MCS9301  Information and Communication Security Issues
Subject Outline
Spring Session 2008

HEAD OF SCHOOL – Associate Professor Peter Hyland, Student Resource Centre, Tel: (02) 4221 3606

GENERAL INFORMATION

Subject Coordinator
Mrs Penney McFarlane
Telephone Number: 0242 21 4864
Email: penney@uow.edu.au
Location: 39.115

Mrs McFarlane’s consultation times during session:
Day  Time
Wednesday  2.00 – 4.00
Thursday  10.00-12.00

Subject Organisation
Session: Spring Session, Wollongong Campus
Credit Points: 6 credit points
Contact hours per week: 1 hours lectures, 2 hours tutorial
Lecture Times & Location: 15.30-16.30 PM Thursday, 35.G20
Tutorial Day, Time and Location can be found at: http://www.uow.edu.au/student/timetables/index.html

Students should check the subject’s web site regularly as important information, including details of unavoidable changes in assessment requirements will be posted from time to time via e-Learning space http://www.uow.edu.au/student/lol. Any information posted to the web site is deemed to have been notified to all students.

Content
This subject will examine current controls, both legislative and technical, aimed at maintaining data integrity, ease of access to information, and protection of ownership, in the light of on going developments in computer security, multimedia communications, international electronic networks, and electronic publishing. The subject will cover communication security; issues relating to the monitoring of international agreements; OECD guidelines for security of information; maintaining privacy provisions; password security; and future IT developments and their implications for monitoring intellectual property rights and communication security.

Objectives
A student who successfully completes this subject should be able to:
(i) Identify current security controls aimed at protecting the availability, confidentiality, and integrity of electronic data;
(ii) Explain the pitfalls (limitations) of existing controls in relation to intellectual property;
(iii) Debate current problems regarding security for ownership of, and access to electronic data;
(iv) Critically analyse current international policies relating to communication security.
For example: OECD guidelines for security of information, and international developments relating to information and communication technologies and intellectual property.

Graduate Qualities
All Schools in the Faculty of Informatics have adopted the UOW Graduate Qualities. On completion of their course graduates will be informed, independent learners, problem solvers, effective communicators and responsible. Further information can be found at http://www.uow.edu.au/about/teaching/qualities/

Attendance Requirements:
It is the responsibility of students to attend all lectures/tutorials/labs/seminars/practical work for subjects for which you are enrolled. It should be noted that the amount of time spent on each 6 credit point subject should be at least 12 hours per week, which includes lectures/tutorials/labs etc.

Attendance rolls will be kept for lectures, tutorials and laboratories. If you are present for less than 80%* you need to apply for special consideration, otherwise a fail grade will be recorded.

Students MUST attend their allocated tutorial unless they have the written permission of the subject coordinator.

Method of Presentation:
In order to maximize learning outcomes, it is strongly recommended that students attend all lectures.

Lecture Schedule:
A proposed Lecture schedule for the subject is as follows:

<table>
<thead>
<tr>
<th>Week</th>
<th>Topic</th>
<th>Reading</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Subject Overview, Assessments</td>
<td>NO TUTORIAL</td>
</tr>
<tr>
<td></td>
<td>~Introduction &amp; Foundation Concepts</td>
<td>Whitman ch 1, Glossary</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Easttom ch 1, Glossary</td>
</tr>
<tr>
<td></td>
<td>~Technical and Non-technical Attacks</td>
<td></td>
</tr>
<tr>
<td>3</td>
<td>Ecommerce Security Breaches</td>
<td>Whitman ch 2,8-9,11</td>
</tr>
<tr>
<td></td>
<td>~Internet Fraud, Espionage &amp; the Web</td>
<td><a href="http://www.cert.org/">http://www.cert.org/</a></td>
</tr>
<tr>
<td>4</td>
<td>Security Tools, Techniques, Methods</td>
<td>Whitman ch 6, 7</td>
</tr>
<tr>
<td></td>
<td>~Firewalls, IDS, Honeypots, Encryption</td>
<td></td>
</tr>
<tr>
<td>5</td>
<td>Security Policies, Procedures, Frameworks</td>
<td>Whitman ch 5, 12</td>
</tr>
<tr>
<td></td>
<td>~Policies, Incident Reporting &amp; Audits</td>
<td><a href="http://www.sans.org/resources/policies">http://www.sans.org/resources/policies</a></td>
</tr>
<tr>
<td>6</td>
<td>Risk Analysis, Disaster Recovery, Emergency</td>
<td>Whitman ch 4</td>
</tr>
<tr>
<td></td>
<td>Management</td>
<td><a href="http://www.sans.org/rr">http://www.sans.org/rr</a></td>
</tr>
<tr>
<td></td>
<td>~Vulnerability Assessment</td>
<td></td>
</tr>
<tr>
<td>7</td>
<td>Introduction to Global GeoPolitics</td>
<td>Snow ch 1-3</td>
</tr>
<tr>
<td></td>
<td>~Cases: Critical Infrastructure Protection</td>
<td></td>
</tr>
<tr>
<td>9</td>
<td>ICT Solutions to National Security</td>
<td>Michael &amp; Masters (2006) ch 7, 8</td>
</tr>
<tr>
<td></td>
<td>~Prevent- Protect- Respond</td>
<td>Communications of the ACM Special Ed. (March 2004)</td>
</tr>
<tr>
<td>10</td>
<td>Legal Repercussions</td>
<td>Whitman ch 3</td>
</tr>
</tbody>
</table>
### Social Implications
--Security, Privacy & Ethics

Michael & Michael (2005)  
http://www.epic.org/,  
http://www.eff.org/  
http://www.aclu.org/Privacy/PrivacyMain.cfm

### International Agreements
--OECD Guidelines, Bilateral, Unilateral

www.oecd.org/dataoecd/16/22/15582260.pdf

Changes to the above schedule will be posted via e-Learning space http://www.uow.edu.au/student/lol. Any information posted to the web site is deemed to have been notified to all students.

**Subject Materials:**
Any readings/references are recommended only and are not intended to be an exhaustive list. Students are encouraged to use the library catalogue and databases to locate additional readings

**Textbook(s):**

**Other Resources:**
Recommended Readings:

**Assessment:**
This subject has the following assessment components.

<table>
<thead>
<tr>
<th>ASSESSMENT ITEMS &amp; FORMAT</th>
<th>% OF FINAL MARK</th>
<th>GROUP/INDIVIDUAL</th>
<th>DUE DATE</th>
</tr>
</thead>
</table>
| 1. Critical Infrastructure Assessment – Preliminary Report | 10% | Group | • Electronically via eLearning, Week of August 11 @ 11:59pm (2359) Sunday night.  
• Hardcopy in the Week 4 tutorial  
• Group |
| 2. Critical Infrastructure Assessment – Final Report | 30% | Group | • Electronically via eLearning, Week of October 13 @ 11:59pm (2359) Sunday night.  
• Hardcopy in the Week 12 tutorial  
• Group |
| 3. Security Policy – Case Study | 20% | Individual | • Electronically via eLearning, Week of September 8 @ 11:59pm (2359) Sunday night.  
• Hardcopy in the Week 9 tutorial  
• Individual |
4. Final Examination | 40% | Individual | Final Exam Period (TBA)

**Notes on Assessment:**
All assignments are expected to be completed independently. Plagiarism may result in a FAIL grade being recorded for that assignment.

**Electronic Submission of Assessment Items:**
Unless otherwise notified by the subject coordinator, all written assignments must be submitted electronically.

**Other Procedures for the submission of assessment items:**
In addition to electronic submission, students are required to submit assignments in hard copy to their tutor.

All assignments will be returned within 2 weeks of their submission.
- All work must be submitted in HARD COPY at the BEGINNING of tutorials.
- A soft copy of assessment items 1, 2 & 3 is required to be uploaded on UOW e-Learning space by the due date.
- All late work to be submitted personally to Penney McFarlane.
- All special consideration applications must be lodged through SOLS.
- Please check the UOW e-Learning space discussion forum regularly for announcements.

**Critical Infrastructure Assessment**
You are to conduct a market analysis of the key landmarks in a city allocated to your group. There are any number of sources you may use to do this exercise including the Telstra White Pages online (or on CD) [http://www.whitepages.com.au](http://www.whitepages.com.au) and/or the Yellow Pages [http://www.yellowpages.com.au](http://www.yellowpages.com.au) and/or [http://www.whereis.com.au](http://www.whereis.com.au) and/or [http://www.abs.gov.au](http://www.abs.gov.au) and/or paper-based maps like those in the UBD street directory. Private data sources like CityScope Australia and other Property Australia publications are also available but the costs for these are prohibitive. Local councils may be willing to assist you in conducting your study, especially as many of these publish annual statistics about their locales- but be sure to check their websites before calling them directly.

Critical infrastructure may include (but is not limited to): energy facilities (oil, gas), utilities (water, electricity), transport hubs, telecommunications hubs, banking facilities, icons, shopping malls, schools/ tertiary institutions. You are to rank these locations/buildings from 1 to 100 in a table and display these graphically or on a map. The method you use for ranking these locations may be based on your assessment of the “risk” to that location and its overall importance to society. You will need to create an Excel spreadsheet or MS Access database with the gathered information and show the working out (i.e. calculations) for the quantitative results.

1. Preliminary Report
Your preliminary report needs to identify 20 landmarks from 4 different categories. The identification process includes what needs to be protected and the risk associated with the landmark. Hint: in order to assess the risk you may need to identify potential breaches in security.

Remember: a landmark is usually a building, not a single business. You need to identify all the tenants in that landmark. E.g. the MLC Centre in Sydney.

This report will be 2000 words in length. You need to submit a template, either in excel or a table in a word document that shows the categories of data you are collecting for analysis.

Your group of 4 will be allocated a city. You will need to define the boundary area of the designated “cities”. See [http://www.abs.gov.au](http://www.abs.gov.au) for helpful information. E.g. will you use a postcode level of detail, a statistical local area, or urban centre location, or other.

2. Final Report
Your final report identifies 20 landmarks from at least 4 categories. Your report should not only identify what needs to be “protected” and the “risk” associated with a given landmark, but it also should address the notion of **how to manage the risk**. In brief, you are to devise a “risk
management” report for the chosen area of your study. The report should be useful to both local government and local businesses.

You may choose to store the information in a database or excel spreadsheet but this must be appended to your final report. Both the spreadsheet/database and the report must be uploaded to UOW e-Learning space (one per group only).

Each member of the group needs to clearly identify which section of the report he/she completed. This is to be shown in the Appendix. In addition, a peer review will be conducted during the Week 12 tutorial. Example roles for this assignment that students may wish to take on include: market researcher, market analyst, risk assessor, risk manager. All students must contribute to the writing of the final document. This report will be 6000 words in length.

3. Security Policy – Case Study

Security policies for organizations are vital. However, many Small-to-Medium Enterprises (SMEs) have either ill-defined, incomplete, or no security policies whatsoever. Your task is to evaluate three (3) policies and provide recommendations on the completeness and appropriateness of each. If the policies are incomplete, you may provide a revision; if the policies are lacking, you may add to these. Maximum 3000 words, excluding policies.

You will be allocated a set of policies.

To be eligible for a Pass in this subject a student must achieve a mark of at least 40% in the final exam. Students who fail to achieve this minimum mark will be given a TF (Technical Fail) for this subject.

Procedures for the return of assessment items:
Assessment items will be returned in tutorials.

Penalties for late submission of assessment items:
Penalties apply to all late work, except if special consideration has been granted. Late submissions will attract a penalty of 25% of the assessment mark per day including weekends. Work more than four (4) days late will be awarded a mark of zero.

Supplementary Exams
Supplementary Exams will be dealt with in accordance with student academic consideration policy (http://www.uow.edu.au/handbook/courserules/specialconsideration.html) 6.2 Timing of Supplementary Exams.

While the School normally grants supplementary exams when the student does not sit the standard exam for an acceptable reason, each case will be assessed on its own merit and there is no guarantee a supplementary exam will be granted. If a supplementary exam is granted, you will normally be notified via SOLS Mail the time and date of this supplementary exam. You must follow the instructions given in the email message.

Please note that if this is your last session and you are granted a supplementary exam, be aware that your results will not be processed in time to meet the graduation deadline.

Special Consideration Policy
The School recognises that it has a responsibility to ensure equity and consistency across its subjects for all students. Sometimes, in exceptional circumstances, students need to apply for student special consideration in order to complete all assessable work.

The University applies strict criteria to the granting of special consideration. Before applying for student special consideration, students should carefully read the University’s policy which can be found at: http://www.uow.edu.au/handbook/courserules/specialconsideration.html

As an example: If a student requires an extension of time for the completion of an assignment this may be granted in certain circumstances. A request for an extension must be made to the Subject
Coordinator via SOLs before the due date.

**Plagiarism**

When you submit an assessment task, you are declaring the following:

1. It is your own work and you did not collaborate with or copy from others.
2. You have read and understand your responsibilities under the University of Wollongong's policy on plagiarism.
3. You have not plagiarised from published work (including the internet). Where you have used the work from others, you have referenced it in the text and provided a reference list at the end of the assignment.

Students must remember that:

- Plagiarism will not be tolerated.
- Students are responsible for submitting original work for assessment, without plagiarising or cheating, abiding by the University’s policies on Plagiarism as set out in the University Handbook under University Policy Directory and in Faculty handbooks and subject guides. Plagiarism has led to the expulsion from the University.

**Student Academic Grievance Policy**

The School aims to provide a fair, equitable and productive learning environment for all its students. The Student Academic Grievance Policy seeks to support the achievement of this goal by providing a transparent and consistent process for resolving student academic grievances.

Any student who has a grievance over a result should obtain a Faculty of Informatics Appeal Against Decision or Action Affecting Academic Experience form from the Informatics Student Enquiry Centre. ([http://www.uow.edu.au/content/groups/public/@web/@inf/@faculty/documents/doc/uow017433.pdf](http://www.uow.edu.au/content/groups/public/@web/@inf/@faculty/documents/doc/uow017433.pdf))

The student should firstly take the form to the marker/lecturer to discuss the matter and, if the student is still not satisfied, s/he should take the next step as outlined on the form.

Once the grievance has been considered by the Faculty, if the student still feels the situation has not been fully resolved s/he may consult the Dean of Students. However, the Dean of Students can have no input into the academic judgment of the lecturer and can only review the grievance to ensure proper procedure has been followed.

**Relevant University Policies, procedures and students services:**

For more information students must refer to the Faculty handbook, online references or consult the UOW policy in full at [http://www.uow.edu.au/handbook/courserules/studacgrievpol.html](http://www.uow.edu.au/handbook/courserules/studacgrievpol.html) which contains a range of policies on educational issues and student matters.
This outline should be read in conjunction with the following documents:

<table>
<thead>
<tr>
<th>Code of Practice - Teaching and Assessment</th>
<th>Code of Practice - Students</th>
</tr>
</thead>
</table>

<table>
<thead>
<tr>
<th>Code of Practice-Honours</th>
<th>Acknowledgement Practice Plagiarism will not be tolerated:</th>
</tr>
</thead>
</table>

<table>
<thead>
<tr>
<th>Key Dates</th>
<th>Special Consideration Policy:</th>
</tr>
</thead>
</table>

<table>
<thead>
<tr>
<th>Course Progress Policy:</th>
<th>Graduate Qualities Policy:</th>
</tr>
</thead>
</table>

<table>
<thead>
<tr>
<th>Academic Grievance Policy (Coursework and honours students)</th>
<th>Non-Discriminatory Language Practice and Presentation</th>
</tr>
</thead>
</table>

<table>
<thead>
<tr>
<th>Occupational Health and Safety</th>
<th>Intellectual Property Policy</th>
</tr>
</thead>
</table>

<table>
<thead>
<tr>
<th>Human Research Ethics:</th>
<th>Rules for student conduct and discipline:</th>
</tr>
</thead>
</table>

<table>
<thead>
<tr>
<th>Information Literacies Introduction Program</th>
<th>Informatics Faculty Librarian, Ms Annette Meldrum, phone: 4221 4637, email: <a href="mailto:ameldrum@uow.edu.au">ameldrum@uow.edu.au</a></th>
</tr>
</thead>
</table>

<table>
<thead>
<tr>
<th>Student Support Services:</th>
<th>SCSSE SISAT Internet Access &amp; Student Resource Centre</th>
</tr>
</thead>
<tbody>
<tr>
<td>Informatics Faculty SEDLO (Student Equity and Diversity Liaison Officers) Virginie Schmelitschek, phone 4221 3833, <a href="mailto:virginie@uow.edu.au">virginie@uow.edu.au</a></td>
<td></td>
</tr>
</tbody>
</table>