Data Backups and Archives
58. Business Continuity Planning
59. Disaster Recovery
60. Insurance Relief
61. Working with Law Enforcement

2.3.4 Part VII: Management’s Role in Security

62. Risk Assessment and Risk Management
63. Management Responsibilities and Liabilities
64. U.S. Legal and Regulatory Security Issues
65. The Role of the ISO
66. Developing Security Policies
67. Developing Classification Policies for Data
68. Outsourcing and Security

2.3.5 Part VIII: Public Policy and Other Considerations

69. Privacy in Cyberspace: U.S. and European Perspectives
70. Anonymity and Identity in Cyberspace
71. Healthcare Security and Privacy
72. Legal and Policy Issues of Censorship and Content Filtering
73. Expert Witnesses and the Daubert Challenge
74. Professional Certification and Training in Information Assurance
75. The Future of Information Assurance
3 IS340. Introduction to Information Assurance

3.1 Course Description
This course provides an overview of design considerations involved with the security of site design. The course will also provide an understanding of the Levels of Trust and system accreditation/certification processes. Life cycle management of software, hardware, and physical plant, from planning through destruction will be examined and reinforced using case studies. Additionally understanding of the variety of security systems involving computers and networks and an ability to evaluate vulnerabilities will be discussed. Prerequisite IS228 or permission of instructor. (3 Credits)

3.2 Course Objectives
By the end of this course, students will be able to discuss the following issues at a management level:

- Recognize, define and use the technical terminology of information assurance (IA).
- Name and define the fundamental concepts of IA.
- Describe models and key elements of information warfare.
- Recognize, name, define and discuss computer crime techniques; present countermeasures.
- Describe and discuss criminal-hacker subculture.
- Recognize, name, define, and discuss techniques of denial-of-service (DoS) attacks and countermeasures.
- Recognize, name, define, and discuss physical (facilities) security vulnerabilities and defenses.
- Recognize, name, define, and discuss identification and authentication techniques.
- Discuss specific security issues pertaining to voice and data networks.
- Recognize, name, define, and discuss fundamentals of firewalls and of intrusion-detection systems.
- Recognize, name, define, and discuss fundamentals of modern cryptography.
- Evaluate requirements and techniques for backing up, archiving, storing, managing, and destroying electronic records.

3.3 Methods of Assessment
All assignments and quizzes are submitted using NUoodle2. Deadlines for each assignment are posted in NUoodle and on the class syllabus.

Responding punctually to professional responsibilities is part of the maturation of students. To encourage promptness, late submissions for any of the essay exams and assignments will result in reduction of grades by 10% per day from the total score allotted. However, because of the constraints on NUoodle quizzes, the time limits on quizzes have to be definite; therefore, quizzes close at their deadlines and cannot be taken or retaken after closure.

3.3.1 Term Project: 20% of final grade
Students will write a 3,500 ± 500 word research paper on a suitable topic to be selected in conjunction with the instructor. Post your topic suggestion in the public discussion group on NUoodle 2. Instructor approval helps to avoid the problem of discovering that you have picked a topic worthy of a textbook and also prevents duplicate topics. Don’t hesitate to work with your instructor to review draft versions before you prepare your final version. Strict deadlines are listed in the syllabus for submission of the topic, preliminary references, one-page outline with references, first draft, and final draft. Failure to comply with these deadlines will result in a 10% penalty imposed on the final grade for the term project; the instructor will not evaluate late submissions, with potentially grave consequences for the next phase of the evaluations. Submit your files via NUoodle2 no later than the deadlines listed there; use DOCX, DOC, RTF, or ODT but not PDF files for your submission. Read the detailed explanation of requirements for the project.
3.3.2 **Review Quizzes: 15% of final grade**

Using NUoodle, there will be 13 sets of weekly quizzes (each individual quiz will cover a week’s assigned readings). These open-book, automatically graded quizzes will test for concepts and technical vocabulary and must be completed in 30 minutes or less. These quizzes open on Thursday mornings (00:05) in the week the material is discussed and will close at the end of Sunday night (23:55) in the following week.

3.3.3 **Mid-term Multiple-Choice Exam: 15% of final grade**

The mid-term exam will be an open-book multiple-choice exam taken via NUoodle 2. Coverage: Weeks 1 to 6.

3.3.4 **Mid-term Memo Question Exam: 10% of final grade**

At mid-term and at the end of the course, once all the chapter readings are completed, students will complete an open-book take-home assignment with five management-level 400 ± 100 memorandum responding to realistic questions raised by managers querying an information systems security officer (ISSO) or chief information security officer (CISO) about security issues. Exam coverage is Weeks 1 through 5 of the course.

3.3.5 **Final Multiple-Choice Exam: 20% of final grade**

The final open-book multiple-choice exam similar to the weekly quizzes but covering all the material in the course. The exam will be offered via NUoodle2.

3.3.6 **Final Memo Question Exam: 15% of final grade**

At the end of the course, once all the chapter readings are completed, students will complete an open-book take-home assignment with five management-level 400 ± 100 word memoranda responding to realistic questions raised by managers querying an information systems security officer (ISSO) or chief information security officer (CISO) about security issues. Exam coverage is Weeks 6 through 13 of the course.

3.3.7 **Term-Paper Presentation: 5% of final grade**

Students will create a narrated PowerPoint lecture for their term-paper topic for posting on NUoodle and will then participate in a class discussion of their research (with or without their PowerPoint). Grading will include the quality of the content and the professionalism of the presentation.

3.3.8 **Extra Work for Extra Points:**

Students may submit extra work for extra points on their final grade with permission of the instructor. For example, the instructor will agree to accept suitable short essays such as summaries of interesting incidents, articles or books relevant to the course materials.

- The rate granted for extra work is 1 point added to the final grade for 500 words of professional-grade writing. Thus a 1,000 word essay could improve the final grade by 2 points.
- Particularly good articles may be considered for publication in collaboration with the student author.
- Contributions to the online discussions can generate 0.1 pt on the final score per good contribution with references or an intelligent response to a posted message. (MAX 10 pts)
- Leading a discussion in class can earn 1 point added to the final grade. Student lecturers must rehearse their proposed discussion plan with the instructor for approval and possible improvement.
3.4 Syllabus

The Syllabus is created using an Excel template. Versions for the first\(^8\) and second\(^9\) courses are available for download.

---

\(^8\) [http://www.mekabay.com/courses/academic/norwich/is340/is340_syllabus.xlsx](http://www.mekabay.com/courses/academic/norwich/is340/is340_syllabus.xlsx)

\(^9\) [http://www.mekabay.com/courses/academic/norwich/is342/is342_syllabus.xlsx](http://www.mekabay.com/courses/academic/norwich/is342/is342_syllabus.xlsx)
3.5 Sample Memo-Exam Instructions and Questions

- Answer the following questions as four memoranda responding to requests from colleagues.
- Your responses should each be 350-450 words. Longer responses are acceptable but an unnecessary use of your valuable time.
- Type your responses in a single DOCX, DOC, RTF or ODT file and upload it to the mid-term upload section on NUoodle no later than 23:55 Thu 3 Oct 2013.
- This is an OPEN-BOOK EXAM. Feel free to use additional reference materials as you see fit but be sure to provide references for anything you quote using author, date, title, journal (if not a book) or Web site URL, and pages if appropriate.
- It is OK to offer the correspondent a reference including the URL for one good place for further reading about the issue but IT IS NOT REQUIRED THAT YOU DO SO HERE.
- Points are given for individual questions as 10 (Wonderful! Can be circulated in public!), 9 (Very good! Can be circulated internally in the organization!), 8 (Well, OK, but it's not as good as it should be – errors, omissions) or 0 (Unacceptable: gross errors of writing or factual error[s]).
- Always restate the question in a simple way as part of your answer.
- NEVER be rude or arrogant in your response. You get ZERO for a rude response.

3.5.1 Mid-Term Exam Questions

1. FROM: Jeff Bridges, CEO  
   TO: YOU as CISO  
   RE: What is the mission of the information security group?
   We have a presentation to the Board of Directors next week and I’d like to have a concise summary of your view of the mission of your security department. What are the key aspects of our information that are at risk and how do you see the most important functions of the security team in our organization?

2. FROM: Cindy Morgan, CFO  
   TO: YOU as CISO  
   RE: Historical and current threats to financial data in recent decades
   My colleagues at last month’s Association of Number Crunchers (ANC) meeting in Oahu were discussing the evolution of threats to our financial data and financial systems over the last 40 years. For example, we talked about the famous Equity Funding fraud of the early 1970s. I’d like to continue the discussion with our own staff in the Department of Finance but I don’t have enough specific examples to present. Please summarize five important examples of threats to security of our company financial systems; you may use bullet points to describe specific incidents in brief to back up your choices.

3. FROM: Peter Jurasik, COO  
   TO: YOU as CISO  
   RE: Using PGP
   I understand that you are instituting a well-known program, PGP, to provide a simple mechanism for securing internal document transfers. I’ve been told that the new system enables us to sign documents electronically so that we know for sure who’s sent them and also to let us be sure that no one has altered a document that has been sent electronically from one person to another. The problem is that I don’t understand how it works, which I always find irritating. Please explain to me what is meant by the “public key” and the “private key” – and how an encryption key can possibly be public!

4. FROM: Lisette Kremer, Director of Sales  
   TO: YOU as CISO  
   RE: Website failure
The CIO has referred me to you to explain how it is possible for us to lose five hours of Web access to our own Website – at an estimated loss of sales of around $385,000 give or take a few thousand dollars. As you very well know, we depend absolutely on our Website for sales – 94% of our total revenue last year was from online purchases. So how on earth could we possibly succumb to a “DDoS”? We surely don’t run DOS, do we? Didn’t that operating system go out in the 1980s? So what happened?? And is there any way that our site can defend itself against such a disaster in future?

3.5.2 Final-Exam Questions

1. FROM: N. Portman, CIO  
   TO: YOU as CISO  
   RE: Parkerian Hexad and Common Language for Security Incidents

I attended a lecture yesterday at the 14th International Conference on Hypercomplex Systems and one of the presenters used two sets of concepts I hadn’t encountered before: the “Parkerian Hexad” and Howard’s “Common Language” for security incidents. I will be reporting to the Board of Directors next week and I need to know the basics of these schemas. What are they and why are they useful? Give me an example of how to apply them by analyzing last month’s hacker break-in (the one where that middle-European group installed a rootkit on our administrative server and stole 110,000 customer records).

2. FROM: H. Weaving, VP Marketing  
   TO: YOU as CISO  
   RE: Information Warfare Today

As you know, our company has been heavily involved with Department of Defense contracts in recent years. I’ll be meeting with some officers next week to discuss the need for our new line of products involving cyber situational awareness. Please provide me with a succinct definition of information warfare, the current state of knowledge about who are key adversaries are, and a summary of the techniques being used to challenge our national infrastructure information systems.

3. FROM: S. Rea, Director of Network Services  
   TO: YOU as CISO  
   RE: Denial of Service Attacks

In the last two weeks, response time has been plummeting. We are seeing major delays in serving up Web pages to our customers and we are now losing significant business, with terrible results on our bottom line. I need to understand how it is possible for these attacks to go unprosecuted by our law enforcement officials and what, if anything, we can do about stopping them.

4. FROM: S. Fry, COO  
   TO: YOU as CISO  
   RE: Operating Systems Security

Yesterday at the executive meeting, you said that you and your colleagues on the IT side of the house have been studying how to “harden” (I think that’s the word you used) the operating system for our integrated supervisory control and data acquisition (SCADA) systems for the water treatment plants we serve. Can you give me a sense of what the key issues are in evaluating and improving operating systems?

5. FROM: J. Hurt, VP Engineering  
   TO: YOU as CISO  
   RE: Secure Coding

As you know, we are moving forward with phase II of the development project for our new wireless neural control systems for the F-45 bomber deployment. In recent months, I have been copied on several of your memos to the development team in which you allude to “secure coding standards.” Please explain your judgement of the top five issues that you see as critical to our software development in this phase.
FROM: T. Piggott-Smith, Director of Administration
TO: YOU as CISO
RE: Backups

Hello again – nice to see you at the picnic a week ago. Have you recovered from swallowing that golf ball?
Anyway, some of the secretaries in the executive offices were talking about the lecture you gave us a couple of months ago about computer safety and we realized that we were not absolutely clear about the different kinds of backups that you mentioned. I think you talked about full, differential, incremental and some other name I forget. You also mentioned the advantages of keeping numbered versions of documents during the development cycle. Can you explain what the types of backups are and why you would use one instead of another? Thanks! And don’t swallow any more golf balls!
4 IS342 Management of Information Assurance

The Methods of Assessment are similar to those for IS340.

4.1 Course Description

This course focuses on management of the information assurance process. Topics include human factors in reducing security breaches, security incident detection and response, remediation, management’s role in information assurance, and other considerations in framing and implementing information assurance policies. The final section reviews current topics of particular interest and activity in the field of information assurance. IS342 may be taken before taking IS340. All specifics of topics, schedule and deadlines are in the IS342 Syllabus. Prerequisite IS228 or permission of instructor. (3 Credits)

4.2 Course Objectives

The goal of the course is to provide a foundation for practical work and further study in information assurance. By the end of the course, students should be able intelligently and usefully to discuss these topics at a management level: Fundamentals of intellectual property law

- Software development and quality assurance
- Managing patches and vulnerabilities
- Principles of ethical decision-making in the information technology field.
- Guidelines for effective security policies.
- Effective employment practices relevant to security in conjunction with human resources staff.
- Vulnerabilities assessments
- Suitable operations security controls on production systems.
- Appropriate-use policies for Internet access and e-mail.
- Effective security-awareness programs.
- Social psychology to implement security policies effectively.
- Standards for security products
- Application-program security controls
- Monitoring and control systems
- Audit and control of information systems.
- Cyber investigations
- Computer security incident response team management
- Data backup and recovery procedures to support business continuity and disaster response plans.
- Business continuity plans.
- Disaster recovery plans.
- Collaboration with law enforcement in data gathering, preservation and forensic analysis.
- Modern principles of risk assessment and risk management.
- Management responsibilities for information assurance.
- US legal and regulatory issues
- The role of the CISO
- Developing security policies
- Outsourcing security
- Privacy online
- Security in the medical informatics field.
- Censorship and content filtering in the USA and overseas
# 4.3 Syllabus

## IS 342 Management of Information Assurance

### Spring 2014 SYLLABUS

**Prof M. E. Kabay, PhD, CISSP-ISMP**

**Office:** Dewey 209 / Tel. 479-7937 / Skype: mkebay / mailto:mkebay@norwich.edu

**CLASS MEETS TR 10:50:03 - 12:04:57 IN DEWEY 211**

<table>
<thead>
<tr>
<th>Week</th>
<th>Date</th>
<th>#</th>
<th>TOPICS &amp; CHAPTERS FROM CS5H</th>
<th>NLoodle QUIZ #</th>
<th>Speakers via WebEx or Skype</th>
<th>Exams &amp; Term Paper Deadlines</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Tue, Jan 14</td>
<td>1</td>
<td>Introduction to the course and the subject matter: Course Description + Term-Paper Guidelines + CATA + SQ3R</td>
<td>0</td>
<td></td>
<td>Explore possible topics; use instructor as resource to bounce ideas around</td>
</tr>
<tr>
<td></td>
<td>Thu, Jan 16</td>
<td>2</td>
<td>Toward a New Framework for Information Security 11 Intellectual Property Law</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>2</td>
<td>Tue, Jan 21</td>
<td>3</td>
<td>39 Software Development &amp; Quality Assurance</td>
<td>CH1,11</td>
<td>Jay Winer (in person)</td>
<td>Project Topic Must be Approved</td>
</tr>
<tr>
<td></td>
<td>Thu, Jan 23</td>
<td>4</td>
<td>40 Managing Patches &amp; Vulnerabilities</td>
<td>CH14,44</td>
<td>Don Holden</td>
<td>Intial Research on Project</td>
</tr>
<tr>
<td></td>
<td>Thu, Jan 30</td>
<td>6</td>
<td>44 Security Policy Guidelines</td>
<td>CH39,40</td>
<td></td>
<td></td>
</tr>
<tr>
<td>3</td>
<td>Tue, Feb 04</td>
<td>7</td>
<td>45 Employment Practices and Policies</td>
<td>CH40,44</td>
<td>K. Rustaph</td>
<td>MT Essay &amp; MC Exams Open</td>
</tr>
<tr>
<td></td>
<td>Thu, Feb 11</td>
<td>9</td>
<td>47 Operations Security</td>
<td>CH40,46</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Thu, Feb 13</td>
<td>10</td>
<td>48 E-mail and Internet Use Policies</td>
<td>CH47,48</td>
<td></td>
<td></td>
</tr>
<tr>
<td>4</td>
<td>Tue, Feb 18</td>
<td>11</td>
<td>49 Security Awareness</td>
<td>CH40,50</td>
<td></td>
<td>MT Essay &amp; MC Exams Close</td>
</tr>
<tr>
<td></td>
<td>Thu, Feb 20</td>
<td>12</td>
<td>50 Social Psychology and Information Security</td>
<td>CH51,52</td>
<td></td>
<td></td>
</tr>
<tr>
<td>5</td>
<td>Tue, Feb 25</td>
<td>13</td>
<td>51 Security Standards for Products</td>
<td>CH55,56</td>
<td></td>
<td>MT Essay &amp; MC Exams Open</td>
</tr>
<tr>
<td></td>
<td>Thu, Feb 27</td>
<td>14</td>
<td>52 Application Controls</td>
<td>CH55,56</td>
<td></td>
<td></td>
</tr>
<tr>
<td>6</td>
<td>Tue, Mar 04</td>
<td>15</td>
<td>53 Monitoring and Control Systems</td>
<td>CH55,56</td>
<td></td>
<td>Work on Term Project</td>
</tr>
<tr>
<td></td>
<td>Thu, Mar 06</td>
<td>16</td>
<td>54 Security Audits, Standards and Inspections</td>
<td>CH55,56</td>
<td></td>
<td></td>
</tr>
<tr>
<td>7</td>
<td>Tue, Mar 11</td>
<td>-</td>
<td>Spring Break</td>
<td></td>
<td></td>
<td>Opt. Draft Review Open for Project Reports</td>
</tr>
<tr>
<td></td>
<td>Thu, Mar 13</td>
<td>-</td>
<td></td>
<td></td>
<td></td>
<td>Opt. Draft Review Ends</td>
</tr>
<tr>
<td>8</td>
<td>Tue, Mar 18</td>
<td>17</td>
<td>55 Cyber Investigations</td>
<td>CH55,56</td>
<td>Michael Krausz</td>
<td>Complete Term Project Report</td>
</tr>
<tr>
<td></td>
<td>Thu, Mar 20</td>
<td>18</td>
<td>56 Computer Security Incident Response Teams</td>
<td>CH55,56</td>
<td>Michael Krausz</td>
<td></td>
</tr>
<tr>
<td>9</td>
<td>Tue, Mar 25</td>
<td>19</td>
<td>57 Backups (also studied in IS340)</td>
<td>CH55,56</td>
<td>Michael Krausz</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Thu, Mar 27</td>
<td>20</td>
<td>58 Business Continuity Planning</td>
<td>CH55,56</td>
<td>Michael Krausz</td>
<td></td>
</tr>
<tr>
<td>10</td>
<td>Tue, Apr 01</td>
<td>21</td>
<td>59 Disaster Recovery Planning</td>
<td>CH55,56</td>
<td>Michael Krausz</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Thu, Apr 03</td>
<td>22</td>
<td>62 Risk Management</td>
<td>CH55,56</td>
<td>Michael Krausz</td>
<td></td>
</tr>
<tr>
<td>11</td>
<td>Tue, Apr 08</td>
<td>23</td>
<td>63 Management Responsibilities &amp; Liabilities</td>
<td>CH55,56</td>
<td>Michael Krausz</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Thu, Apr 10</td>
<td>24</td>
<td>64 Developing Security Policies</td>
<td>CH55,56</td>
<td>Michael Krausz</td>
<td></td>
</tr>
<tr>
<td>12</td>
<td>Tue, Apr 15</td>
<td>25</td>
<td>65 Role of CISO</td>
<td>CH55,56</td>
<td>Michael Krausz</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Thu, Apr 17</td>
<td>26</td>
<td>66 Developing Security Policies</td>
<td>CH55,56</td>
<td>Michael Krausz</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Thu, Apr 22</td>
<td>27</td>
<td>67 Classification Policies</td>
<td>CH55,56</td>
<td>Michael Krausz</td>
<td></td>
</tr>
<tr>
<td>13</td>
<td>Tue, Apr 15</td>
<td>25</td>
<td>68 Outsourcing</td>
<td>CH55,56</td>
<td>Michael Krausz</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Thu, Apr 17</td>
<td>26</td>
<td>69 Privacy in Cyberspace</td>
<td>CH55,56</td>
<td>Michael Krausz</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Thu, Apr 24</td>
<td>27</td>
<td>71 Medical Records Security</td>
<td>CH55,56</td>
<td>Michael Krausz</td>
<td></td>
</tr>
<tr>
<td>14</td>
<td>Tue, Apr 29</td>
<td>28</td>
<td>72 Censorship &amp; Content Filtering</td>
<td>CH55,56</td>
<td>Michael Krausz</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Thu, May 01</td>
<td>29</td>
<td>Student research presentations</td>
<td>CH55,56</td>
<td>Michael Krausz</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>CH55,56</td>
<td>Michael Krausz</td>
<td></td>
</tr>
</tbody>
</table>

---

Copyright © 2014 M. E. Kabay. All rights reserved.
4.4 Sample Memo-Exam Questions

4.4.1 Mid-Term Exam Questions

1. From: William Smith, Director of Marketing  
   To: YOU as CISO  
   Re: Limitations on Web content  
   I am deeply disturbed by your recent notification to my staff that they are not permitted to use materials taken from public Web sites in our marketing materials without obtaining written permission from the copyright owners. The Web is public: anything posted on it is by definition in the public domain and does not require permission to re-use freely. Kindly rescind your regulation and stop interfering in our creative process.

2. From: Mary McDonnell, Director of Internal Programming  
   To: YOU as CISO  
   Re: Automated SQA tools  
   Was very interested in your comment at yesterday’s Software Engineering Group meeting about the value of automated testing tools, especially when developing mission-critical software. Please explain your thinking.

3. From: Jeff Goldblum, COO  
   To: YOU as CISO  
   Re: Delay in installing “non-critical” patches  
   You have established a policy which requires patches released on Patch Tuesday to be prioritized according to need and urgency. Your policy also establishes a minimum delay of a week for critical patches (except in emergencies) and of a month for non-critical patches. I do not understand the reasoning behind these policies – shouldn’t we install patches instantly all the time?

4. From: Margaret Colin, CEO  
   To: YOU as CISO  
   Re: Security aspects of hiring procedures  
   Great seeing you at the company picnic last week. Some of the Board members were asking me about the new hiring policies you have put into place for protecting our corporate interests; can you summarize the top five of them and explain the reasoning behind each one?

5. From: Randy Quaid, CIO  
   To: YOU as CISO  
   Re: Penetration Testing  
   How are you going to establish a rational basis for penetration testing of our networks and systems? Aren’t you worried about damaging morale among our employees if the pen-testers show them up as idiots using social engineering techniques? And what are we going to do when we find the inevitable holes in our security – fire people?

6. From: Vivica A. Fox, CFO  
   To: YOU as CISO  
   Re: New policies about e-mail  
   I'm totally confused about the rules you presented at the Executive Meeting yesterday for using the TO, CC, BCC, and SUBJECT fields of an e-mail message. What does it all mean? And what did you mean by using the body of the e-mail message effectively? Who cares about setting such formal policies for e-mail, anyway – why bother?
4.4.2 Final-Exam Questions

1. From:  Mira Furlan, Chief Operating Officer  
To:  YOU as CISO  
Re:  Cyberinvestigation and collaborating with GBI

Hi! It was great seeing you at the company picnic last week on Epsilon III! Weren’t those pickled gurling eggs great? Anyway, I was talking with Marcus Cole in the facilities security group yesterday and he said that you’re currently collaborating with the Galactic Bureau of Investigation on the recent case of theft of industrial secrets about the White Star fleet. As you can imagine, we Minbari are terribly concerned about this breach; indeed, the Warrior Caste is all for attacking Earth right away even though we don’t know the full extent of the breach or how it was accomplished.

Can you summarize for me how your cyber-investigation team is handling the evidence from the station’s computers? How are you extracting the data with assurance that you have not modified them? And what is meant by “chain of custody” – I just heard about that this cycle – in this situation? Finally, what determined your decision to go beyond depending on Security Chief Garibaldi’s office for the investigation and involving the GBI?

Thanks!

2. From:  Peter Jurasik, Chief Financial Officer  
To:  YOU as CISO  
Re:  New approach to determining backup policies

Hello! We have not met yet in person, but I have heard many good things about you from my colleagues on the Board of Directors of the Allied Planets in the cycles since I joined the Board. I understand that you have a comprehensive new approach to configuring and scheduling backups that you and your colleagues have been working on for the last few months. I have a long-standing interest in backups, so I wonder if I could trouble you to lay out for me briefly a comprehensive overview of your plans. For example, I hear that you are very strong on such issues as tailoring the type of backup to the specific requirements of each operational system and adjusting the period of retention of such backups. What are the types of backup you are considering? How do you decide how often to perform them? What determines the retention period of the backups? Where are you proposing to store them and why?

I look forward to your summary, which I will share immediately with Lennier and Talia in the policy committee of the Board.

3. From:  Claudia Christian, Chief Executive Officer  
To:  YOU as CISO  
Re:  Working with the Centauri

I was deeply disturbed by the news that you are seriously considering a proposal from Ambassador Londo Molari to work with a Centauri company on some of our critical computer applications.

One of our Narn colleagues (Ambassador G’Kar, actually) described the performance of the Narn companies providing outsourcing as “A bunch of Squirlings running after mating pasthel grubs.” Some of us feel that we may lose control over highly sensitive data about the plans for a new Babylon VI station; access to these plans may well give the Shadows significant advantage in their military planning. Now that you have been named to replace the Chief Information Security Officer (I understand that the Vorlons insisted on his replacement and that he is now growing mushrooms out of his eye sockets), how are you proposing to evaluate the proposal to prevent industrial espionage and other security incidents that could result? What are your key proposals for evaluating the risks of outsourcing to the Centauri and why are you proposing them? This project is a high priority and I look forward to reading your report.
4. From: Richard Biggs, Chief Medical Officer  
   To: YOU as CISO  
   Re: Medical records security

Hey! Great to participate with you in the SocketBall contest last week. I tell you, your left-handed spincrack really faked me out! That sucker must have been traveling at lightspeed; I swear I thought I saw some relativistic Lorentz-Fitzgerald field expansion!

Anyway, yesterday I was talking to one of the grotzholes from EarthGov (Sheridan was disgusted to see him) and he was nattering on and on about being sure that we perform a security audit on our medical systems security. Can you send me an explanation of the key elements of the medical systems that you will be looking at? What are the major elements of medical information security that the EarthGov auditors will be looking for? I know that you have worked on the history of medical information security that dates all the way back to the 20th century USA, so feel free to make reference to those famous laws and regulations.

Thanks. And don’t think you’re going to win our next match at SocketBall! See ya next week!

5. From: Andreas Katsulas, Chief Information Officer  
   To: YOU as CISO  
   Re: Committee on Information Infrastructure

First, I want to thank you for your leadership of the Committee on Backups and Business Continuity (CBBC). I have heard excellent reports of your performance from several members of the CBBC and these are perfectly consistent with my already high opinion of your competence and commitment to excellence. The Vorlons have explicitly praised your work by saying, “His egg will rapture the fornagel manogradly.” We’re still working on what that means, but it seems positive according to our computerized phoneme analysis.

I would like you to summarize the changes you are proposing to our operations security (OPSEC). For example, please explain what you mean by distinguishing between production systems and non-production systems. Tell me in detail about the security principles you’ve mentioned in several memos such as separation of duties, change-control, maintaining a trusted operating system, and data validation as part of OPSEC.

I need your report by no later than Friday morning – and please be sure that it is readable to members of our Board of Directors, among whom I will circulate it.

Again, keep up the good work!

6. From: Tracy Scoggins, Director of Personnel Resources  
   To: YOU as CISO  
   Re: Your pending promotion – need CISO Job Description

First, my congratulations on your promotion to Chief Operating Officer! I know that you will enjoy the new challenges you will face and that you will succeed in your new position. I just need your help in crafting the job description for your current position – after all, you have made some radical improvements over the last six years, and the old description no longer fits. Keep in mind that the Minbari are real sticklers for documentation for every hiring operation. So I’d really appreciate your summarizing the key points about the CISO’s primary responsibilities. If you have general information about ideal orientation, include that too. Please feel free to comment in more detail on any points you wish so we in the Personnel group can better understand your view of our needs as we screen candidates.
5  NUoodle2 (variant of Moodle) Teaching Platform

Detailed teaching objectives, review questions, and pointers to the PowerPoint slide decks (in PPTX and PDF formats) are posted on an implementation of Moodle called NUoodle2. Weekly review quizzes, the mid-term multiple-choice exam, and the final multiple-choice exam are loaded on the platform, as are versions with twice as much time allowance to support students with learning disabilities as identified by the Academic Achievement Center. The following screenshots show samples of how the material is presented.

5.1  Introductory Section

The News forum allows permanent posting of announcements; they can also be sent to all participants by email.

Error Reports are an opportunity for continuous performance improvement. Students offering corrections and suggestions for improvement are assigned extra points on their final grade.
5.2 Typical Weekly Section

Week 1

Introduction to the course and the subject matter: Course Description + Term-Paper Guidelines + CATA + SQ3R.

- CSH 3 Toward a New Framework for Information Security
- CSH 11 Intellectual Property Law

COURSE NOTES & REVIEW QUESTIONS

- CSH 5 Ch 3 Toward a New Framework for Information Security
- CSH 5 ch 53 new framework review.pdf
- Supplement to CSH 11: Overview of Intellectual Property Law
- CSH 6 ch 11 ip law review.pdf

WEEKLY QUIZZES

Read the Course Documentation

- Quiz 0: Course Information and resources - RTFM Quiz #1
- Quiz 0: Course Information and resources - RTFM Quiz #2
- Quiz 0: Course Information and resources - RTFM Quiz #3

Quizzes on Assigned Chapter Readings

- Quiz CSHE Chapter 3
- Quiz CSHE Chapter 11
6  Multiple-Choice Question Bank

The following screenshot shows part of the question bank that is of greatest concern to the instructor:

The question bank is an EXCEL XLSX file with the following column headings:

- Course (340, 342, 34x = both)
- CH – chapter number in textbook
- Q# – question number
- QUESTION – text
- CORRECT ANSWER
- (INCORRECT ANSWERS) b, c, d, e
- Any dupes? – automatically scans all answers in a question and shows “OK” if there are no duplications or “ERR” if two or more answers are identical

Not shown is the following column:

- GIFT format – automatically combines question text and all answers into a format such as the following:

  A computer criminal specializing in social engineering stole VAX VMS source code and eventually went underground for several years to escape prosecution, eventually becoming a prominent author and speaker on defending against social engineering techniques. {=Kevin Mitnick ~Jerry Neal Schneider ~Eric Corley ~Josef Ingressia ~none of the other choices is correct}
The QUESTION column can be used to extract the questions for use in a review document. For input to the Moodle teaching system, the instructor copies the GIFT format versions of the questions and answers and imports them into Moodle, as shown in the following screenshots:
The imported questions can then be assigned to a quiz or to an exam.
7  PowerPoint Slides

Detailed slide sets based on the CSH are freely available to anyone. Most slides have been enhanced over the years by incorporation of images, many of which are from the iClipart collection, which supplies licensed access to about 8 million images for about $40 a year. PDF handouts are included for all chapter files.

10 Repositories at <http://www.mekabay.com/courses/academic/norwich/is340/is340_lectures/index.htm> and <http://www.mekabay.com/courses/academic/norwich/is342/is342_lectures/index.htm>

11 (Vital Imagery Ltd. 2014)
8 General Resources

New instructors may benefit from having access to term-paper guidelines, term-paper topic ideas, term-paper outline and sample, memo-exam sample, and grading standards for exams and for term papers.

The following image from the IS342 course page shows these resources.

---

12 <http://www.mekabay.com/courses/academic/norwich/research.pdf>
13 <http://www.mekabay.com/courses/academic/norwich/is342/is342_ideas_for_term_paper.pdf>
17 <http://www.mekabay.com/courses/academic/norwich/essay-exam_standards.jpg>
18 <http://www.mekabay.com/courses/academic/norwich/term-paper_standards.jpg>
19 <http://www.mekabay.com/courses/academic/norwich/is342/index.htm>
9 Using Facebook as a Repository

For up-to-date information that can serve students in a single course, the Moodle features provide an excellent way of uploading links to useful articles, papers, and videos. However, if material is useful in more than one course, posting links several times may become onerous. In addition, the contents of forums (a typical way of posting links) are not ordinarily copied and transferred from one course to another using the Moodle import function.

Facebook, on the other hand, can be accessible to anyone with a Facebook account who wishes to check a public page. A recent study suggests that 73% of the US adults with Internet access have a Facebook account. Another demographic study suggests that almost a quarter of US residents between 18 and 24 years of age have Facebook accounts (although the percentage seems to be dropping).

It is not necessary to force students to friend the instructor for them to be able to see everything (s)he posts. In addition, many news services and aggregators such as ZITE provide easy ways of sharing the links at the click of a button.

20 https://www.facebook.com/michkabay
21 (Duggan and Smith 2013)
22 (Saul 2014)
23 http://zite.com/
10 Concluding Remarks

Anyone may download and use PowerPoint files and their PDF equivalents from any of the author’s courses in accordance with the copyright restrictions posted on the Web site.24

Instructors wishing to access Excel files with multiple-choice examination questions and examples of review questions for the two undergraduate courses described above or any others25 may write the author using their institutional email address and a link showing their inclusion in the official faculty of their institution. Send the request to <mailto:mkabay@norwich.edu> with a subject line similar to “REQUESTING COURSE MATERIALS.”

---

24 See <http://www.mekabay.com/copyright.htm>
25 See <http://www.mekabay.com/courses/index.htm>
11 Works Cited


