Brandeis University
Graduate Professional Studies

Rabb School of Continuing Studies

Course Syllabus

I. Course Information

1. Course Name

Principles of Computer Incident Response and Investigations

2. Course Number

RIAS 125

3. Course Start & End Dates; Online Course Week Start/End Days

The course week runs from Wednesday to Tuesday, with assignments due by 23:59 Tuesday night, or as specified by the instructor.

Course Start: 07/19/17

Course End: 09/26/17

Mid-term due: 08/29/17

Final due: 09/27/17

4. Instructor's Name and Contact Information

- Louw Smith, M.Sc
- Adjunct instructor, Graduate Professional Studies, Rabb School of Continuing Studies, Brandeis University
- Email – louw.smith@brandeis.edu
- Office Hours/Availability – By appointment, available between 6-10PM EST

**Please note, that email will always be the best way to contact me.

5. Document Overview

This syllabus contains all relevant information about the course: its objectives and outcomes, the grading criteria, the texts and other materials of instruction, and of weekly topics, outcomes, assignments, and due dates.

Consider this your roadmap for the course. Please read through the syllabus carefully and feel free to share any questions that you may have. Please print a copy of this syllabus for reference.

6. Course Description

- This course presents the lifecycle of incident response management providing a foundation in computer incident response principles, addressing concepts such as preparation, detection and response, risk and regulatory impact, policies and procedures, roles and relationships of different workgroups, implementation, data collection and custody, and rehearsal testing of the plan.
- At the end of the course, students will hopefully be able to demonstrate the following:
    - Prepare an incident response plan that addresses the entire lifecycle from preparation, organization, detection, communication, reaction, recovery, maintenance, and root cause attribution.

- Align the incident response plan to relevant regulatory compliance frameworks, and demonstrate auditable compliance to these frameworks.
- Build and manage an incident response team and provide guidance during the course of an incident
- Critically asses incident preparedness through testing and rehearsal

- Prerequisites: Familiarity with information security principles and technologies. An understanding of project management as it applies to information technology will also be helpful.

7. Materials of Instruction

a. Required Texts

- Mandia, Kevin, Pepe, Matthew, & Luttgens, Jason (2014). Incident response and computer forensics (3rd ed.). New York, NY: McGraw-Hill Osborne Media ISBN: 9780071798686 or ISBN: 9780071798693 (eBook)

b. Required Software and Other Supplies

- None (Note however that it will be very helpful to have completed RIAS 101 and RIAS 102, which will familiarize you with foundational concepts and vocabulary in IT Security)

c. Recommended Text(s) / Journals

- Ó Ciardhuáin, Séamus (2004). An extended model of cybercrime investigations, International Journal of Digital Evidence, 3(1) https://www.utica.edu/academic/institutes/ecii/publications/articles/A0B70121-FD6C-3DBA-0EA5C3E93CC575FA.pdf
- Mukasey, Michael B., Sedgwick, Jeffrey L., Hagy, David W. (2008). U.S. Department of Justice Office of Justice Programs National Institute of Justice Special REPORT Electronic Crime Scene Investigation: A Guide for First Responders, (2nd ed.) https://www.ncjrs.gov/pdffiles1/nij/219941.pdf
- Kent, Karen, Chevalier, Suzanne, Grance, Tim & Dang, Hung (2006). Guide to Integrating Forensic Techniques into Incident Response. Gaithersburg, MD: The Information Technology Laboratory (ITL) http://csrc.nist.gov/publications/nistpubs/800-86/SP800-86.pdf
- N.K. McCarthy (2012) The Computer Incident Response Planning Handbook: Executable Plans for Protecting Data at Risk. The McGraw-Hill Companies

d. Online Course Content

- *This section of the course will be conducted completely online using Brandeis' LATTE site, available at http://latte.brandeis.edu. The site contains the course syllabus, assignments, discussion forums, links/resources to course-related professional organizations and sites, and weekly checklists, objectives, outcomes, topic notes, self-tests, and discussion questions. Access information is emailed to enrolled students before the start of the course. To begin participating in the course, review the Welcome Message and the materials found in the Week 1 block.*

8. Course Grading Criteria

It might be clear by now that the course being taught assyncronously is a bit different from a traditional in-person lecture. Many of us are professionals and have many duties/responsibilities during the work week. If you find that you are having difficulty completing assignments or meeting deadlines, please contact me as soon as possible. Regardless your issue, I can guarantee that you will have a better outcome if you notify me sooner rather than later. I respond quickest to emails.

VERY IMPORTANT: The core of this course is driven by engagement and interaction and these assignments are meant to encourage interaction with your fellow students and peers. Your knowledge, experience, opinions, and ideas are welcome. This is a high functioning group, and the collective brain trust in this group means that we will all benefit from each other's input. No question or comment should be left out or over analyzed as not worthy. Because we are not using a traditional classroom setting to discuss topics face-to-face, we cannot see each other to gauge how are opinions are being received, so you need to let your fellow students know what you are thinking. If you disagree, please let it be known, because that invites debate. No one is going to take it personally. You will find that many times I will disagree with you and this should not be construed as a rebuke or correction. You online posts will make this course a rich and beneficial experience, the more you post the bigger the benefit.

With that in mind your grade is determined by your performance in three broad categories:

Percent	Component
35 %	Discussions /on-line participation Each week, respond to both of the two (2) Discussion Questions with a substantial post, the first, due by Saturday at midnight (Eastern) and the second due by midnight Monday. The expectation is that you will read the background materials that are provided (along with any other supplemental materials if appropriate), and respond to the best of your ability based on your own analysis, opinion and real-world experience. Each week, you must post at least two (2) other substantive comments in response to your classmate's substantial post by Tuesday at midnight (Eastern). The expectation is that you will read the substantial post of your classmates to enhance your own learning, and respond to those posts of your choice based upon your own experiences, insights, opinions, and ability to extend and add value to the discussion. After Week One we will each meet for 15 minutes to discuss the class, your goals and my expectations. After that, assignment grades and feedback will be provided every week after Tuesday and before Sunday
25 %	Mid-term Assignment You will write two (2) executive level memos of 2000 words each, from a pool of four possible memo topics. Please see

	the resource “Writing an executive memo.doc” for guidelines on format and style. Do not create your own memo style without prior written permission from the instructor. Please see the APA guide for style. You must convey to me your opinion, idea, or recommendation in a composed manner with, if appropriate, supporting references. Please see the APA guide for style.
40 %	Final Assignment The final essay paper will be your design of a computer incident response plan AND proposal for the creation of an operational team. Create a plan that is encompassing of your organization. In proposing your team, please consider the business benefit of the function, outline the component roles and responsibilities, as they relate to the plan and to the daily operation of the team. Be sure to identify stakeholders, consider staffing, retention, and training, and compose a minimal operating budget that accounts for initial capital funding and projects ongoing operating costs. Therefore, you are creating one paper, with two goals, a plan (CIRP) and a team to execute and sustain the function. The paper should be a minimum of 8-10 pages. Please see the APA guide for style.

Guidelines / evaluation criteria for discussions and on-line participation are summarized in the following table.

Percentage	Criteria
General	The expectation is that you will read the background materials, along with any other supplemental materials, and respond to the best of your ability based on your own analysis and experience. Include references as appropriate to weekly-required readings and/or other external sources, cited appropriately. Please see the APA guide for style. Please bring your real world experience to the classroom. You MUST write two substantial posts, one for each of the two weekly questions. You MUST reply to at least two of your classmate's substantial posts with two original replies of your own. A reply of "I agree." Is not acceptable. Replies should enhance, guide, questions or continue the conversation in a meaningful way. Keep to a reasonable length, e.g., less than 1000 words for a substantial post and approximately 200-300 words for replies. Well written, clear and concise, with no spelling, textual or grammatical errors, e.g. No 'lol' or skipping verbs or parts of speech. Post on time
95-100%	Responses that meet the minimum guidelines below, and are more substantive, insightful, engaging, questioning, relevant, and guiding to fellow students. These are posts that get everyone talking.
81-94%	Solid original post. Make substantive replies (e.g., more than "I agree"), including follow-on points from readings or from your related experiences; follow-up questions for others to extend the conversation are encourage.
70-80%	Post and responses that do not meet the guidelines above – in terms of completeness, substance, or timeliness (posted on time).
0	Failure to post any responses during the course week. NOTE: Communicate immediately with instructor if you are unable to post.

- Description of work expectations for online assignments
- Each week, post two [2] substantive posts on weekly topics generated by the instructor, and respond to at least two [2] peers responses to discussion questions. All posts must be submitted by 23:59 Tuesday evening.
- The mid-term will consist of two essays of 2000 words. The mid-term is due in Latte by 23:59, 10/18/2016.
- The final paper of at least 5000 words outlining, in detail, a computer incident response plan will be due in Latte by 23:59, 11/22/2016
- Assignments submitted late without prior arrangement with the instructor will be marked down 10% each day late.
- Late final essays will not be accepted after 23:59, 11/22/2016. Failure to submit the final essay will lead to an 'incomplete' grade awarded for the course.
- Percentages earned per assignment; for example:

Percent	Component

35%	Discussions/Online participation
25%	Mid-term essays
40%	Final paper

II. Weekly Information

Week 1	July 19-25
Objectives	Introduction to the class and to the topic
Outcomes	Familiarize yourself with the function, generally. Introduce yourself Begin to change how you read media reports of incidents to filter out the value to your constituent.
Discussions	1. Please introduce yourself and tell us what you would like to take away from this class. Please also tell us your current role in Information Security and where you are heading in your career. 2. Find one "incident" reported in the media and provide us your summary of the event and the most important failure and your opinion of the incidents impact to the business or constituent affected.
Readings	Incident Response & Computer Forensics (IRCF) Chapter 1 and Chapter 2 Expectations for Computer Security Incident Response https://www.ietf.org/rfc/rfc2350.txt This document is a great historical reference Talk through with yourself the questions at the end of Chapter 1 of IRCF.
Assignments / Self-Assessments	Online discussion

Week 2	July 26 - Aug 1
Objectives	Understanding IR Management Thinking about your business and how incident response priorities will integrate into planning.
Outcomes	Be able to articulate the IR process and goals Be able to describe the benefit to the business in supporting an IR function
Discussions	1. What are the most important relationships in your business? Who are your constituents? How do the goals of IR intersect with the goals of your organization? 2. How has your organization prepared for incidents, what are the priorities, is there a documented plan, and how do they ensure that the planning is fit for purpose? Who should handle internal incidents?

Readings	Computer Security Incident Handling Guide http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-61r2.pdf How good is your cyberincident-response plan? http://www.mckinsey.com/insights/business_technology/how_good_is_your_cyberincident_response_plan Playing war games to prepare for a cyberattack http://www.mckinsey.com/insights/business_technology/playing_war_games_to_prepare_for_a_cyberattack Talk through with yourself the questions at the end of Chapter 2 of IRCF.
Assignments / Self-Assessments	Online discussion

Week 3	Aug 2 - 8
Objectives	Planning for the incident Understanding recent trends in technology and their impact on IR planning
Outcomes	Understand and articulate the CIRP development process
Discussions	1. What are the most important legal and regulatory considerations for your company in incident response planning? 2. What are the most important considerations regarding the Cloud in developing an IP plan for your business? How do you support your argument and what will need to be different about your plan?
Readings	IRCF Chapter 3 Updating Incident Response For The Cloud http://blog.trendmicro.com/pdating-incident-response-for-the-cloud/ Computer Forensics and Incident Response in the Cloud http://www.rsaconference.com/writable/presentations/file_upload/anf-t07a-computer-forensics-and-incident-response-in-the-cloud.pdf The Essence of Winning and Losing, by John R. Boyd https://fasttransients.files.wordpress.com/2010/03/essence_of_winning_losing.pdf The OODA Loop, Wikipedia entry http://en.wikipedia.org/wiki/OODA_loop Talk through with yourself the questions at the end of the chapter of IRCF. Supplemental reading Destruction and Creation by John R. Boyd. http://www.goalsys.com/books/documents/DESTRUCTION_AND_CREATION.pdf
Assignments / Self-Assessments	Online discussion

Week 4	Aug 9 - 15
Objectives	Defining the incident Understanding detection and the beginning investigation
Outcomes	Understand the priorities when responding to an incident Understand the process of managing an incident
Discussions	1. Why is training and practice important and what are the most important scenario exercises you will run for your enterprise and how will they develop you IR response and team? 2. How is your organization currently detecting events and does the design of your detection provide comprehensive coverage?
Readings	IRCF Chapter 4 and Chapter 5 Intelligence-Driven Computer Network Defense Informed by Analysis of Adversary Campaigns and Intrusion Kill Chains http://www.lockheedmartin.com/content/dam/lockheed/data/corporate/documents/LM-White-Paper-Intel-Driven-Defense.pdf Quantum Dawn http://www2.deloitte.com/content/dam/Deloitte/us/Documents/financial-services/us-fsi-quantum-dawn-2-report-102213.pdf Talk through with yourself the questions at the end of the chapter of IRCF.
Assignments / Self-Assessments	Online discussion

Week 5	Aug 16 - 22
Objectives	Response protocols Beginning the investigation and collecting data
Outcomes	Understand what data to collect and why Understand data collection best practices
Discussions	1. What do you see as the most important points to consider when collecting data? How should one approach data analysis and what are the most important priorities? 2. What emerging technologies must be considered for inclusion in our IR plan? What "non-standard" types of data may they possess?
Readings	IRCF Chapter 6 and Chapter 7 A Ten Step Process for Forensic Readiness http://www.digital4nzics.com/Student%20Library/A%20Ten%20Step%20Process%20for%20Forensic%20Readiness.pdf Talk through with yourself the questions at the end of the chapter of IRCF.
Assignments / Self-Assessments	Online discussion

Week 6	Aug 23 - 29
Objectives	Working with vendors and manufacturers Roles and responsibilities Evidence Collection
Outcomes	Complete your mid-term on time. Determine the best way to integrate forensic tools into your teams repertoire.
Discussions	1. What has been your greatest challenge in crafting your mid-term essay? What are the key factors one must consider in communicating technical information and management points to a non-technical executive audience?
Readings	IRCF Chapter 8 and Chapter 9 Talk through with yourself the questions at the end of the chapter of IRCF.
Assignments / Self-Assessments	• See the Week 6 Checklist in Latte for the Mid-term Essay topics • The mid-term is due in Latte by 23:59, 10/24/2016 • Assignments submitted late without prior arrangement with the instructor will be marked down 10% each day late.

Week 7	Aug 30 - Sep 5
Objectives	Understand the methodology for analyzing data Monitoring the enterprise
Outcomes	Understand technical configurations and their relation to IR Understand how to approach and improve visibility through your enterprise Articulate the methodology for IR data analysis
Discussions	No discussion in lieu of a GUEST LECTURE. Your attendance and participation will equate to full discussion marks this week, so please be in attendance.
Readings	IRCF Chapter 11 Talk through with yourself the questions at the end of the chapter of IRCF. Optional reading: IRCF Chapter 10 and 12. You should review these, but for our work here I would like to focus on the analysis methods.
Assignments / Self-Assessments	**Submit an outline for your final paper.** You should have been working on the outline for your CIRP, and this weeks assignment is to submit that outline. This is an outline, so bulleted points and topic areas, NO developed content needs to be submitted this week.

Week 8	Sep 6 - 12
Objectives	Understand Malware, Zero Days and APT
Outcomes	Articulate the impact of advanced threats on your enterprise Understand and methods used to investigate applications
Discussions	1. Provide an analysis of your approach to dealing with malware in your environment. How will you response plan address this topic? 2. What are the primary differences between static and dynamic analysis techniques? What are the advantages of each? How can this inform your CIRP?
Readings	IRCF Chapter 15 Chinese Hackers Suspected In Long-Term Nortel Breach http://www.wsj.com/articles/SB10001424052970203363504577187502201577054 APT1: Exposing One of China's Cyber Espionage Units http://intelreport.mandiant.com/Mandiant_APT1_Report.pdf Talk through with yourself the questions at the end of the chapter of IRCF. Optional reading: IRCF Chapter 13 and 14. You should review these and be familiar with their contents.
Assignments / Self-Assessments	Online discussion

Week 9	Sept 13 - 19
Objectives	Understand remediation Understand and facilitate root cause analysis reporting
Outcomes	Understand and articulate the remediation process and root cause analysis Understand and articulate the process of remediation
Discussions	1. How should the SOC or CIRT facilitate a root cause analysis and why is it beneficial to perform this analysis? 2. How does self-identification and remediation inform the CIRT as a business? Who are the stakeholders for self-identification and why is it important for the CIRT to participate in re-mediation activities?

Readings	IRCF Chapter 17 and Chapter 18 The Application of Formal Methods to Root Cause Analysis 0f Digital Incidents https://www.utica.edu/academic/institutes/ecii/publications/articles/A0B62ABA-F4C9-CBCE-8B9812B7B4055CAC.pdf Cage the Beast: Root Cause Analysis http://www.cxoware.com/wp-content/uploads/2014/02/ghdposter022514.pdf Understanding How to Use The 5 Whys for Root Cause Analysis http://www.lifetime-reliability.com/tutorials/lean-management-methods/How_to_Use_the_5-Whys_for_Root_Cause_Analysis.pdf Talk through with yourself the questions at the end of the chapter of IRCF. Optional reading: IRCF Chapter 16. You should review this chapter
Assignments / Self-Assessments	Online discussion

Week 10	Sept 20 - 26
Objectives	Final paper
Outcomes	Integrate what you have learned to develop your plan. Complete your final paper and discussion on time.
Discussions	**(Optional choice- you pick one. You will also need to reply to a peer's original post.)** 1. What are the main learnings you are leaving this class having found? OR 2. How has your work in the last two months informed your approach to IR as a manager or IR team leader?
Readings	None required
Assignments / Self-Assessments	See the Week 10 Checklist in Latte for the Final Essay topic material. **The final paper will be due in Latte by 23:59, 11/22/2016** Assignments submitted late without prior arrangement with the instructor will be marked down 10% each day late.

III. Course Policies and Procedures

1. Asynchronous Work

a. All required work for the course may be done asynchronously; i.e., participants can login to the course, read/download materials, post to the Discussions, and submit assignments throughout the course week. Please carefully follow the Course Syllabus and the weekly checklists to help manage your time throughout each course week.

b. At one or more points throughout the course, I may make myself available for synchronous Chat sessions using the course site's Chat Room. These optional sessions will be open Q&A. I will post a log of each such chat session so that those participants who did not participate can view the recorded synchronous discussions.

2. Late Policies

a. Participants are encouraged to complete all posts, responses and project assignments by the due dates provided. This will help ensure that everyone stays in synch with the pace of the course, and realizes the designed outcomes for the course. (Likewise, please do not work ahead! The topics and Discussion Questions for upcoming weeks may be modified and adjusted by the instructor, based on the discussions for current and previous weeks.)
b. If you find that you will not be able to complete something for a given week by the due date, please contact the instructor in advance. Unless previously arranged, credit will be deducted for work that is submitted late, out of fairness to other students.
c. Keep in mind that all course deadlines reflect the Eastern time zone, which may not be the same as your local time zone. (Note: an appropriate grace period will be provided to accommodate students in different time zones.)
d. Written projects generally should be submitted through the designated assignment drop box in LATTE (e.g., do not submit directly to the instructor via email) unless otherwise requested, or unless otherwise arranged in advance.

3. Work Expectations

a. Participants are responsible for exploring each week's materials and submitting all required work by its respective due date. On average, a participant can expect to spend approximately 3-5 hours per week reading and approximately 3-5 hours per week completing assignments and participating in online discussions. The calendar of assignments and due dates is outlined in this Course Syllabus.

4. Grading Standards and Feedback

a. Feedback will be provided on all assignments within seven (7) days of the due date, unless otherwise noted. Participants will receive weekly feedback within seven (7) days of the close of the first two weeks, which will include a breakdown of grades earned to date along with instructor narratives evaluating work and discussions submitted to date. Subsequently, participants will receive similar bi-weekly feedback within seven (7) days of the close of each two-week period.
b. Total points (which in this case are the same as percentages) equate to final letter grades as follows:

93-100 A
90-93 A-
87-90 B+
83-87 B
80-83 B-
77-80 C+
73-77 C
70-73 C-

c. Often, students receive tuition reimbursement from their employers that varies based on final grades. Instructors have no control over these policies and cannot take them into account when determining grades. Students are responsible for knowing about their employer's reimbursement policy.

5. Confidentiality

a. We can draw on the wealth of experience and examples from our own organizations in class discussions and in our written work. However, it is imperative that we not share information that is confidential, privileged or proprietary in nature. All of us must be mindful of any contracts we have agreed to with our respective companies. In addition, we should respect our fellow classmates and work under the assumption that what is discussed here (as it pertains to the workings of particular organizations) stays within the confines of the course.
b. Members of the University's technical staff have access to all course sites, to aid in course setup and technical troubleshooting. Program Chairs and a small number of Graduate Professional Studies (GPS) staff also have access to all GPS courses, for oversight purposes. Students enrolled in GPS courses can expect that individuals other than their fellow classmates and the course instructor(s) may visit their course for various purposes. Their intentions are to aid in technical troubleshooting and to ensure that quality course delivery standards are met. Strict confidentiality of student information is maintained.

6. Class Schedule

Week	Dates
Week 1	Jul 19 - 25
Week 2	Jul 26 - Aug 1
Week 3	Aug 2 - 8
Week 4	Aug 9 - 15
Week 5	Aug 16 - 22
Week 6	Aug 23 - 29

Week 7	Aug 30 - Sep 5
Week 8	Sept 6 - Sep 12
Week 9	Sept 13 - Sep 19
Week 10	Sept 20 - Sep 26

Please review the policies and procedures of Graduate Professional Studies, found at http://www.brandeis.edu/gps/students/studentresources/policiesprocedures/index.html. We would like to highlight the following.

Learning Disabilities

If you are a student with a documented disability on record at Brandeis University and wish to have a reasonable accommodation made for you in this course, please contact me immediately.

Academic Honesty and Student Integrity

Academic honesty and student integrity are of fundamental importance at Brandeis University and we want students to understand this clearly at the start of the term. As stated in the Brandeis Rights and Responsibilities handbook, “Every member of the University Community is expected to maintain the highest standards of academic honesty. A student shall not receive credit for work that is not the product of the student’s own effort. A student's name on any written exercise constitutes a statement that the work is the result of the student's own thought and study, stated in the students own words, and produced without the assistance of others, except in quotes, footnotes or references with appropriate acknowledgement of the source." In particular, students must be aware that material (including ideas, phrases, sentences, etc.) taken from the Internet and other sources MUST be appropriately cited if quoted, and footnoted in any written work turned in for this, or any, Brandeis class. Also, students will not be allowed to collaborate on work except by the specific permission of the instructor. Failure to cite resources properly may result in a referral being made to the Office of Student Development and Judicial Education. The outcome of this action may involve academic and disciplinary sanctions, which could include (but are not limited to) such penalties as receiving no credit for the assignment in question, receiving no credit for the related course, or suspension or dismissal from the University.

Further information regarding academic integrity may be found in the following publications: "In Pursuit of Excellence - A Guide to Academic Integrity for the Brandeis Community", "(Students') Rights and Responsibilities Handbook" AND " Graduate Professional Studies Student Handbook". You should read these publications, which all can be accessed from the Graduate Professional Studies Web site. A student that is in doubt about standards of academic honesty (regarding plagiarism, multiple submissions of written work, unacknowledged or unauthorized collaborative effort, false citation or false data) should consult either the course instructor or other staff of the Rabb School Graduate Professional Studies.

University Caveat

The above schedule, content, and procedures in this course are subject to change in the event of extenuating circumstances.