A View from the Bridge: Leading an Information Security Team
T81-561
Spring 2019

Instructor: Mike Jenkins
Office Telephone: 618-698-1022
Email: m.jenkins@wustl.edu

Course Format – Hybrid Learning
3.0 credit hours

<table>
<thead>
<tr>
<th>Date</th>
<th>Event</th>
</tr>
</thead>
<tbody>
<tr>
<td>Jan 11</td>
<td>Online course opens to students</td>
</tr>
<tr>
<td>Apr 23</td>
<td>Online course closes – all assignments due</td>
</tr>
<tr>
<td>Jan 15</td>
<td>Face to Face Class 1</td>
</tr>
<tr>
<td>Feb 5</td>
<td>Face to Face Class 2</td>
</tr>
<tr>
<td>Feb 26</td>
<td>Face to Face Class 3</td>
</tr>
<tr>
<td>Mar 19</td>
<td>Face to Face Class 4</td>
</tr>
<tr>
<td>Apr 2</td>
<td>Face to Face Class 5</td>
</tr>
<tr>
<td>Apr 16</td>
<td>Face to Face Class 6</td>
</tr>
<tr>
<td>Apr 23</td>
<td>Face to Face Class 7</td>
</tr>
</tbody>
</table>

Eight (8) course modules
Seven (7) in-class Face-to-Face sessions
Room Assignment for Face-to-Face Classes: To be provided.

Course Overview
This hybrid learning course addresses the practical aspects of developing, organizing, staffing and leading a Cyber Security/Information Security organization. The course will address how constructs such as the CIS Critical Security Controls and the National Institute of Standards and Technology (NIST) Cyber Security Framework contribute to these objectives. We will discuss how to synchronize regulatory standards, information security best practices, and organizational practices and procedures in establishing, leading, and optimizing an effective cybersecurity organization.

The course explores the concepts of information technology governance, utilizing IT management frameworks and internal controls. It provides a deeper understanding of best practices for managing cyber security operations and meeting the multiple needs of enterprise management by achieving an effective balance between business risks, technical issues, control needs, and reporting metrics. Emphasis is placed on the emerging challenges faced by security leaders and practical methods of meeting those challenges.

Required Course Materials
The primary goal in this course is to provide students with information and proven techniques needed to plan and execute effective cyber security programs within business organizations. For the course text, we will use The Adventures of an IT Leader, Updated Edition with a New Preface by the Authors, by Robert D. Austin, Shannon O’Donnell, and Richard Nolan, by Harvard Business Review Press (2016). In addition, we will use a broad selection of readings, case studies, and application exercises.
As of: Monday, October 22, 2018

1. **Readings.** Case studies 1, 2, and 4 are in the course text. Case study 3 and the Harvard Case “Who Should Take the Fall?” must be accessed via the Harvard Business School Course Pack. The URL is: To be provided.

If you do not already have an account set-up with Harvard Business Publishing, you will have to create one during your initial log in. For the other listed Harvard articles, if the direct link provided in Canvas does not work you may obtain them via the Washington University Library. Instructions for how to accomplish this may be found in the Syllabus page on the course Canvas site.

<table>
<thead>
<tr>
<th>Module</th>
<th>Item/Reading</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Article: Why senior leaders are the front line against cyberattacks (Tucker Bailey, James Kaplan, and Chris Rezek)</td>
</tr>
<tr>
<td>1</td>
<td>Article: Root Cause Analysis for Beginners (James J. Rooney and Lee N. Vanden Heuvel)</td>
</tr>
<tr>
<td>1</td>
<td>Article: The Five Whys Technique (Olivier Serrat)</td>
</tr>
<tr>
<td>1</td>
<td>eBook: Executive Summary, Symantec Internet Security Threat Report</td>
</tr>
<tr>
<td>2</td>
<td>HBR Article: The Emerging Role of the Chief Information Security Officer (CISO) (Val Hooper; Jeremy McKissack)</td>
</tr>
<tr>
<td>2, 5</td>
<td>Article: Structuring the CISO Organization (Software Engineering Institute, Allen et. al)</td>
</tr>
<tr>
<td>2</td>
<td>eBook: NIST Cybersecurity Framework</td>
</tr>
<tr>
<td>3</td>
<td>eBook: CIS Security Controls</td>
</tr>
<tr>
<td>3</td>
<td>Document: CIS Risk Assessment Method</td>
</tr>
<tr>
<td>3</td>
<td>Web document: NIST 800-53, r5, Chapters 1, 2</td>
</tr>
<tr>
<td>3</td>
<td>HBR Article: Why the Entire C-Suite Needs to Use the Same Metrics for Cyber Risk (Jason J Hogg)</td>
</tr>
<tr>
<td>4</td>
<td>HBR Case 1: <em>The Adventures of an IT Leader: Crisis</em> (Due Feb 5)</td>
</tr>
<tr>
<td>4</td>
<td>eBooks: Verizon DBIR, pp. 1-30; Mandiant M-Trends 2018; Combating Threats in Critical Infrastructure Through Due Diligence (Scott Schlimmer)</td>
</tr>
<tr>
<td>5</td>
<td>HBR Article: Cybersecurity Has A Serious Talent Shortage. Here’s How to Fix It; <a href="https://hbr.org/2017/05/cybersecurity-has-a-serious-talent-shortage-heres-how-to-fix-it">https://hbr.org/2017/05/cybersecurity-has-a-serious-talent-shortage-heres-how-to-fix-it</a></td>
</tr>
</tbody>
</table>
2. Course Grading and Requirements.

Case Study Analyses: 40% (400 points)

40% of your course grade is derived from (four) at 100 points each) cyber security case study analyses, designed to enhance understanding and experience with the course material. Case study analysis submissions will:

a. Utilize the Root Cause Analysis (RCA) process to identify key issues and root cause considerations.

b. Address the specific issues or questions identified for the case on the Canvas module page.

c. Demonstrate comprehension of security concepts covered in the course material, readings, research, and discussions.

Case 1: The Adventures of an IT Leader: Crisis
Case 2: The Adventures of an IT Leader: Damage
*Case 3: The Phoenix Project
Case 4: The Adventures of an IT Leader: Emerging Technology

*Case study 3 is obtained via the Harvard Course Pack.
Team Research Project: 30% (300 points)

30% of your course grade will consist of a group 45-minute presentation selected from one of the following options:

Option One:

- Create a new cyber/information security organization, based on one of the three cases below.

Based on concepts covered in the course material, readings, discussions, and additional research, prepare an executive summary and submit it via Canvas along with any visual aids to be used, the night before the date of your presentation. Prepare a 45-minute presentation and present your plan, to include your analysis, ideas, rationale, and recommendations on creation of an Information Security/Cybersecurity Organization in a company that has never had such an organization. Include the goals, objectives, functions, and proposed structure of the proposed organization.

Case 1 – Your company is a small start-up company (20 – 40 personnel) in the cyber sector that has developed a new data compression algorithm that you want to make available to cloud providers.

Case 2 – Your company is a medium sized company (1000 – 3000 personnel) in the Critical Infrastructure Energy sector. Your residential and business customers depend on you for the generation and transmission of electricity, together with construction and maintenance of the infrastructure required for reliable delivery.

Case 3 – Your company is a large company (80,000+ personnel) specializing in retail clothing and household goods sales via its big box storefronts located across the United States and in 54 countries world-wide, and on-line via your company’s internet web presence.

Be certain your business case document and presentation address the following:

- Challenges and priorities to create a new information security/cyber security organization
- Emerging issues in ethics and privacy
- Anticipated risk environment in your industry
- Proposed organizational alignment of the security organization
- Role the CISO plays in policy and culture
- Address any specific issues or questions identified for this case on the Canvas module page
- Provide examples of similar companies who were either successful or unsuccessful in developing their culture around information security

Both your executive summary document and presentation material must be submitted to the instructor via Canvas prior to your presentation.

Option Two:

- In the role of an external cybersecurity consultant team, prepare a plan for presentation to the CEO and CIO to improve and/or restructure the cybersecurity organization and functions in the IVK Corporation. The fictitious IVK Corporation serves as the backdrop in the course text, The Adventures of an IT Leader.
As of: Monday, October 22, 2018

Online Assignments and Discussions: 30% (300 points)

An important part of your learning comes from your preparation for, and engagement in, classroom discussion with your peers and the instructor. For the online portion of this class, the opportunity for participation will include on-line discussions, critical reflections, and content analysis as assigned by the instructor.

Additionally, a peer evaluation will be conducted by all students for each member of their team for the end of course Team Major Project. Peer evaluations are considered as part of overall student class participation.

Requirements for peer evaluations:

- The evaluation will be due the last class session and will be uploaded using the link provided in the Canvas assignment page.
- Criteria for peer evaluation are: completion of assigned tasks, quality and timeliness of work, teamwork, and overall contribution to the group.
- Peer evaluations will consist of completing the peer evaluation form with an evaluation addressing each member of your group, excluding yourself.

Grading

| Case Study Analyses (4 @ 100 each): | 400 |
| Team Research Project: | 300 |
| On-Line Assignments and Participation (includes online and in-class): | 300 |
| Total: | 1000 |

LATE AND MISSED ASSIGNMENTS

Assignments and presentations are due on the date/time specified. If permission is obtained in advance from the instructor, late work may be accepted, with a possible reduction in points for the assignment.

Ethics

In this course, you will learn about vulnerabilities in information systems, and how they may potentially be exploited. This is intended in the spirit of open intellectual inquiry to help you understand how such vulnerabilities may be avoided or repaired, and how attackers go about circumventing security measures. You have the responsibility to use this information responsibly, legally, and ethically. Under no circumstances should you access or alter any computing system without permission from its legitimate owner. Information security can be fraught with ethical and legal pitfalls, so you should consult me if you are ever in doubt about a particular action.
Notes:

- **Updates.** The applicable course Canvas module page should always be referred to for the most up to date information on assignments, due dates, and other course related information.
- **On-line Collaboration Sessions/Virtual Office Hours.** During the weeks in which we do not have a face-to-face class, there will normally be on-line collaboration sessions or other events conducted via Canvas. The dates/times will be determined in advance and you will receive an invitation through Canvas or email to join these events.

---

**Overview of Course Modules**

<table>
<thead>
<tr>
<th>Module</th>
<th>Focus Area</th>
<th>Dates</th>
</tr>
</thead>
</table>
| 1 | Course Introduction and Overview  
*Face to Face Class #1 Jan 15, 2019, 6:00 pm* | Jan 15-21, 2019 |
| 2 | Information Security and CISO Functions  
*On-Line Session via Canvas, Jan 22, 2019, 6:00 pm* | Jan 22-28, 2019 |
| 3 | Information Security Controls and Governance Frameworks  
*On-Line Session via Canvas, Jan 29, 2019, 6:00 pm* | Jan 29-Feb 4, 2019 |
| 4 | Information Security in Business Environments and Industry Specific Threats  
*Face to Face Class #2 Feb 5, 2019, 6:00 pm*  
*Case Study 1 Due* | Feb 5-11, 2019 |
| 5 | Building Effective Information Security Organizations  
*On-Line Session via Canvas, Feb 19, 2019, 6:00 pm* | Feb 12-18, 2019 |
| 6 | Leading Security Operations  
*Face to Face Class #3 Feb 26, 2019*  
*Case Study 2 due* | Feb 19-25, 2019 |
| 7 | Security Leader Unique Considerations and Organizational Responsibilities  
*On-Line Session via Canvas, Mar 5, 2019, 6:00 pm* | Feb 26-Mar 18, 2019  
*Spring Break Mar 10-16, 2019* |
| **Face to Face Class #4 Mar 19, 2018** | **Case Study 3 due**  
**On-Line Session via Canvas, Mar 26, 2019, 6:00 pm** |
|-------------------------------------|-------------------------------------------------------------|
| **8** Future Challenges in Information and Cyber Security Leadership | **Face to Face Classes: Apr 2, 16, 23**  
**Apr 2:** Case Study 4 due  
**Apr 16:** Major Project Presentations  
**Apr 23:** Major Project Presentations, Course Concepts Synthesis, Wrap-Up | **Mar 19-Apr 23, 2019** |
Resources for Students

DISABILITY RESOURCES: If you have a disability that requires an accommodation, please speak with your instructor and consult the Disability Resource Center at Cornerstone (cornerstone.wustl.edu). Cornerstone staff will determine appropriate accommodations and will work with your instructor to make sure these are available to you.

WRITING ASSISTANCE: For additional help on your writing, consult the expert staff of The Writing Center (writingcenter.wustl.edu) in Olin Library (first floor). It can be enormously helpful to ask someone outside a course to read your essays and to provide feedback on strength of argument, clarity, organization, etc.

The Engineering Communication Center http://engineering.wustl.edu/current-students/student-services/Pages/default.aspx offers students in the School of Engineering and Applied Sciences help with oral presentations, writing assignments, and other communications.

Accommodations based upon sexual assault:

The University is committed to offering reasonable academic accommodations to students who are victims of sexual assault. Students are eligible for accommodation regardless of whether they seek criminal or disciplinary action. Depending on the specific nature of the allegation, such measures may include but are not limited to: implementation of a no-contact order, course/classroom assignment changes, and other academic support services and accommodations. If you need to request such accommodations, please direct your request to Kim Webb (kim_webb@wustl.edu), Director of the Relationship and Sexual Violence Prevention Center. Ms. Webb is a confidential resource; however, requests for accommodations will be shared with the appropriate University administration and faculty. The University will maintain as confidential any accommodations or protective measures provided to an individual student so long as it does not impair the ability to provide such measures.

If a student comes to me to discuss or disclose an instance of sexual assault, sex discrimination, sexual harassment, dating violence, domestic violence or stalking, or if I otherwise observe or become aware of such an allegation, I will keep the information as private as I can, but as a faculty member of Washington University, I am required to immediately report it to my Department Chair or Dean or directly to Ms. Jessica Kennedy, the University’s Title IX Director. If you would like to speak with directly Ms. Kennedy directly, she can be reached at (314) 935-3118, jw kennedy@wustl.edu, or by visiting the Title IX office in Um Rath Hall. Additionally, you can report incidents or complaints to the Office of Student Conduct and Community Standards or by contacting WUPD at (314) 935-5555 or your local law enforcement agency. See: Title IX

You can also speak confidentially and learn more about available resources at the Relationship and Sexual Violence Prevention Center by calling (314) 935-8761 or visiting the 4th floor of Seigle Hall. See: RSVP Center
Bias Reporting:
The University has a process through which students, faculty, staff and community members who have experienced or witnessed incidents of bias, prejudice or discrimination against a student can report their experiences to the University’s Bias Report and Support System (BRSS) team. See: brss.wustl.edu

Mental Health:
Mental Health Services’ professional staff members work with students to resolve personal and interpersonal difficulties, many of which can affect the academic experience. These include conflicts with or worry about friends or family, concerns about eating or drinking patterns, and feelings of anxiety and depression. See: shs.wustl.edu/MentalHealth