

Instructional Resources for New IA Instructors

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

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> >

Instructional Resources for New IA Instructors

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 Mid-term Memo Question Exam: 10% of final grade.....	7
3.3.5 Final Multiple-Choice Exam: 20% of final grade	7
3.3.6 Final Memo Question Exam: 15% of final grade.....	7
3.3.7 Term-Paper Presentation: 5% of final grade.....	7
3.3.8 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

Instructional Resources for New IA Instructors

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 edition⁵ of the text to widen its scope and to serve as a teaching textbook. The work continued has with the fifth⁶ and sixth⁷ 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)

Instructional Resources for New IA Instructors

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

Instructional Resources for New IA Instructors

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

Instructional Resources for New IA Instructors

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 \pm 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.

Instructional Resources for New IA Instructors

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 \pm 100 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 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 \pm 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.

Instructional Resources for New IA Instructors

3.4 Syllabus

The Syllabus is created using an Excel template. Versions for the first⁸ and second⁹ courses are available for download.

IS 340 Information Assurance Fundamentals								
Fall 2013 Syllabus / D211 MW 15:00:03-16:14:57								
Prof M. E. Kabay, PhD, CISSP-ISSMP								
Office: Dewey 209 / Tel (802) 479-7937 / E-mail: mkabay@norwich.edu / Skype: mekabay								
TEXT: Bosworth, Kabay & Whyne (2009). <i>Computer Security Handbook, 5th Edition. Volume 1. Wiley (ISBN 0-471-71652-9).</i>								
Week	Day	Date	TOPICS	Readings: CSHS Chapters...	QUIZ ON	Exams	Term Project Deadlines	
1	Mon	26-Aug	Introduction to the course, research, SQ3R, CATA	SQ3R: On Writing: CATA	Quizzes use	Symbols: » receive submit »		
	Wed	28-Aug	History and Mission of Information System Security & History of Computer Crime	1 & 2	Noodle 2			
2	Mon	2-Sep	LABOR DAY					
	Wed	4-Sep	Parkerian Hexad & Common Language for Incidents	3 & 8	Wk 1			
3	Mon	9-Sep	Hardware & Data Comm	4, 6			topic for approval »	
	Wed	11-Sep	History of Cryptography & Secret-Key Cryptography	7	Wk 2			
4	Mon	16-Sep	Public-Key Cryptography & Recent Developments	7		» mt memo questions Wk 1-5		
	Wed	18-Sep	IW & Penetrating computer systems and networks	14 & 15	Wk 3			
5	Mon	23-Sep	Malicious/Mobile Code	16 & 17			» 6 references	
	Wed	26-Sep	Denial of Service & Social Engineering	18 & 19	Wk 4			
6	Mon	30-Sep	Spam, Phishing, Trojans & Web-based Vulnerabilities	20 & 21		mt memos »		
	Wed	2-Oct	Physical & Facilities Security (1)	22	Wk 5			
7	Mon	7-Oct	Physical & Facilities Security (2)	23		» mt mc exam Wk 1-6	» 1 page outline w/ 10 refs	
	Wed	9-Oct	Operating Systems Security & LANs	24 & 25	Wk 6			
8	Mon	14-Oct	Gateway Security Devices	26		» mt memos graded		
	Wed	16-Oct	Intrusion Detection & Intrusion Prevention	27	Wk 7			
9	Mon	21-Oct	Identification & Authentication	28			» 1st draft	
	Wed	23-Oct	E-Commerce Security	30	Wk 8			
10	Mon	28-Oct	Virtual Private Networks & Secure Remote Access	32				
	Wed	30-Oct	Wireless Security & Securing VoIP	33 & 34	Wk 9			
11	Mon	4-Nov	Backups & Securing Stored Data	57 & 36			» draft w/ comments	
	Wed	6-Nov	PKI / Certificate Authorities	37	Wk 10			
12	Mon	11-Nov	Writing Secure Code	38		» final memo questions		
	Wed	13-Nov	Antivirus Technology	41	Wk 11			
13	Mon	18-Nov	Mathematical Models of Computer Security	9			» final version	
	Wed	20-Nov	Course Review		Wk 12			
	Mon	25-Nov	THANKSGIVING VACATION					» narrated PPTX
	Wed	27-Nov						
14	Mon	2-Dec	Student Presentations					
	Wed	4-Dec				Wk 13		
15	Mon	9-Dec					final memos »	project grade & edits »
		TBD	FINAL MULTIPLE CHOICE EXAM VIA NUODLE2					

⁸ http://www.mekabay.com/courses/academic/norwich/is340/is340_syllabus.xlsx

⁹ http://www.mekabay.com/courses/academic/norwich/is342/is342_syllabus.xlsx

Instructional Resources for New IA Instructors

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

Instructional Resources for New IA Instructors

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.

Instructional Resources for New IA Instructors

6. **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!

Instructional Resources for New IA Instructors

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

- | | |
|--|---|
| <ul style="list-style-type: none">• 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 | <ul style="list-style-type: none">• 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-ISSMP							
Office: Dewey 209 / Tel. 479-7937 / Skype: mekabay / mailto:mekabay@norwich.edu							
CLASS MEETS TR 10:50:03 - 12:04:57 IN DEWEY 211							
Week	Date	#	TOPICS & CHAPTERS FROM CSH5	NUoodle QUIZ #	Speakers via WebEx or Skype	Exams & Term Paper Deadlines	
1	Tue, Jan 14	1	Introduction to the course and the subject matter: Course Description + Term-Paper Guidelines + CATA + SQ3R	0		Explore possible topics; use instructor as resource to bounce ideas around	
	Thu, Jan 16	2	3 Toward a New Framework for Information Security 11 Intellectual Property Law				
2	Tue, Jan 21	3	39 Software Development & Quality Assurance	1: CH 3,11			
	Thu, Jan 23	4	40 Managing Patches & Vulnerabilities				
3	Tue, Jan 28	5	43 Ethical Decision Making in High Technology	2: CH 39,40		Project Topic Must be Approved	
	Thu, Jan 30	6	44 Security Policy Guidelines				
4	Tue, Feb 04	7	45 Employment Practices and Policies	3: CH43,44	Jay Wisner (in person)	Initial Research on Project	
	Thu, Feb 06	8	46 Vulnerability Assessment				
5	Tue, Feb 11	9	47 Operations Security	4: CH45,46	Don Holden	MT Essay & MC Exams Open	
	Thu, Feb 13	10	48 E-mail and Internet Use Policies				
6	Tue, Feb 18	11	49 Security Awareness	5: CH47,48	K Rudolph Mani Akella		
	Thu, Feb 20	12	50 Social Psychology and Information Security				
7	Tue, Feb 25	13	51 Security Standards for Products	6: CH49,50		MT Essay & MC Exams Close	
	Thu, Feb 27	14	52 Application Controls				
8	Tue, Mar 04	15	53 Monitoring and Control Systems	7: CH51,52		Work on Term Project	
	Thu, Mar 06	16	54 Security Audits, Standards and Inspections				
	Tue, Mar 11 Thu, Mar 13	- -	Spring Break				
9	Tue, Mar 18	17	55 Cyber Investigations 61 Working with Law Enforcement	8: CH53,54	Peter Stephenson	Opt. Draft Review Open for Project Reports	
	Thu, Mar 20	18	56 Computer Security Incident Response Teams		Michael Krausz		
10	Tue, Mar 25	19	57 Backups (also studied in IS340)	9: CH55,61,56		Opt. Draft Review Ends	
	Thu, Mar 27	20	58 Business Continuity Planning				
11	Tue, Apr 01	21	59 Disaster Recovery Planning	10: CH57,58	Michael Miora	Complete Term Project Report	
	Thu, Apr 03	22	62 Risk Management		Michael Krausz		
12	Tue, Apr 08	23	63 Management Responsibilities & Liabilities 65 Role of CISO	11: CH59,62	Eric Whyne	Term Project Report Due	
	Thu, Apr 10	24	66 Developing Security Policies 67 Classification Policies				
13	Tue, Apr 15	25	68 Outsourcing 69 Privacy in Cyberspace	12: 63,65,66,67			
	Thu, Apr 17	26	71 Medical Records Security 72 Censorship & Content Filtering				
14	Tue, Apr 22	Student research presentations		13: 68,69, 71,72		Final Essay and MC Exams Open	
	Thu, Apr 24						
15	Tue, Apr 29						Final Exams Close
	Thu, May 01						

Instructional Resources for New IA Instructors

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?

Instructional Resources for New IA Instructors

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 Scurlings 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.

Instructional Resources for New IA Instructors

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

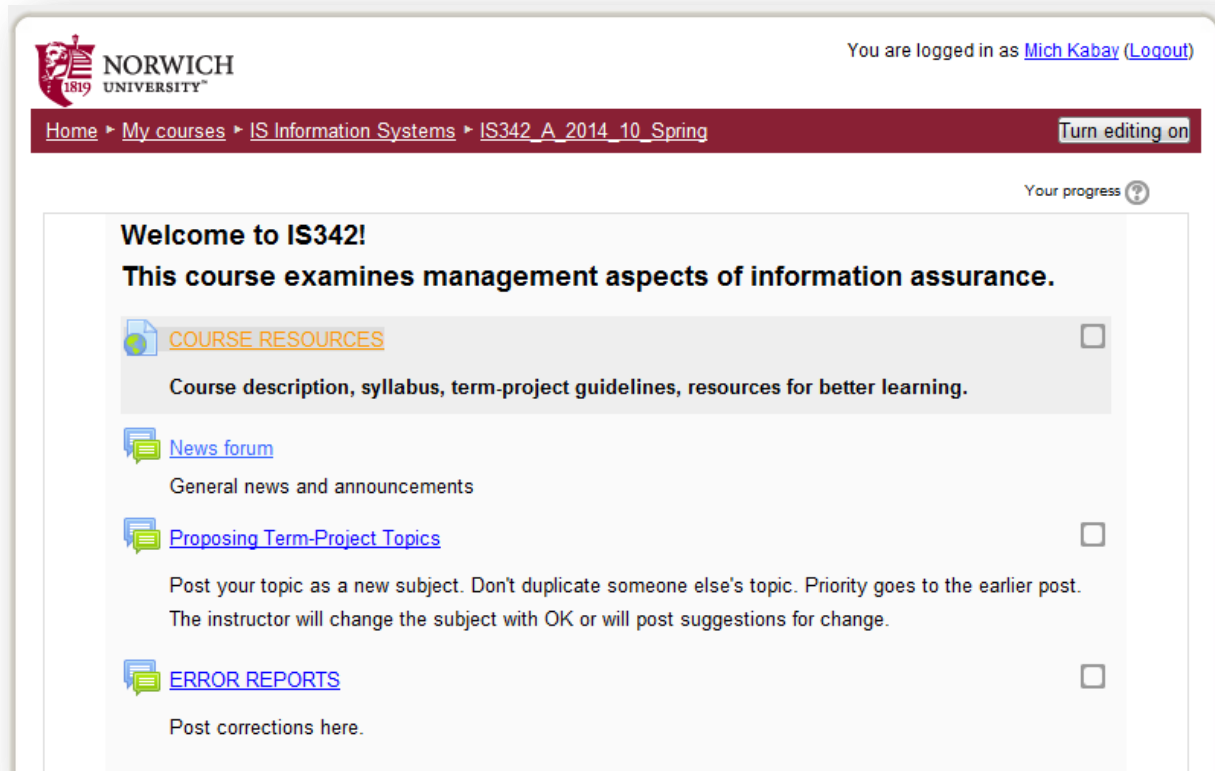
First, my congratulations on your promotion to Chief Operating Officer! I know that you will enjoy the new challenges you will face and that you will succeed in your new position. I just need your help in crafting the job description for your current position – after all, you have made some radical improvements 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.

Instructional Resources for New IA Instructors

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.

Instructional Resources for New IA Instructors


5.2 Typical Weekly Section

13 January - 19 January
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


 [IS342 WEEK 1 DISCUSSIONS](#) ☐


Topics relevant to the week's discussions to be posted by instructor & by students. Students may post new items at any time during course.


 [Introduction to the course](#) ☐

COURSE NOTES & REVIEW QUESTIONS ☐

 [CSH5 Ch 3 Toward a New Framework for Information Security](#)


 [csh5_ch_03_new-framework_review.pdf](#) ☐

 [Supplement to CSH5 Ch 11: Overview of Intellectual Property Law](#)


 [csh5_ch_11_ip_law_review.pdf](#) ☐


WEEKLY QUIZZES ☐


Read the Course Documentation ☐


 [Quiz 0: Course information and resources -- RTFM Quiz #1](#)


Pushing students to READ THE **** MANUAL.
30 questions, 60 minutes. You may also take RTFM Quiz #2 and RTFM Quiz #3 if you are dissatisfied with your grade -- the highest grade of the three counts.
Deadline 23:55 SUN 9 FEB 2014.

 [Quiz 0: Course information and resources -- RTFM Quiz #1 -- AAC](#)


 [Quiz 0: Course information and resources -- RTFM Quiz #2](#) ☐

 [Quiz 0: Course information and resources -- RTFM Quiz #2 -- AAC](#) ☐


 [Quiz 0: Course information and resources -- RTFM Quiz #3](#) ☐


 [Quiz 0: Course information and resources -- RTFM Quiz #3 -- AAC](#) ☐

Quizzes on Assigned Chapter Readings ☐


 [Quiz CSH5 Chapter 3](#) ☐


Parkerian Hexad. 15 questions, 30 minutes, 1 try. Deadline 23:55 SUN 9 FEB 2014.

 [Quiz CSH5 Chapter 3 -- AAC](#) ☐

 [Quiz CSH5 Chapter 11](#) ☐

Intellectual Property Law. 30 questions, 60 minutes, 1 try. Deadline 23:55 MON 10 FEB 2014 as apology for having STUPIDLY PUT A PASSWORD ON THIS.
< slap > [hits forehead with palm of hand]
< thud > [falls off ergonomic chair]
< scabble, scabble > [climbers back on chair]

 [Quiz CSH5 Chapter 11 -- AAC](#) ☐

 [Quiz CSH5 Chapter 11 -- AAC2](#) ☐

Instructional Resources for New IA Instructors

6 Multiple-Choice Question Bank

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

D2Insert blank line between every question after exporting to DOCX file and before saving as TXT file using UTF8 format.										
A	B	C	D	E	F	G	H	I	J	
EXAM QUESTION SELECTION ENGINE				DO NOT TERMINATE ANSWERS WITH PERIODS. NEVER INCLUDE THE = or ~ SIGNS IN QUESTIONS OR ANSWERS.						
CSH5				Insert blank line between every question after exporting to DOCX file and before saving as TXT file using UTF8 format.						
ANSWERS:										
Course (340, 342, 34x = both)	CH	Q#	QUESTION	CORRECT ANSWER	b	c	d	e		
340	0	66	Which step in the recommended study method is this? At the end of your study period, and then at the end of the week, ask yourself to answer questions about what you are studying using your own questions and the course notes or chapter review questions provided.	Review	Read	Recite	Survey	none of the other choices is correct	OK	
340	0	67	What is Professor Kabay's Skype address?	mekabay	mkabay	mekabay@norwich.edu	mekabay@gmail.com	none of the other choices is correct	OK	
340	0	68	Where can you find Professor Kabay's office hours posted?	all of the other choices are correct except _none_ ... is correct	on his office door	as a PDF file on his Web site	as a JPG file on his Web site	using a link on NUoodle	OK	
340	0	69	What is Professor Kabay's phone number?	802-479-7937	802-497-9737	802-485-7937	he doesn't own a phone	none of the other choices is correct	OK	
340	0	70	When is it OK to call Prof Kabay on the phone?	any time of day or night – his phone doesn't ring in his home but only in his offices	from 08:00 to 18:00 only	only in the afternoons	on days whose day of the month plus the number of the month add up to 42	none of the other choices is correct	OK	
340	0	71	What is Professor Kabay's Norwich e-mail address?	mekabay@norwich.edu	mekabay@norwich.edu	labaym@norwich.edu	all of the other choices are correct except the one that says _none_ is correct	none of the other choices is correct	OK	
340	0	72	Where is Professor Kabay's Norwich office?	Dewey 209	Dewey 223b	Web 115	Ainsworth 209	none of the other choices is correct	OK	
342	0	1	How many class sessions may you miss without permission and still stay in IS342?	2	0	1	3	4	OK	
342	0	2	Where are the IS342 class assignments and links to reference materials located?	NUoodle	Library of Congress	mekabay.com page for class only	in a meat locker under the stairs in Dewey	none of the other choices is correct	OK	
342	0	3	When should students first read or at least scan the assigned materials for IS342?	before coming to class where the materials will be discussed	after the class where the materials have been discussed	during the class where the materials are being discussed	never	none of the other choices is correct	OK	
342	0	4	When should students arrive in class for IS342 to avoid being registered as absent?	anytime from 10 minutes before class is scheduled to begin or within a minute or so of the scheduled start	anytime from 10 minutes before class is scheduled to begin to 10 minutes after the scheduled start	anytime from 10 minutes before class is scheduled to begin to 15 minutes after the scheduled start	anytime from 10 minutes before class is scheduled to begin to 1 second after the scheduled start	none of the other choices is correct	OK	

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 dups? – 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}

Instructional Resources for New IA Instructors

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:

NORWICH UNIVERSITY 1819

You are logged in as [Mich Kabay](#) ([Logout](#))

[Home](#) ▶ [My courses](#) ▶ [IS Information Systems](#) ▶ [IS342 A 2014 10 Spring](#) ▶ [Question bank](#) ▶ [Import](#)

Import questions from file ?

File format

- * ? ☐ Aiken format
- ? ☐ Blackboard
- ? ☐ Blackboard V6+
- ? ☐ Embedded answers (Cloze)
- ? ☐ Examview
- ? ☒ Gift format
- ? ☐ Learnwise format
- ? ☐ Missing word format
- ? ☐ Moodle XML format
- ? ☐ WebCT format

General

Import category ? 57 Backups ▼

☒ Get category from file ☒ Get context from file

Match grades ? Error if grade not listed ▼

Stop on error ? Yes ▼

Import questions from file


Import* Choose a file... Maximum size for new files: 50MB

[csh5_ch_57_backups_gift.txt](#)

[Import](#)

Instructional Resources for New IA Instructors

The imported questions can then be assigned to a quiz or to an exam.

**NORWICH**
UNIVERSITY

You are logged in as [Mich Kabay](#) ([Logout](#))

[Home](#) > [My courses](#) > [IS Information Systems](#) > [IS342_A_2014_10_Spring](#) > [24 March - 30 March](#) > [QUIZ_CSH5_CH_57: BACKUPS](#) > [Preview](#)

Quiz navigation

[1](#) [2](#) [3](#) [4](#) [5](#) [6](#) [7](#)

[8](#) [9](#) [10](#)

[Finish attempt...](#)

Time left 0:19:55

[Start a new preview](#)

Add a block

Add...

Question 1
Not yet answered
Marked out of 1.00
[Flag question](#)
[Edit question](#)

The best place to store backups offsite is in

Select one:
☐ a. a data vault
☐ b. a bank vault
☐ c. the CIO's fire-resistant safe
☐ d. none of the other choices is correct
☐ e. an employee's home

Question 2
Not yet answered
Marked out of 1.00
[Flag question](#)
[Edit question](#)

One terabyte has

Select one:
☐ a. 1,024 megabytes
☐ b. 1E9 bytes
☐ c. 1,024 megabits
☐ d. 1E15 bytes
☐ e. 1,024 gigabytes

Question 3
Not yet answered
Marked out of 1.00
[Flag question](#)
[Edit question](#)

One megabyte has

Select one:
☐ a. 1,024 bits
☐ b. 1,000,000 bits
☐ c. 1,024 bytes
☐ d. 1,000,000 bytes
☐ e. 1,024 kilobytes

Question 4
Not yet answered
Marked out of 1.00
[Flag question](#)
[Edit question](#)

DVD disks using single-sided, double-layer technology have a data-storage capacity of about

Select one:
☐ a. 8.5 EB
☐ b. none of the other choices is correct
☐ c. 8.5 GB
☐ d. 8.5 MB
☐ e. 8.5 TB

Instructional Resources for New IA Instructors

7 PowerPoint Slides

Detailed slide sets based on the CSH are freely available to anyone.¹⁰ 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.¹¹ PDF handouts are included for all chapter files.


IS 342 Class Notes

Backups

CSH5 Chapter 57
Backups
M. E. Kabay & Don Holden


Topics

- Backup Bloopers
- Definitions and Needs
- Strategies
- Archives, Maintenance and Retention
- Storage
- Disposal
- Costs
- Optimizing Frequency



Backup Bloopers


➤ BerkshireNet	➤ US Customs
➤ Margot Kidder	➤ US National Archives
➤ Digital Technologies Group	➤ MIT "Cheating Scandal"
➤ Amtrak Reservations	➤ Office of the Vice President of the USA
➤ Newcastle University Prof	➤ Norwegian Banks
➤ Sun Valley Ski Resort	➤ Swisscom Mobile GSM Network Failure
➤ Stanford University Grad School of Business	➤ Macomb County (Michigan) Sheriff's Dept
➤ McAfee's QuickBackup 2.04	➤ Electronic Voting Machines



BerkshireNet

Feb 96 -- RISKS 17.83


- BerkshireNet, Pittsfield, MA
 - ❑ Swastikas and racist messages
 - ❑ Masqueraded as provider's administrator
 - ❑ Erased data on two computers
 - ❑ Shut down system
- Down 12 hours
- ❑ no current backup
- ❑ older deleted files restored
- ❑ but several days of data lost



Margot Kidder

Sept 96 -- People Online via RISKS 18.46


- Computer virus was last straw
- Led to nervous breakdown
- Unidentified virus apparently destroyed only copy of her book
- No backup



Digital Technologies Group

Oct 96 -- AP

- Digital Technologies Group lost all computer files and backups
 - ❑ US\$17,000 direct costs
 - ❑ loss of months of work
 - ❑ 1-week shutdown
 - ❑ seriously damaged credibility as ISP
- Disgruntled ex-employee
- Alleged perpetrator arrested



Copyright © 2014 M. E. Kabay1All rights reserved.

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)

Instructional Resources for New IA Instructors

8 General Resources

New instructors may benefit from having access to term-paper guidelines,¹² term-paper topic ideas,¹³ term-paper outline¹⁴ and sample,¹⁵ memo-exam sample,¹⁶ and grading standards for exams¹⁷ and for term papers.¹⁸

The following image from the IS342 course page¹⁹ shows these resources.

IS342 Management of IA -- Spring 2014

Course Description.

This course examines management aspects of information assurance, including standards for security products, policy guidelines, security awareness, ethical decision-making, employment practices and policies, operations security and production controls, e-mail and Internet use policies, working with law enforcement, using social psychology to implement security policies, and auditing computer security. The course includes sections on detection of security breaches, methods of remediation such as computer emergency quick-response teams, backups and archives, business continuity planning, disaster recovery planning and insurance. Students examine fundamentals of management responsibilities and liabilities and risk assessment methodologies. The course ends with a review of current hot topics in the field such as medical records security, censorship, privacy, and anonymity. IS340 (Introduction to Information Assurance) is recommended but not required as a prerequisite. Required for BCSLA degree.

Spring 2014: Tuesdays and Thursdays from 10:50:03 to 12:04:57 in Dewey 211

[Home Page](#)

(PDF FILES unless otherwise indicated)

[Contact info](#)

[Courses](#)

[CV](#)

[Cyberwatch](#)

[Ethics](#)

[InfoSec Perception](#)

[IYIR](#)

[Methods](#)

[NetworkWorld Archive](#)

[Opinion](#)

[Ops Mgmt](#)

[Overviews](#)

[Security Mgmt](#)

[Course description](#) -- detailed assignments, grading, standards, requirements, policies, rewards, penalties, and also the Secret of Life, the Universe and Everything.

[Syllabus/schedule](#) -- day-by-day listing of every required reading, quiz, exam, and deadline.

[Term-Paper Guidelines](#) -- how to avoid falling into a swamp of errors.

[Term-Paper Topic Ideas](#) -- suggestions, just suggestions

[Term-Paper Outline](#) -- example from Anna Knapp of organizing one's research

[Term-Paper Sample](#)
used by kind permission of alumna Anna Knapp NU ('07)

[Memo-Exam Sample](#) written by Gregory Antonellis in 2013

[Grading Standards for Essay Exams \(JPG\)](#)

[Grading Standards for Term Papers \(JPG\)](#)

[Lecture files](#) (PowerPoint PPTX and Acrobat PDF)

[Presentation Schedule 2013](#) [PDF](#)

[Instructor Office Hours / Schedule](#) [JPG](#)

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 >

¹⁴ < http://www.mekabay.com/courses/academic/norwich/model_outline.pdf >

¹⁵ < http://www.mekabay.com/courses/academic/norwich/model_paper.pdf >

¹⁶ < http://www.mekabay.com/courses/academic/norwich/memo-exam_sample.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> >

Instructional Resources for New IA Instructors

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.²⁰ A recent study suggests that 73% of the US adults with Internet access have a Facebook account.²¹ 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).²²

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 ZITE²³ 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/> >

Instructional Resources for New IA Instructors

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> >

Instructional Resources for New IA Instructors

11 Works Cited

- Bosworth, S., and M. E. Kabay. *Computer Security Handbook*. 4th. 1 vols. Wiley, 2002.
- Bosworth, S., M. E. Kabay, and E. Whyne . *Computer Security Handbook*. 6th. 2 vols. Wiley, 2014.
- Bosworth, S., M. E. Kabay, and E. Whyne. *Computer Security Handbook*. 5th. 2 vols. Wiley, 2009.
- Duggan, M., and A. Smith. "Social Media Update 2013." *Pew Research Internet Project*. 12 30, 2013. <http://www.pewinternet.org/2013/12/30/social-media-update-2013/> (accessed 04 16, 2014).
- Hutt, A. E., S. Bosworth, and D. B. Hoyt, . *Computer Security Handbook*. 3rd. 1 vols. Wiley, 1995.
- Saul, D. J. "3 Million Teens Leave Facebook In 3 Years: The 2014 Facebook Demographic Report." *iSTRATEGYLABS [sic]*. 01 15, 2014. <http://istrategylabs.com/2014/01/3-million-teens-leave-facebook-in-3-years-the-2014-facebook-demographic-report/> (accessed 04 16, 2014).
- Vital Imagery Ltd. *iCLIPART.com*. 2014. <http://www.iclipart.com/index2.php> (accessed 03 23, 2014).