2018

Introduction - Syllabus

C. Ariel Pinto
Old Dominion University

Multidisciplinary Risk Management in Cybersecurity

Prerequisites: Knowledge of probability theory

Length of Completion: 12 weeks

Level of Instruction: Appropriate for both upper level undergraduate courses, as well as graduate-level courses with its additional advanced topics.

This module is suitable for non-majors and majors in engineering and management.

Learning Setting: This course is suitable with minimal modifications for in-class, online, and hybrid modes of delivery.

Course Description

Cybersecurity risk management is a necessary tool for decision making for all management levels from tactical to strategic and creating a common understanding between people from diverse domains or having different priorities. This course adopts a multidisciplinary perspective. It creates a common understanding of risk for a diverse set of students which are coming from different disciplines such as technical, social, economics, law, and politics to remove communication barriers between strategic, operational, and tactical level decision makers.

The course covers related government and industry regulations and standards along with best practices frequently used to assess, analyze and manage cyber risks, along with the fundamental methods of risk management. Also, applications of cybersecurity risk management on emerging topics such as Internet of things and cloud systems are discussed along with traditional applications areas.

This course helps students to bridge the gap between theory and practice. For example, case studies are provided to help students comprehend how to manage risks in the real world. The course also enhances field skills in cybersecurity risk management to prepare students for real work settings.

In addition, the course helps prepare students who may be entering federal jobs where knowledge of cyber security risk management is a requirement.

Learning Outcomes:

Upon completion of this course, students will be able to:

- Adapt risk management methods and skills to their current area of expertise in cybersecurity
- Communicate cybersecurity risks to a decision maker of any level (i.e., tactical, operational and strategic) in an understandable manner
- Apply cybersecurity risk management standards and best practices

Materials:

Required Text (none)

Supplementary Readings

1. Vidalis, S., Jones, A. (2005). *Analyzing threat agents and their attributes.* https://www.researchgate.net/profile/Andy_Jones8/publication/220947230_Analyzing_Threat_Agents_and_Their_Attributes/links/00b49539bff10d7f49000000.pdf

2. ENISA. (2017). *ENISA Threat landscape report 2016.* https://www.enisa.europa.eu/publications/enisa-threat-landscape-report-2016

3. Shenk, J. (2013). *Layered Security: Why it works.* SANS Institute. https://www.sans.org/reading-room/whitepapers/analyst/layered-security-works-34805

4. ENISA. (2016). *ENISA Threat taxonomy: A tool for structuring threat information.* https://www.enisa.europa.eu/topics/threat-risk-management/threats-and-trends/enisa-threat-landscape/etl2015/enisa-threat-taxonomy-a-tool-for-structuring-threat-information

5. Welch, L. D. (2013). *Cyberspace - the fifth operational domain.* https://www.ida.org/~/media/Corporate/Files/Publications/Resear

chNotes/RN2011/2011%20Cyberspace%20-%20The%20Fifth%20Operational%20Domain.pdf

6. Mandiant. (2013). *Advanced Persistent threat - Exposing One of China's Cyber Espionage Units.* https://www.fireeye.com/content/dam/fireeye-www/services/pdfs/mandiant-apt1-report.pdf

7. Software Engineering Institute, Carnegie Mellon University. (2017). *Ransomware: Best Practices for Prevention and Response.*https://www.youtube.com/watch?v=Nk-EwaVzYAQ

8. Volynkin, A., Horneman, A. (2017). *Ransomware: Best Practices for Prevention and Response.* http://www.sei.cmu.edu/podcasts/podcast_episode.cfm?episodeid=502998

9. Schneier, B. (2010). *The Story Behind The Stuxnet Virus.* https://www.forbes.com/2010/10/06/iran-nuclear-computer-technology-security-stuxnet-worm.html

10. Bethune, P. (2017). *Understanding Risk Management and ISO Standards.* https://www.qualitydigest.com/inside/risk-management-article/understanding-risk-management-and-iso-standards-071717.html

11. Bowler, C. (2015). *Risk, Risk Assessments, and Risk Management.* http://www.isaca.org/chapters3/Atlanta/AboutOurChapter/Documents/GW2015/081015-3PM-RiskRiskAssessmentsAndRiskMgmt.pdf

12. SANS Institute. (2014). Teri Radichel, *Case Study: Critical Controls that Could Have Prevented Target Breach*. https://www.sans.org/reading-room/whitepapers/casestudies/case-study-critical-controls-prevented-target-breach-35412

13. IRGC. (2009). *Risk Governance Deficits.* http://irgc.org/wp-content/uploads/2012/04/IRGC_rgd_web_final1.pdf

14. NIST. (2011) *SP 800-39 Managing Information Security Risk - Organization, Mission, and Information System View.* https://csrc.nist.gov/publications/detail/sp/800-39/final

15. Kevin Richards, & Ryan LaSalle. (2017). *Cost of Cyber Crime Study 2017 - Insights on the Security Investments that Make a Difference*. Ponemon Institute. Retrieved from https://www.accenture.com/t20170926T072837Z__w__/us-en/_acnmedia/PDF-61/Accenture-2017-CostCyberCrimeStudy.pdf

16. The Council of Economic Advisers. (2018). *The Cost of Malicious Cyber Activity to the U.S. Economy*. Washington DC: The Executive Office of the President of the United States. https://www.whitehouse.gov/wp-content/uploads/2018/02/The-Cost-of-Malicious-Cyber-Activity-to-the-U.S.-Economy.pdf

17. United States Computer Emergency Reediness Team. (2016). Assessments: Cyber Resilience Review (CRR). https://www.us-cert.gov/ccubedvp/assessments.

18. Velasquez, M. and Hester, P. T. (2013). An Analysis of Multi-Criteria Decision Making Methods. *International Journal of Operations Research.* Vol. 10. No. 2. 56-66.

19. Cisco Security. (2016). *Cyber Resilience: Safeguarding the Digital Organization*. Retrieved October 02, 2017, from https://www.cybrary.it/channelcontent/cyber-resilience-safeguarding-digital-organization-white-paper/

20. Pagliery, J. (2015, August 15). The inside story of the biggest hack in history. *CNN*. Retrieved October 15, 2017, from http://money.cnn.com/2015/08/05/technology/aramco-hack/index.html

21. NIST. (2014). *Document 3764, CSF Core*. https://www.nist.gov/document-3764

22. DoD. (2014). *8510.01 Risk Management Framework (RMF) for DoD Information Technology (IT)*.http://www.esd.whs.mil/Portals/54/Documents/DD/issuances/dodi/851001_2014.pdf

23. DoD. (2015). *DoD Program Manager's Guidebook for Integrating the Cybersecurity Risk Management Framework (RMF) into the System Acquisition Lifecycle.* https://www.dau.mil/tools/Lists/DAUTools/Attachments/37/DoD%20-

%20Guidebook,%20Cybersecurity%20Risk%20Management%20Framework,%20v1.08,%20Sep%202015.pdf

24. White House. (2013). *Executive Order - Improving Critical Infrastructure Cybersecurity.* https://obamawhitehouse.archives.gov/the-press-office/2013/02/12/executive-order-improving-critical-infrastructure-cybersecurity

25. NIST. (2017). *SP 800-37 Risk Management Framework for Information Systems and Organizations - A System Life Cycle Approach for Security and Privacy.* https://csrc.nist.gov/CSRC/media/Publications/sp/800-37/rev-2/draft/documents/sp800-37r2-discussion-draft.pdf

26. Irwin. L, (2017). *How to implement an ISMS.* https://www.itgovernance.co.uk/blog/how-to-implement-an-isms/

27. FFEIC. (2017). *Cybersecurity Assessment Tool - Overview for Chief Executive Officers and Boards of Directors.* https://www.ffiec.gov/pdf/cybersecurity/FFIEC_CAT_CEO_Board_Overview_June_2015_PDF1.pdf

28. NIST. (2018). *Risk Management*. https://csrc.nist.gov/projects/risk-management

29. The Open Group. (2009). *Risk Taxonomy-Technical Standard.* http://pubs.opengroup.org/onlinepubs/9699919899/toc.pdf

30. Software Engineering Institute. (2007). *Introducing OCTAVE Allegro: Improving the Information Security Risk Assessment process.* https://resources.sei.cmu.edu/asset_files/TechnicalReport/2007_005_001_14885.pdf

31. Lloyd's. (2018). *Cloud Down Impacts on the US Economy*. https://www.lloyds.com/news-and-risk-insight/risk-reports/library/technology/cloud-down

32. Walsh, M. (2018). *Microsoft case underscores legal complications of cloud computing.* http://www.abajournal.com/magazine/article/microsoft_case_underscores_legal_complications_of_cloud_computing_

33. Robinson, N., Valeri, L., Cave, J., Starkey, T., Graux, H., Creese, S., & Hopkins, P. P. (2010). The cloud: understanding the security, privacy and trust challenges. [Read page 70-77]. http://www.jstor.org/stable/pdf/10.7249/tr933ec.12.pdf?refreqid=excelsior%3A5f058dcacf3a9dc54c2ed7cd9e428021

34. NIST. (2011). *NIST SP 800-144 Guidelines on Security and Privacy in Public Cloud Computing.* [Read Page 37-39. Cloud Transition Case Study] https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-144.pdf

35. Harvey, C. (2016). *Top 10 Cloud Computing Failures*. https://www.datamation.com/cloud-computing/slideshows/top-10-cloud-computing-failures.html

36. Gonyea, C. (2010). *DNS: Why It's Important & How It Works.* https://dyn.com/blog/dns-why-its-important-how-it-works/

37. Krebs, B. (2016). *Hacked Cameras, DVRs Powered Today's Massive Internet Outage*. https://krebsonsecurity.com/2016/10/hacked-cameras-dvrs-powered-todays-massive-internet-outage/

38. Capgemini Consulting. (2017). *Securing the Internet of Things Opportunity: Putting Cybersecurity at the Heart of the IoT*. https://www.capgemini.com/wp-content/uploads/2017/07/securing_the_internet_of_things_opportunity_putting_cyber_security_at_the_heart_of_the_iot.pdf

Technical Specifications:

- Microsoft Word, Microsoft Excel, Microsoft PowerPoint
- Web Browser

Grading:

Assessment Mechanism	Percentage
Participation	10%
Exam 1	30%
Exam 2	30%
Exam 3	30%
Total:	**100%**

Course Schedule:

Week	Module/Micromodule	Assignments due
	Module 1. Fundamentals of Cyber Risk Management	
1	**Micromodule 1. Fundamentals of Cybersecurity** • Evolution of cyber • Principles of cybersecurity • Related concepts of cyber vulnerabilities, actors, and threats • Cyber threat examples • Countermeasures	Supplementary Readings 1-9
2	**Micromodule 2. Fundamentals of Risk Management** • Definition of risk • Measurement scales • Basics of risk and decision theory ○ Elements of probability theory ○ Bayes' Rule ○ Value function ○ Certainty equivalent of a lottery & risk preference ○ Utility theory and function GRADUATE ○ Extreme event analysis GRADUATE • Risk management process	Supplementary Readings 10-11
3	**Micromodule 3. Risk Management Tools and Techniques** • Risk Management (RM) Tools and Techniques ○ Cause and Consequences Analysis (CCA) ○ Preliminary Hazard Analysis (PHA) ○ Hazard and Operability Analysis (HAZOP) ○ Failure Mode and Effects Analysis (FMEA) ○ Fault Tree Analysis (FTA) ○ The principle of As Low As Reasonably Practicable (ALARP) • Integrating risk management concepts into cybersecurity risk assessments	Supplementary Readings 12
4	**Micromodule 4. Cybersecurity Risk Governance** • Risk Governance • Complexity of Cybersecurity Risk Governance • Communication of Cyber Security Risk • Dilemmas of Cybersecurity Risk Governance • Organizational Cybersecurity Governance Decisions GRADUATE	Supplementary Readings 13-14

Week	Module/Micromodule	Assignments due
5	**Micromodule 5. Economics of Cyber Systems Risk Management** • Economics for cybersecurity risk management • Quality and cost of cybersecurity • Portfolio of technology investments	Supplementary Readings 15-16
6	**Micromodule 6. Cyber Resilience and Decision Making** • Overview of cyber resilience • Cyber resilience goals • Principles of cyber resilience • Capabilities of a cyber resilient organization • Cyber resilience review (CRR) • Decision making steps • Multi criteria decision making methods • Cyber security risk management decision making methods • Soft skills required in cyber security risk management	Supplementary Readings 17-20
	Module 2. Applied Standards and Cyber Risk Management	
7	**Micromodule 7. Cybersecurity Framework and DoD Risk Management Framework** • Cybersecurity Framework for Improving Critical Infrastructure o Cybersecurity Framework o Component of the Framework • DoD Risk Management Framework o DoD Cybersecurity Concepts and Principles o Identify NIST risk management standards relevant with DoD RMF • Application of Risk Management Framework: Steps 1 & 2 o RMF Step 1: Categorize Information System ▪ Information Types and Information Systems ▪ Determination of the impact for information and information systems o RMF Step 2: Select Security Controls ▪ Introducing Security Controls	Supplementary Readings 21-24
8	**Micromodule 8. Risk Management Framework and Information Security Management Systems**	Supplementary Readings 25-26

Week	Module/Micromodule	Assignments due
	• Application of Risk Management Framework (RMF): Steps 3 - 6 ○ RMF Step 3: Implement Security Controls ○ RMF Step 4: Assess Security Controls ○ RMF Step 5: Authorize System ○ RMF Step 6: Monitor Security Controls • Information Security Management System (ISMS) • Comparison of DoD RMF to ISMS	
9	**Micromodule 9. Government Standards and Regulations** • Federal Information Security Modernization Act (FISMA) • National Institute of Standards and Technology (NIST) Risk Management Framework (RMF) • Department of Defense Risk Management Framework (DoD RMF) • Federal Financial Institutions Examination Council (FFIEC) Cybersecurity Assessment Tool	Supplementary Readings 27-28
10	**Micromodule 10. Industry Standards and Best Practices** • Factor Analysis of Information Risk (FAIR) ○ What is FAIR ○ Fair Framework ○ Decomposing Risk ○ Fair Ontology • Operationally Critical Threat, Asset, and Vulnerability Evaluation (OCTAVE) Methodology ○ OCTAVE-Original ○ OCTAVE-S ○ OCTAVE Allegro ○ OCTAVE Allegro-Process ○ OCTAVE Allegro-Worksheets ○ OCTAVE Allegro Example	Supplementary Readings 29-30
	Module 3. Field Skills on Cyber Risk Management	
11	**Micromodule 11. Cyber Risk Management in Cloud Environment** • Introduction to Cloud Computing ○ What is a Cloud? ○ How is it being used? ○ Why is it so popular? • Recent Cyber Incidents in the Cloud – See notes ○ List of incidents • Risks in Cloud Computing ○ Technical ○ Economic	Supplementary Readings 31-35

Week	Module/Micromodule	Assignments due
	○ Legal ○ Political ○ Social • Managing Risks in Cloud Computing ○ Tactical ○ Operational ○ Strategic ○ Case study: The City of Los Angeles – see notes • Phishing and Cloud Computing	
12	**Micromodule 12. Cyber Risk Management in Internet of Things** • Introduction to Internet of Things (IoT) ○ What is IoT? ○ Elements of IoT ○ Why is it so popular? • Recent Cyber Incidents with IoT ○ List of incidents ○ Case study: Dyn DDOS Attack • Risks in IoT ○ Technical ○ Economic ○ Legal ○ Political ○ Social • Managing Risks of IoT ○ Strategic ○ Operational ○ Tactical • Phishing and IoT	Supplementary Readings 36-38