REPORT OF THE SENATE COMMITTEE ON UNIVERSITY PLANNING

(SCUP)

Fall 2012 Entrance Standards for Undergraduate First-Year Admissions

Five-Year Enrolment Projections

Report on Year One Class Entering Averages

Vice-Provost's Report on Faculty Recruitment and Retention

Annual Report of the Working Group on Information Security (WGIS)

FOR APPROVAL

1. **Fall 2012 Entrance Standards for Undergraduate First-Year Admissions**

Recommended: That Senate approve the targets and processes for first-year, first-entry undergraduate enrolment for the constituent University and Affiliated University Colleges and outlined in **Appendix 1**.

Background

See **Appendix 1**.

2. **Five-Year Enrolment Projections**

Recommended: That five-year enrolment projections (**Appendix 2**) be used for purposes of tuition revenue estimates in the University's budget projections.

See **Appendix 2**.

FOR INFORMATION

3. **Report on Year One Class Entering Averages**

See **Appendix 3**.

4. **Vice-Provost's Report on Faculty Recruitment and Retention**

See **Appendix 4**.

5. **Annual Report of the Working Group on Information Security (WGIS)**

See **Appendix 5**.

The University of Western Ontario

SCUP's Subcommittee on Enrolment Planning and Policy (SUEPP)

Fall 2012 Entrance Standards for First-Year Undergraduate Admissions

---

A. Constituent University

At its November 2010 meeting, Senate approved SUEPP's recommendation on Western's enrolment strategy for the coming years. The specifics of the recommendations were as follows:

1. Western maintain the current (i.e. fall 2010) minimum entrance requirement for first-year admission at 83% mid-year grade (and 81% final grade). For selected limited-enrolment programs, based on annual reviews by the Provost and the Deans, the entrance requirements could be higher.

2. The approach of using the common entrance requirement be continued. The result of this approach is that student demand/choice drives program-specific enrolments.

3. By the end of the upcoming 4-year planning period, we work to increase our first-year international enrolment to 400 from the current level of 150.

4. We continue to monitor the gap in entrance requirements between Western and the Ontario average -- with the objective of maintaining the current gap.

5. We continue to monitor the size of our overall first-year class -- in order to ensure that the undergraduate population does not reach a level that cannot be accommodated within our current physical infrastructure.

6. We continue with our First-Year Residence Guarantee initiative -- with the understanding that we may need to expand our residence capacity.

7. The Provost encourage the Faculties (through the Deans) to develop upper-year entry niche undergraduate programs, including 2+2 programs and partnership arrangements.

8. Western continue with the graduate enrolment aspirations outlined in *Engaging the Future*, and continue the doctoral expansion trends of the past decade. In 2009-10, full-time graduate enrolments comprised of 17% of the total full-time enrolment at Western.

9. As a research-intensive institution, enrolment planning will include the objective of maintaining or increasing the relative proportion of graduate student enrolments (currently 17%).

Update on Fall 2011 Admissions
The minimum entrance requirement was 83% (mid-year) and 82% (final).
First-year international enrolment totaled 347 students.

Plans For Fall 2012 Admissions
For the fall 2012 admissions cycle, the above recommendations will be followed for the Constituent University and it is expected that the entrance requirement will be no less than 83% mid-year grade and 82% final grade. The Constituent University's 2012-13 first-year class is planned to be 4,800 students, with an international student target of 450 students.

B. <u>Affiliated University Colleges</u>

For fall 2011, entrance requirements (final grades) at the Affiliated University Colleges were as follows:

Brescia	76%
Huron	76%
King's	76%

As a follow-up to the Constituent University's strategy on enrolment planning, the Affiliated University Colleges have committed to narrowing the gap in entrance requirements between the Colleges and the Constituent University. The specifics of the Colleges' strategy are as follows:

1. For 2012-13, the entrance requirement (final grades) at each Affiliated University College will be 77.0% at Huron and King's, 76.0% at Brescia.

2. By 2014-15, the Colleges will increase their entrance requirements (final grades) to 78%, as follows:

	Brescia	Huron	King's
2013-14	tbd	77.0%	77.0%
2014-15	78.0%	78.0%	78.0%

3. As is the case at present, in situations where additional assessment is required (for students with exceptional/unusual circumstances), the Colleges may admit students with grades below the minimum requirement. The proportion of the entering class with final averages below the minimum requirement (e.g. 78% in 2014-15) shall not exceed 2%.

4. The 2012-13 first-year targets for the Affiliated University Colleges are as follows:

Brescia	308
Huron	405
King's	860

5. The Affiliated University Colleges will be bound to the minimum entrance requirements established by the Constituent University for limited-enrolment programs, where applicable, including BHSc and Kinesiology.

SUMMARY OF ENROLMENT FORECAST

		Actual					Projected				
		2007-08	2008-09	2009-10	2010-11	2011-12	2012-13	2013-14	2014-15	2015-16	2016-17
1	**Constituent University**										
2	**Full-Time Undergraduates**										
3	Arts & Humanities	1,358	1,312	1,275	1,260	1,232	1,238	1,266	1,279	1,287	1,296
4	Business (HBA)	635	706	812	935	979	1,065	1,130	1,130	1,130	1,130
5	Dentistry	247	249	251	251	260	266	264	264	264	264
6	Education	803	728	726	732	700	668	668	668	668	668
7	Engineering	1,138	1,098	1,132	1,147	1,262	1,303	1,346	1,378	1,383	1,392
8	Health Sciences										
9	BHSc Program	1,057	1,056	1,098	1,117	1,185	1,142	1,187	1,207	1,222	1,237
10	Kinesiology	1,148	1,159	1,194	1,204	1,246	1,222	1,235	1,249	1,246	1,246
11	Nursing	746	781	777	797	808	805	805	805	805	805
12	Therapies	27	39	40	0	0	0	0	0	0	0
13	Sub-Total	2,978	3,035	3,109	3,118	3,239	3,169	3,227	3,261	3,273	3,288
14	Law	472	456	467	458	465	450	445	450	450	450
15	Media, Information, & Tech	810	915	890	972	963	975	948	925	918	918
16	Medicine										
17	MD Program	552	569	591	621	646	672	684	684	684	684
18	BMedSci Program	758	603	591	653	688	828	892	892	892	892
19	Music	555	555	535	535	527	529	538	547	556	558
20	Science	3,693	3,795	3,737	4,020	4,222	4,236	4,312	4,356	4,358	4,385
21	Social Science	5,941	6,035	6,408	6,433	6,618	6,686	6,723	6,732	6,682	6,666
22	**Total Full-Time Undergraduates**	**19,940**	**20,056**	**20,524**	**21,135**	**21,801**	**22,085**	**22,443**	**22,566**	**22,545**	**22,591**
23	Concurrent Programs	68	81	110	121	144	155	155	155	155	155
24	Medical Residents	674	685	725	798	810	810	810	810	810	810
25	**Full-Time Graduates**										
26	Masters	2,547	2,606	2,648	2,800	2,823	2,981	3,229	3,305	3,370	3,405
27	Ph.D.	1,516	1,614	1,771	1,904	1,947	2,022	2,100	2,175	2,220	2,240
28	**Total Full-Time Graduates**	**4,063**	**4,220**	**4,419**	**4,704**	**4,770**	**5,003**	**5,329**	**5,480**	**5,590**	**5,645**
29	**Total Full-Time Enrolment**	**24,745**	**25,042**	**25,778**	**26,758**	**27,525**	**28,053**	**28,737**	**29,011**	**29,100**	**29,201**
30	**Part-Time FTEs**										
31	Undergraduate	2,199	2,067	2,134	2,197	2,243	2,250	2,300	2,300	2,300	2,300
32	Education (AQs)	897	929	922	803	745	725	725	725	725	725
33	Masters	120	130	129	134	140	140	140	140	140	140
34	Ph.D.	20	29	24	21	26	25	25	25	25	25
35	**Total Part-Time FTEs**	**3,236**	**3,155**	**3,209**	**3,155**	**3,154**	**3,140**	**3,190**	**3,190**	**3,190**	**3,190**
36	**Total Constituent FTEs**	**27,981**	**28,197**	**28,987**	**29,913**	**30,679**	**31,193**	**31,927**	**32,201**	**32,290**	**32,391**
37	**Affiliated University Colleges**										
38	**Full-Time Undergraduates**										
39	Brescia	912	918	934	964	1,067	1,102	1,161	1,216	1,250	1,277
40	Huron	1,088	1,143	1,235	1,254	1,272	1,250	1,250	1,250	1,250	1,250
41	King's	3,088	3,118	3,122	3,216	3,286	3,246	3,252	3,272	3,309	3,345
42	**Total Full-Time Undergraduates**	**5,088**	**5,179**	**5,291**	**5,434**	**5,625**	**5,598**	**5,663**	**5,738**	**5,809**	**5,872**
43	**Part-Time Undergraduate FTEs**										
44	Brescia	80	81	82	83	94	90	90	90	90	90
45	Huron	45	54	57	56	70	55	55	55	55	55
46	King's	260	238	249	245	252	245	245	245	245	245
47	**Total Part-Time FTEs**	**385**	**373**	**388**	**384**	**416**	**390**	**390**	**390**	**390**	**390**
48	**Graduate FTEs**										
49	Brescia	13	27	26	30	29	30	30	30	30	30
50	Huron	12	15	13	12	14	20	20	20	20	20
51	King's	24	33	30	34	31	34	34	34	34	34
52	**Total Graduate FTEs**	**49**	**75**	**69**	**76**	**74**	**84**	**84**	**84**	**84**	**84**
53	**Total Affiliate FTEs**	**5,522**	**5,627**	**5,748**	**5,894**	**6,115**	**6,072**	**6,137**	**6,212**	**6,283**	**6,346**
54	**Total UWO FTEs**	**33,503**	**33,824**	**34,735**	**35,807**	**36,794**	**37,265**	**38,064**	**38,413**	**38,573**	**38,737**

SUMMARY OF ENROLMENT FORECAST

		Actual					Projected				
		2007-08	2008-09	2009-10	2010-11	2011-12	2012-13	2013-14	2014-15	2015-16	2016-17
	Rows 55 to 86 Included above										
55	**International Students**										
56	Constituent Full-Time										
57	Undergraduates	618	573	631	703	923	1,295	1,670	2,010	2,010	2,010
58	Medical Residents	119	120	109	121	127	127	127	127	127	127
59	Masters (excluding Ivey)	245	254	320	378	452	417	431	442	450	450
60	MBA (Regular), Ivey MSc	17	21	17	27	30	30	42	44	44	44
61	Executive MBA	62	71	71	80	44	56	67	70	70	70
62	Ph.D.	341	361	426	463	510	514	521	530	530	530
63	**Year 1 Only**										
64	**Constituent**										
65	Arts & Humanities	297	312	259	258	272	275	300	300	300	300
66	Engineering	320	327	343	351	416	375	400	400	400	400
67	Health Sciences										
68	BHSc Program	283	273	270	273	314	275	300	300	300	300
69	Kinesiology	365	349	347	330	366	350	350	350	350	350
70	Nursing	127	129	130	133	128	125	125	125	125	125
71	Media, Information, & Tech	287	363	333	361	334	330	330	330	330	330
72	MOS Program	703	727	773	717	846	820	790	790	790	790
73	Music	151	153	135	141	142	150	150	150	150	150
74	Science	1,084	1,097	1,106	1,366	1,388	1,325	1,380	1,380	1,380	1,380
75	Social Science	795	789	757	794	850	775	775	775	775	775
76	**Total Year 1 - Constituent**	**4,412**	**4,519**	**4,453**	**4,724**	**5,056**	**4,800**	**4,900**	**4,900**	**4,900**	**4,900**
77	**Affiliated University Colleges**										
78	Brescia	290	254	268	260	292	308	328	326	332	339
79	Huron	383	406	397	404	381	405	405	405	405	405
80	King's	858	949	946	916	878	860	880	895	910	925
81	**Total Year 1 - Affiliates**	**1,531**	**1,609**	**1,611**	**1,580**	**1,551**	**1,573**	**1,613**	**1,626**	**1,647**	**1,669**
82	**Total UWO Year 1**	**5,943**	**6,128**	**6,064**	**6,304**	**6,607**	**6,373**	**6,513**	**6,526**	**6,547**	**6,569**
83	**Masters**										
84	All Programs (excluding MBAs)	2,115	2,204	2,262	2,364	2,380	2,593	2,789	2,855	2,920	2,955
85	Ivey (excl EMBA)	168	162	157	188	183	167	208	215	215	215
86	Executive MBA	264	240	229	248	260	221	232	235	235	235

For Information

87	Year 1 International Students	101	122	120	146	347	450	450	500	500	500

The University of Western Ontario

Year 1 Class and Entering Averages

SCUP – March 5, 2012

Context

- Western continues Approach using "Standard Minimum Entrance Requirement"
  - Fall 2011 83.0%
  - Fall 2010 83.0%
  - Fall 2009 83.0%
  - Fall 2008 82.5%
  - Fall 2007 82.0%
  - Fall 2006 81.0%
  - Fall 2005 80.5%
  - Fall 2004 80.5%
  - Fall 2003 83.0% (peak Double Cohort year)
  - Fall 2002 79.5%
  - Fall 2001 77.0%

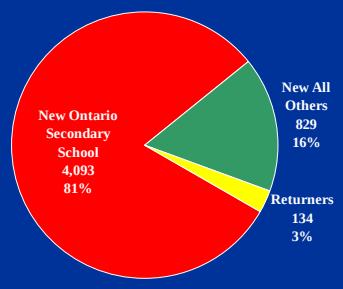
Student Profile:

Applicant Type and Geographical Origin

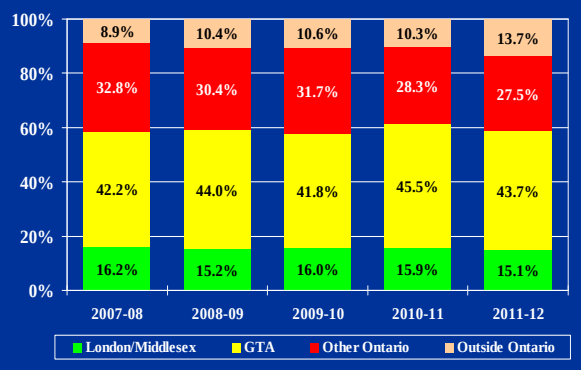
Constituent University

2011-12 Year 1 Students by Applicant Type
Constituent University

Total Year 1 = 5,056

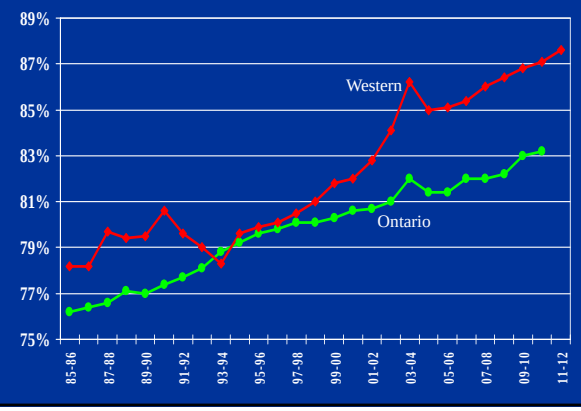


Geographical Origin of Year 1 Students
Constituent University

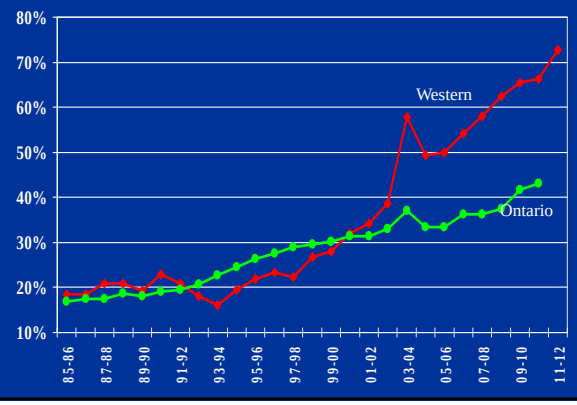


Entering Grades of New Ontario Secondary School Students

Average Entering Grade

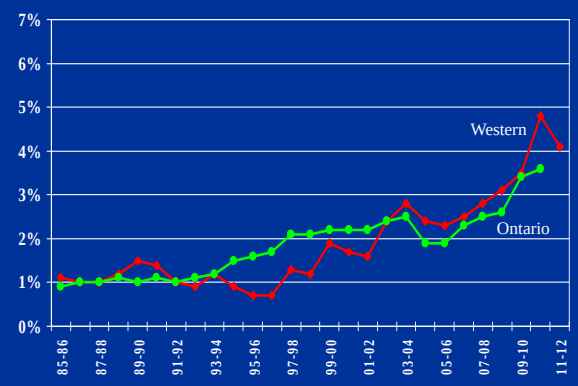


Proportion with Entering Grades of 85% or More

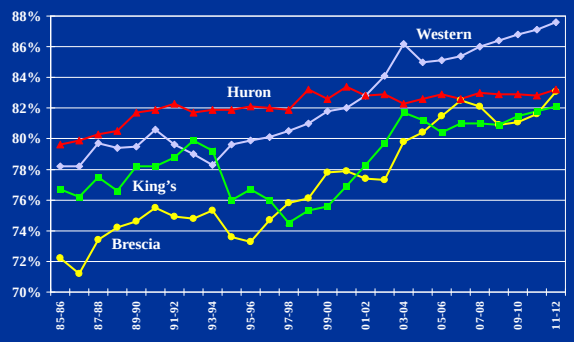


Proportion with Entering Grades of 90% or More

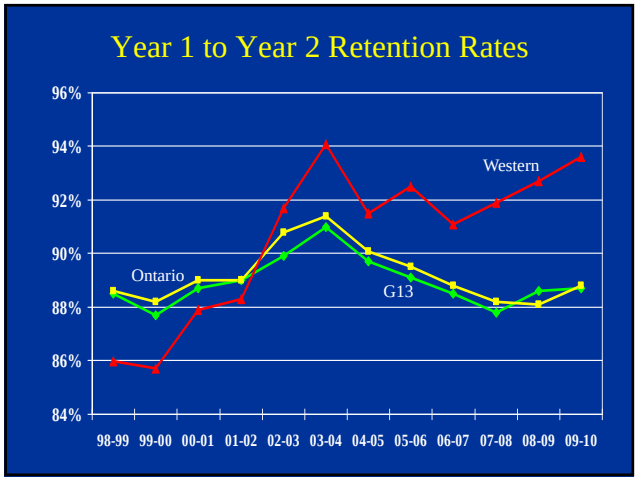
Proportion with Entering Grades of 95% or More

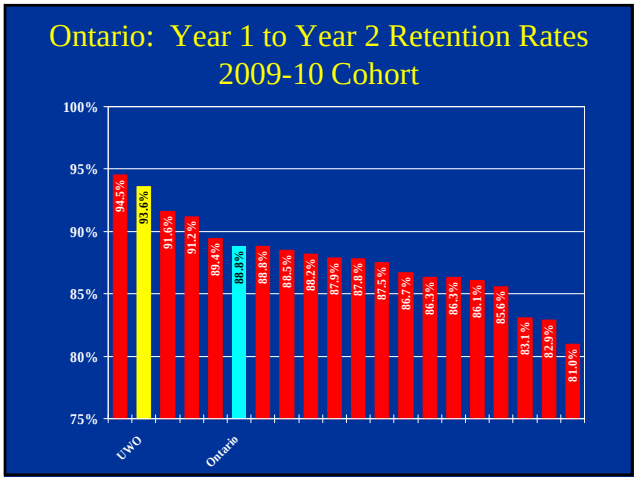


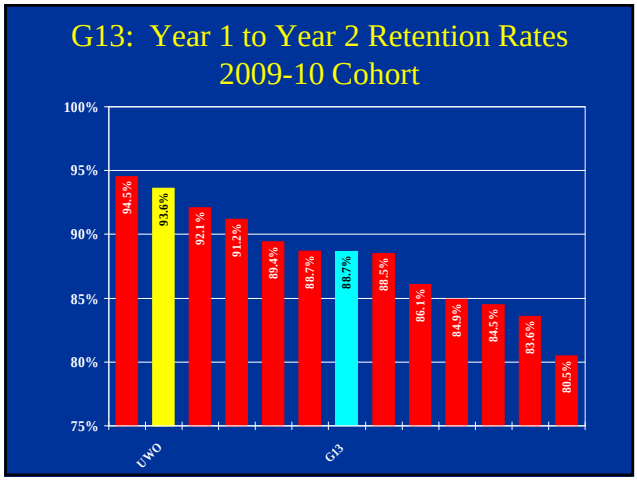
Average Entering Grade Western and Affiliated University Colleges



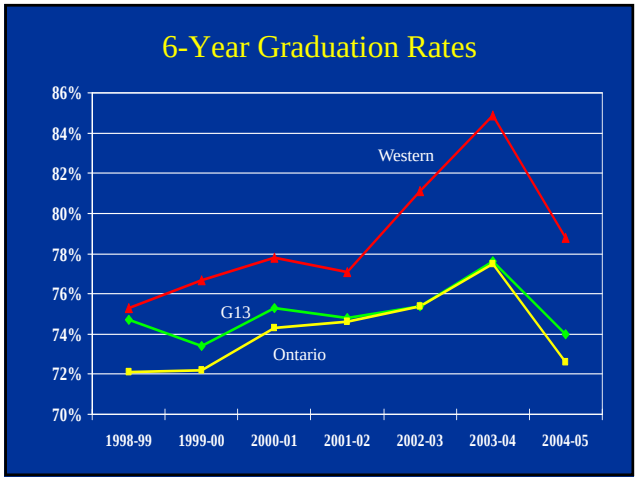
Retention Rates

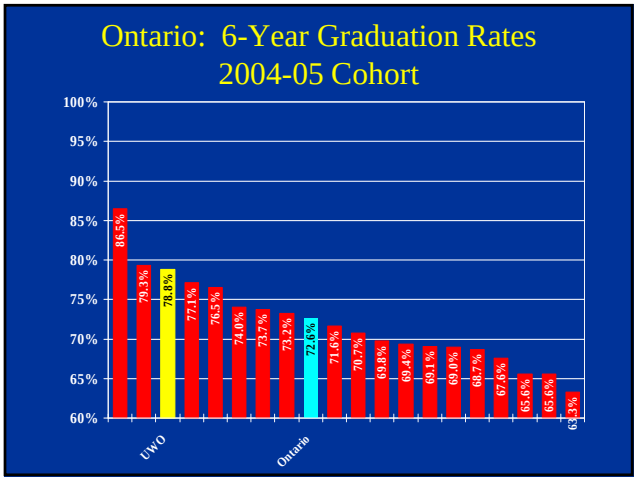


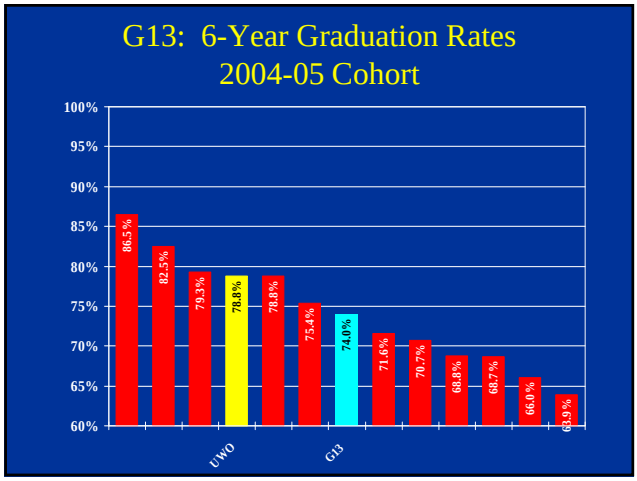




Graduation Rates



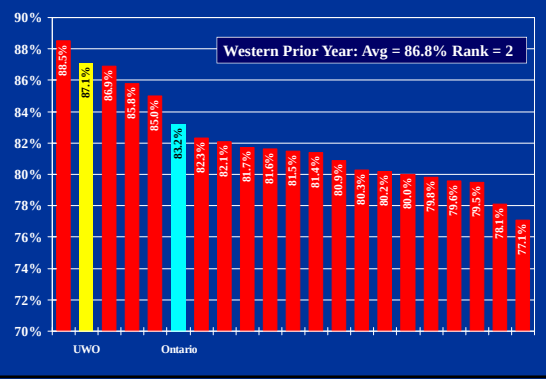




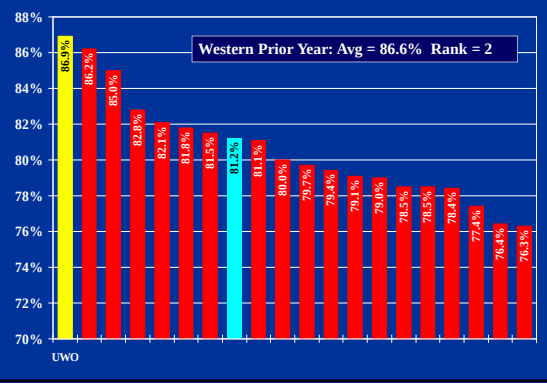
Entering Grades of New Ontario Secondary School Students by University and Program

2010-11

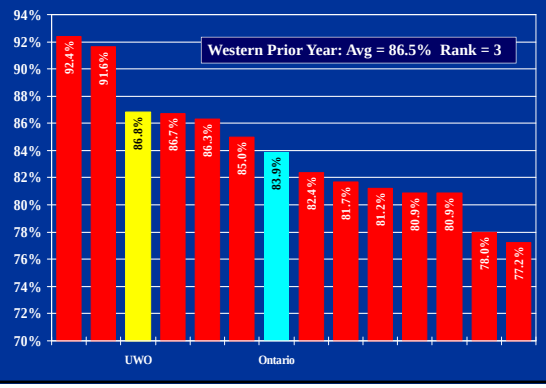
2010-11 Average Entering Grade
All Programs



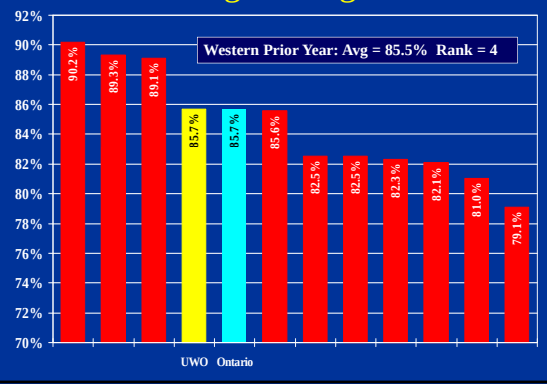
2010-11 Average Entering Grade
Arts & Humanities / Social Science

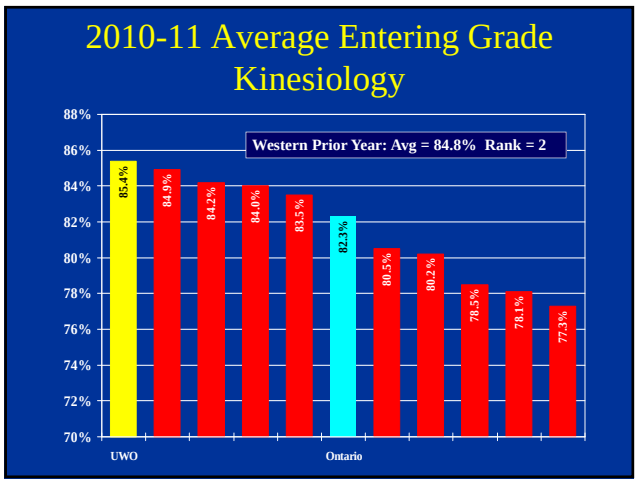


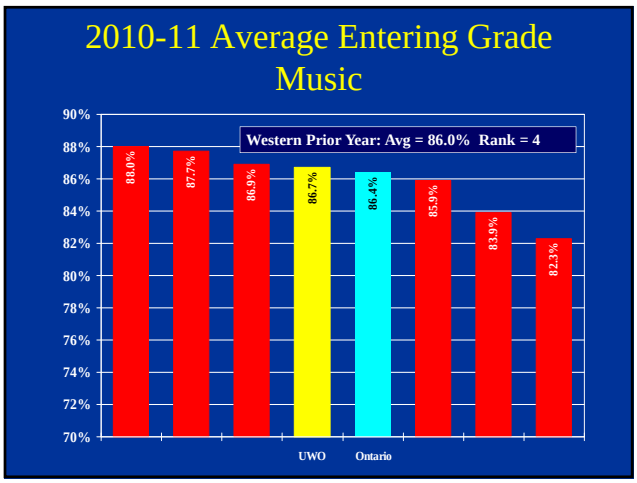
2010-11 Average Entering Grade
MOS / Commerce

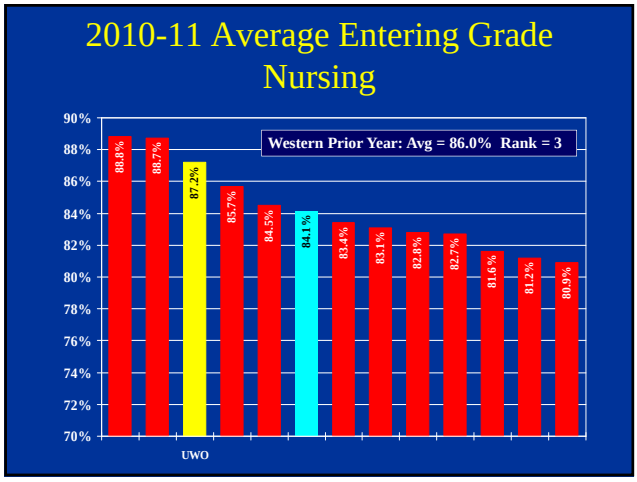


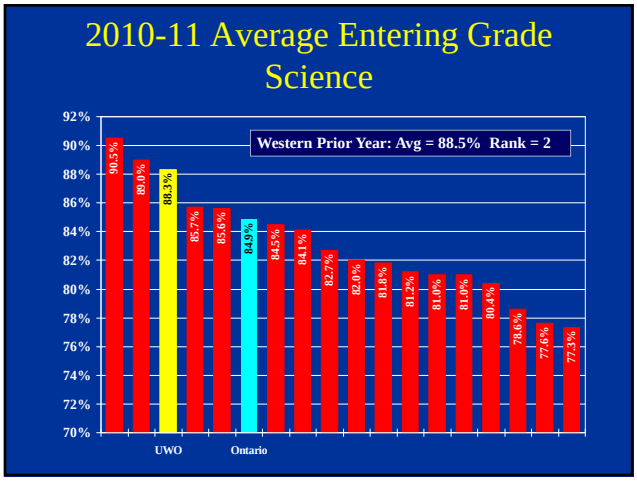
2010-11 Average Entering Grade
Engineering




2010-11 Average Entering Grade
Kinesiology
Western Prior Year: Avg = 84.8% Rank = 2
88%
86%
84%
82%
80%
78%
76%
74%
72%
70%
85.4%
84.9%
84.2%
84.0%
83.5%
82.3%
80.5%
80.2%
78.5%
78.1%
77.3%
UWO
Ontario


2010-11 Average Entering Grade
Music
Western Prior Year: Avg = 86.0% Rank = 4
90%
88%
86%
84%
82%
80%
78%
76%
74%
72%
70%
88.0%
87.7%
86.9%
86.7%
86.4%
85.9%
83.9%
82.3%
UWO
Ontario


2010-11 Average Entering Grade
Nursing
Western Prior Year: Avg = 86.0% Rank = 3
90%
88%
86%
84%
82%
80%
78%
76%
74%
72%
70%
88.8%
88.7%
87.2%
85.7%
84.5%
84.1%
83.4%
83.1%
82.8%
82.7%
81.6%
81.2%
80.9%
UWO


2010-11 Average Entering Grade
Science
Western Prior Year: Avg = 88.5% Rank = 2
92%
90%
88%
86%
84%
82%
80%
78%
76%
74%
72%
70%
90.5%
89.0%
88.3%
85.7%
85.6%
84.9%
84.5%
84.1%
82.7%
82.0%
81.8%
81.2%
81.0%
81.0%
80.4%
78.6%
77.6%
77.3%
UWO
Ontario

Western
UNIVERSITY · CANADA

Report to SCUP on Faculty Recruitment and Retention Office of the Vice Provost (Academic Planning, Policy and Faculty)

February 2012

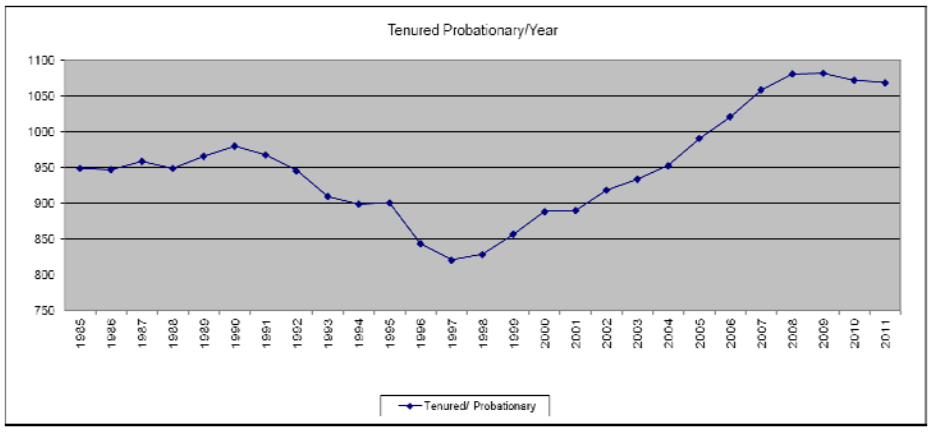
Available at http://www.uwo.ca/pvp/facultyrelations/index-vppf.html

Western

Contents:

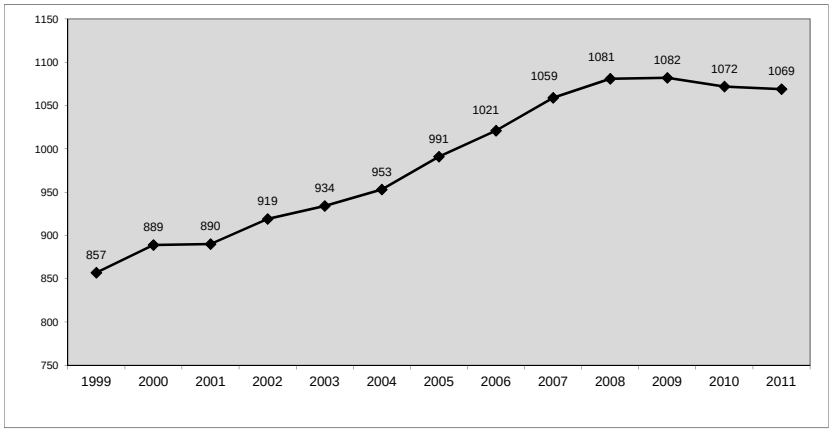
- Probationary and Tenured Faculty
  - Appointments
  - Resignations
  - Retirements
- Part-Time Faculty
- Limited-Term Faculty
- Full-Time Clinical Faculty

Probationary and Tenured Faculty at Western 1985 - 2011



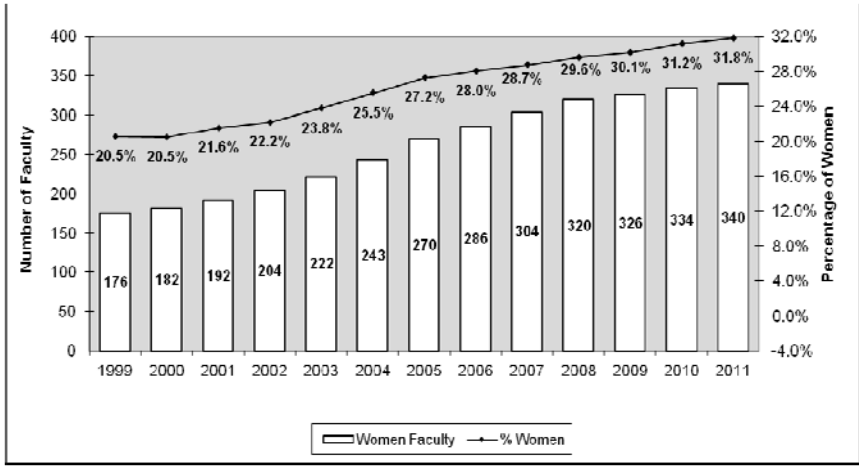
Source: Western Corporate Information 1985 – 1999
UCASS Data 1999 – 2010
Western Human Resources Information Systems 2011

Probationary and Tenured Faculty at Western, 1999 to 2011



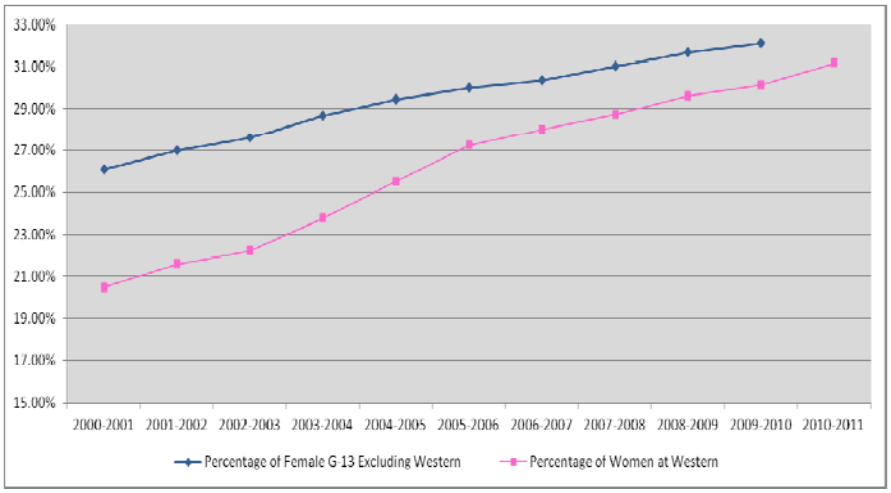
Source: UCASS Data for 1999 – 2010 (October 1);
Western Human Resources Information Systems for 2011 (October)
The 2007 data includes Robarts Scientists who became Probationary and Tenured on July 1, 2007.

Probationary and Tenured Women Faculty at Western, 1999 to 2011



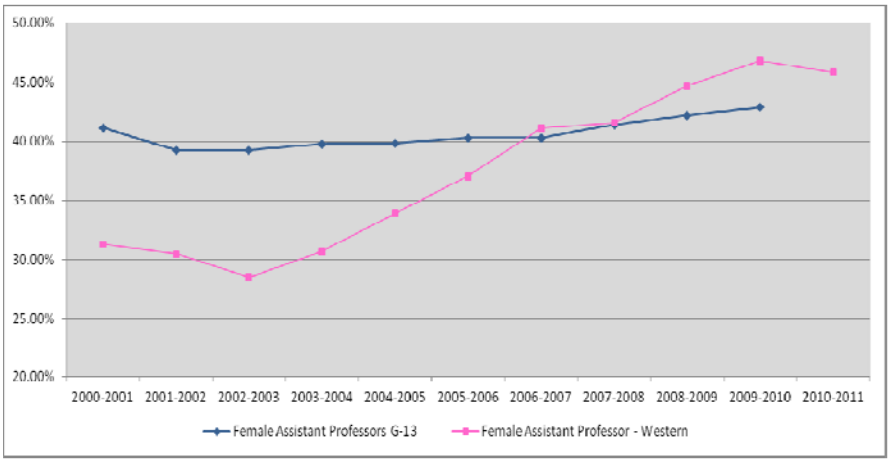
Source: UCASS Data for 1999 – 2010 (October 1);
Western Human Resources Information Systems 2011 (October)

Women as a Percentage of Tenured/Probationary Faculty: G-13 vs. Western



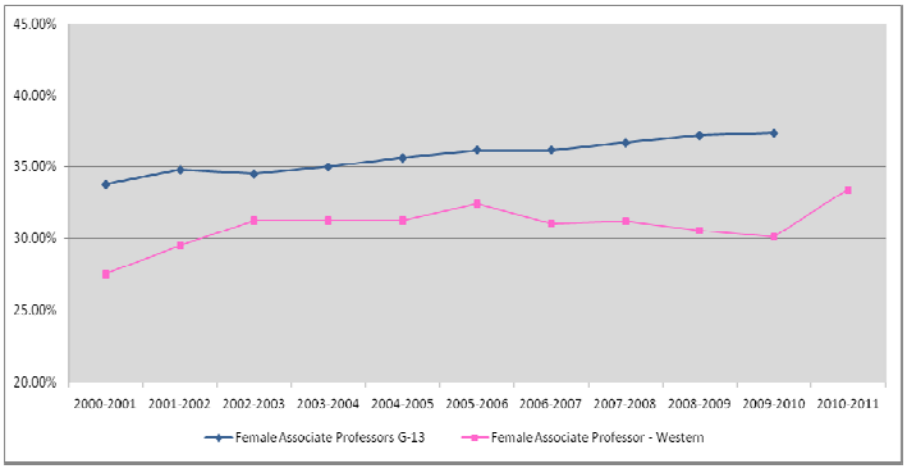
Source: UCASS Data

Women as a Percentage of Tenured/Probationary Faculty, Assistant Professor Rank: G-13 vs. Western



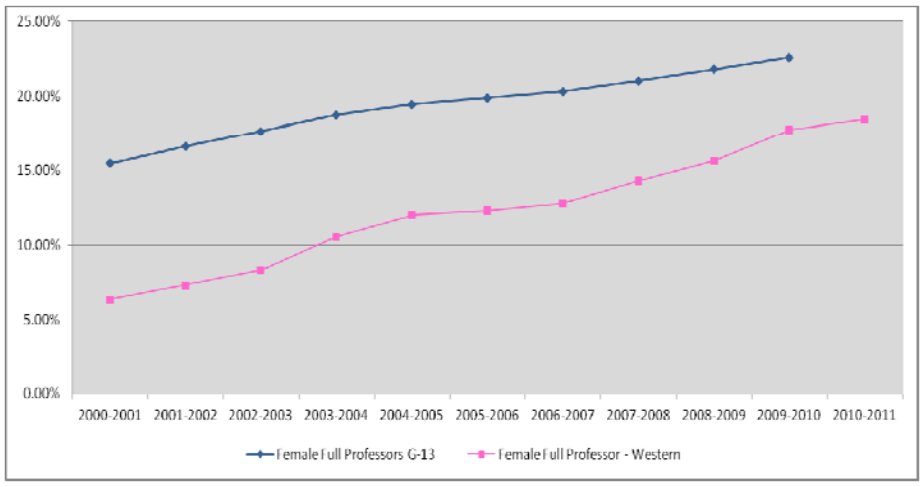
Source: UCASS Data

Women as a Percentage of Tenured/Probationary Faculty, Associate Professor Rank: G-13 vs. Western



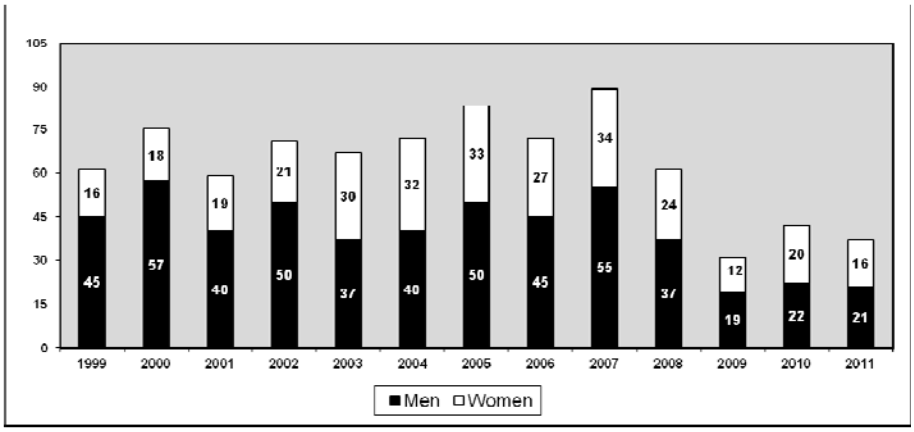
Source: UCASS Data

Women as a Percentage of Tenured/Probationary Faculty, Full Professor Rank: G-13 vs. Western



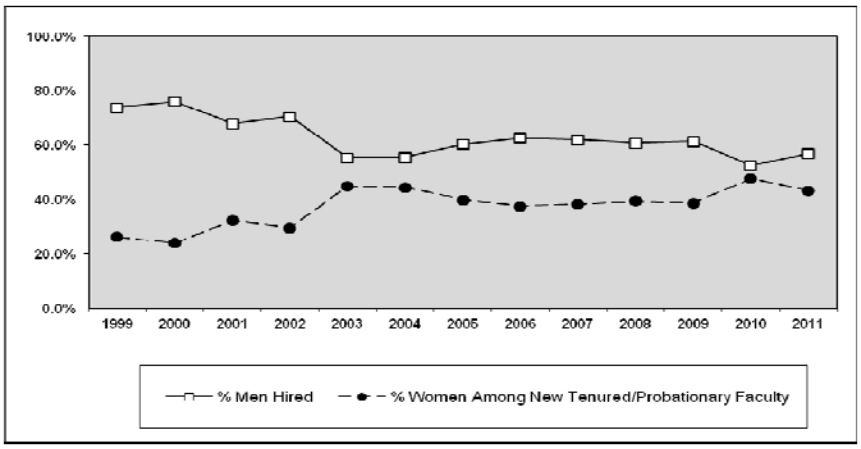
Source: UCASS Data

New Tenured & Probationary Faculty at Western by Gender (including those at Western previously in a Limited Term position): 1999 – 2011 Cohorts



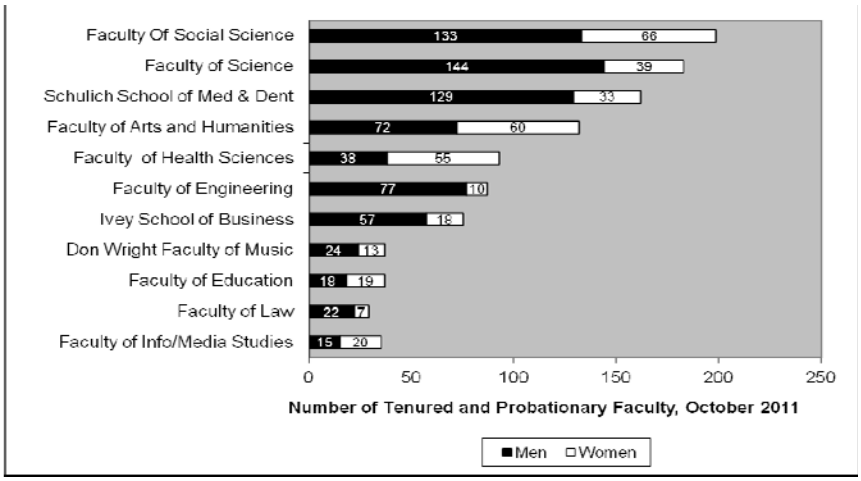
Source: UCASS Data for 1999 – 2010 (October 1);
Western Human Resources Information Systems 2011 (October)
Data excludes faculty joining from Robarts.

Percentage of New Tenured and Probationary Faculty at Western by Gender (including those at Western previously in a Limited Term position): 1999 – 2011



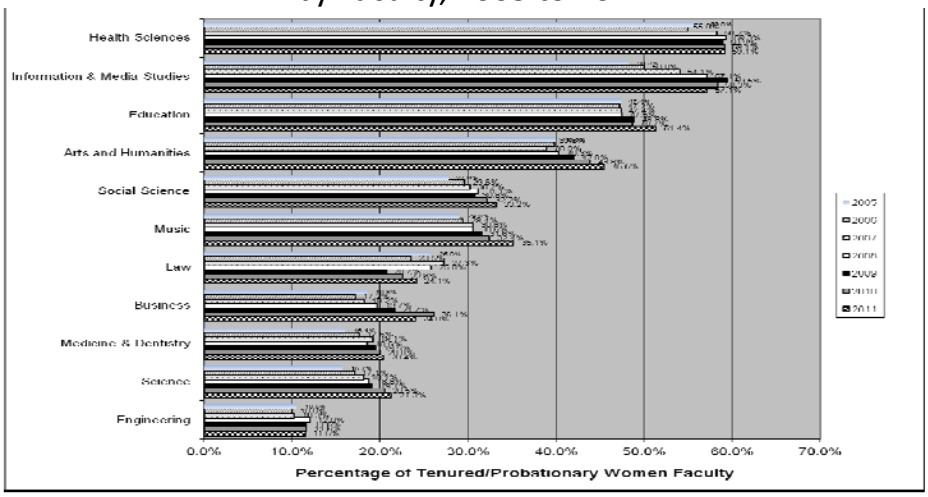
Source: UCASS Data for 1999 – 2010 (October 1)
Western Human Resources Information Systems 2011 (October)
Data excludes faculty joining from Robarts

Probationary and Tenured Faculty, by Faculty and Gender, October 2011



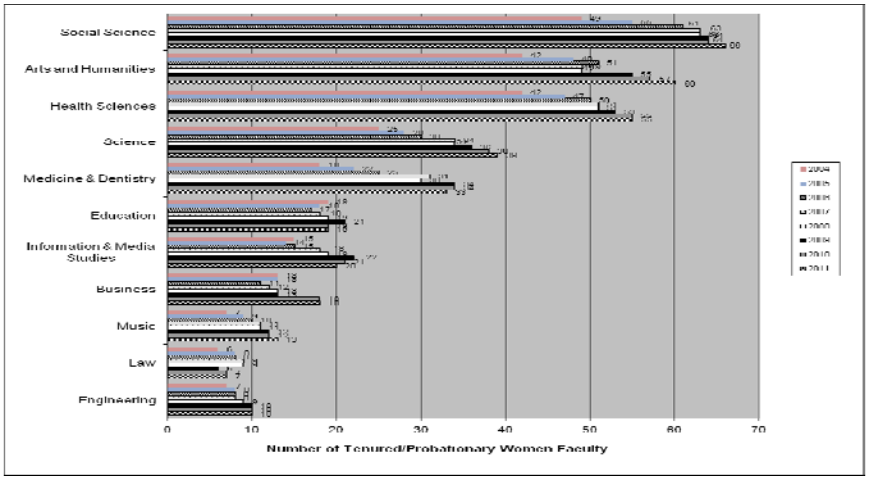
Source: Western Human Resources Information Systems for 2011 (October)

Percentage of Tenured/Probationary Women Faculty, by Faculty, 2005 to 2011



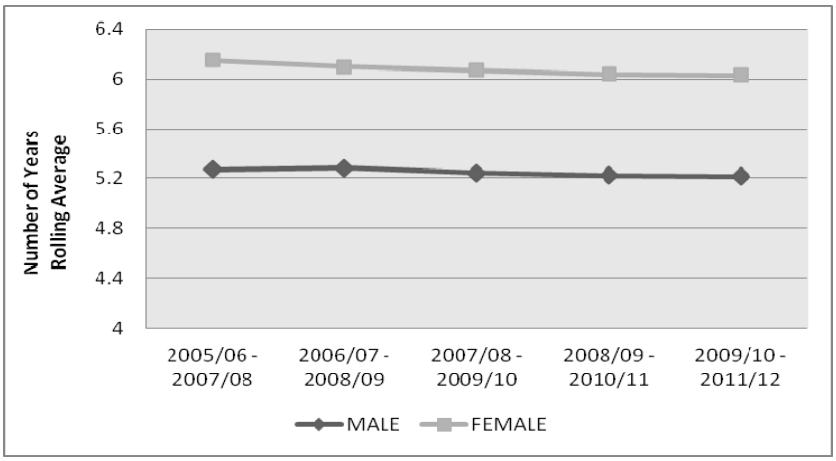
Source: UCASS data for 2005 – 2007 (October 1);
Western Human Resources Information System 2008 - 2011 (October).

Number of Tenured/Probationary Women Faculty, by Faculty, 2005-2011



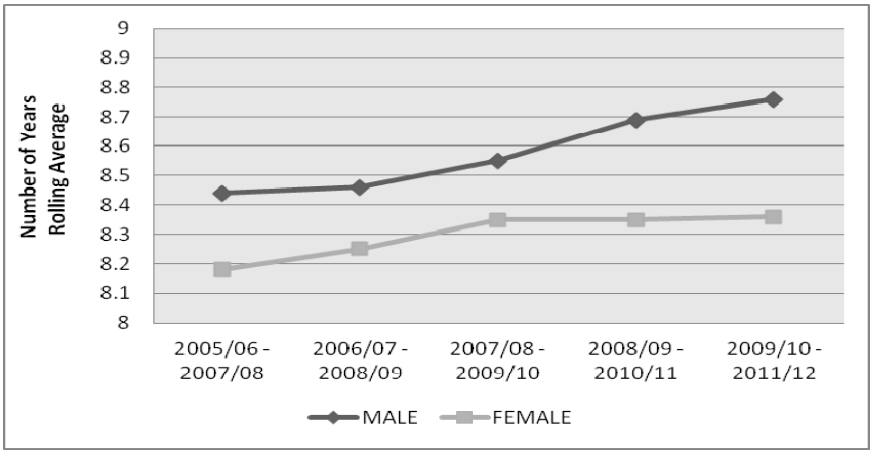
Source: UCASS data for 2005 - 2007;
Western Human Resources Information System 2008 - 2011 (October).

Average Time to Tenure from Full Time Start at Western



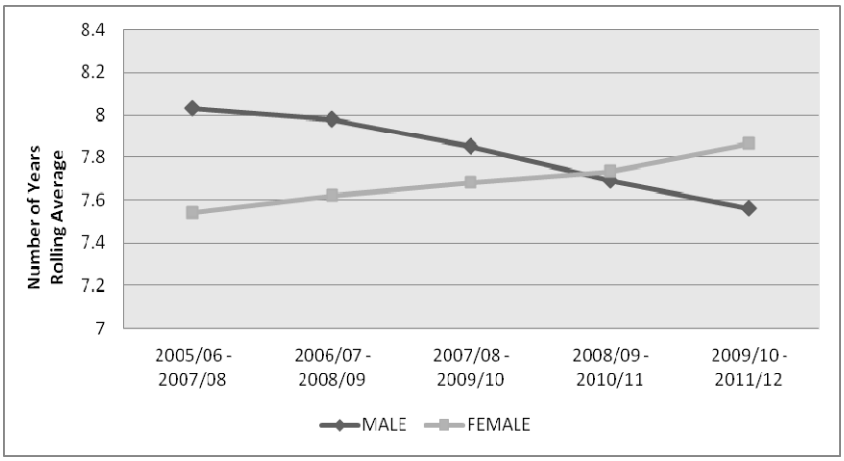
Source: Western Human Resources Information System 2005 – 2012
Excludes those hired into a tenured position

Average Time to Tenure from Highest Degree



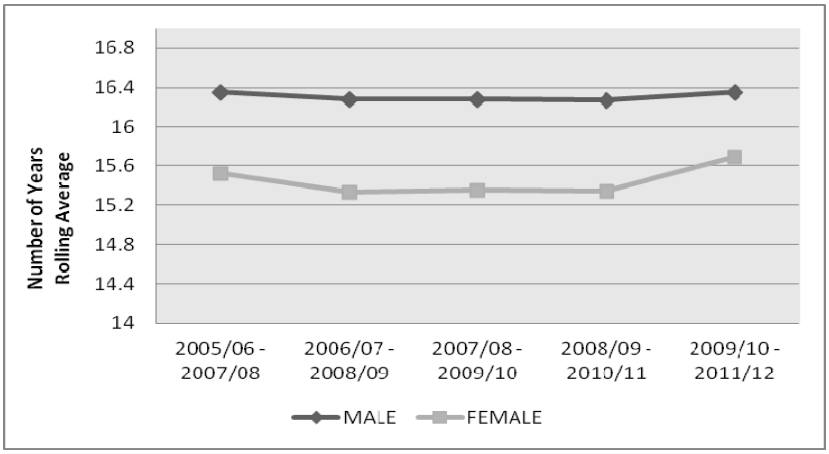
Source: Western Human Resources Information System 2005 – 2012
Excludes those hired into a tenured position

Average Time to Full Professor from Tenure



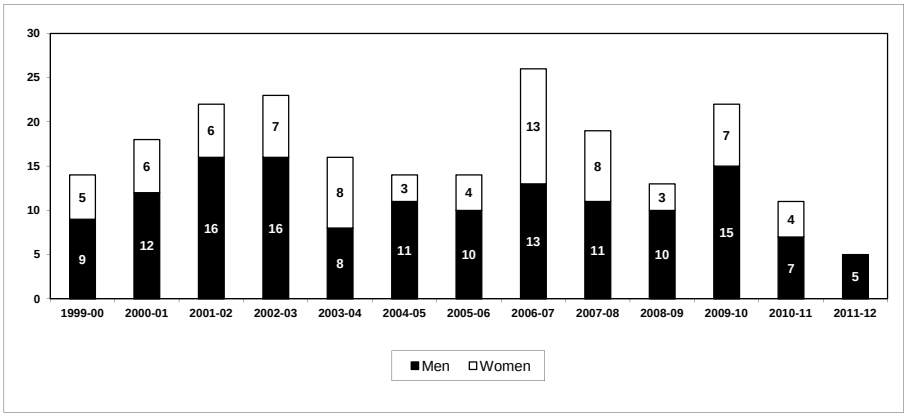
Source: Western Human Resources Information System 2005 – 2012
Excludes those already Full Professor at time of Tenure

Average of Time to Full Professor from Highest Degree



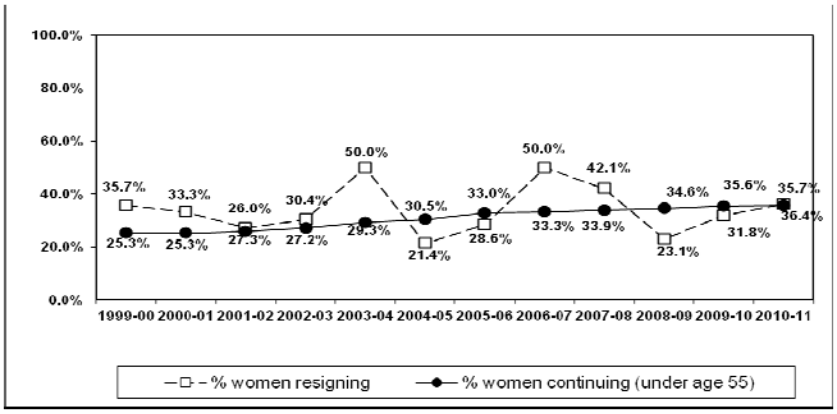
Source: Western Human Resources Information System 2005 – 2012
Excludes those already Full Professor at time of Tenure

Probationary & Tenured Faculty Resignations by Gender: 1999-2000 to 2011-12 (interim)



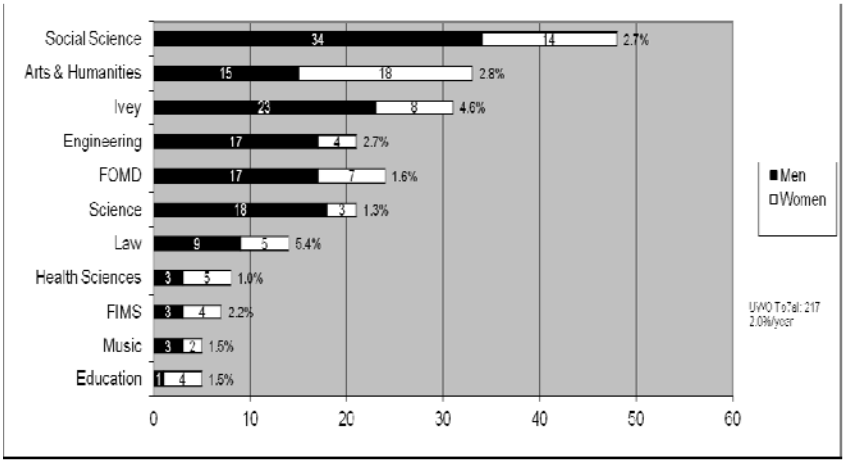
Source: Western Information Systems as of January 2012
Includes only faculty under age 55 at the time of resignation.

Women as a Percentage of Probationary & Tenured Faculty Resignations and Women as a Percentage of Continuing Population: 1999-2000 to 2010-2011



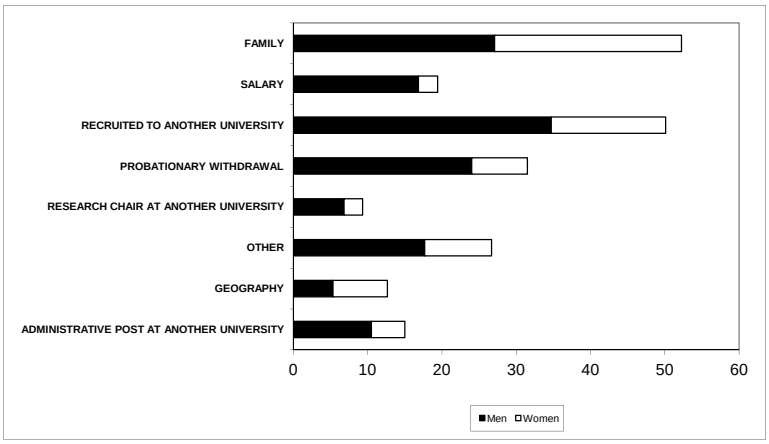
Source: Western Information Systems (October 2011) for resignation data and UCASS Data for 1999-2007, and Western's Human Resources Information Systems for 2007-11 for continuing population data.

Total Probationary & Tenured Resignations by Faculty: 1999-00 to 2010-11



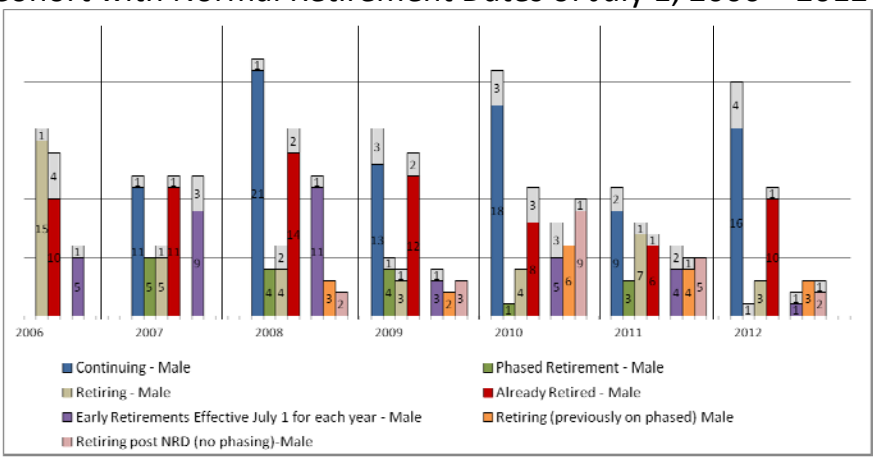
Source: Western's Human Resources Information Systems.
Percentages based on Tenured/Probationary faculty as of January 2012.

Probationary and Tenured Faculty Reasons for Leaving: 1999-00 to 2011-12 (Interim)



Source: Exit interviews conducted with the Faculty Member or Chair/Dean of the Department/Faculty and letters received from Faculty Member

Probationary and Tenured Faculty at Western: Cohort with Normal Retirement Dates of July 1, 2006 – 2012



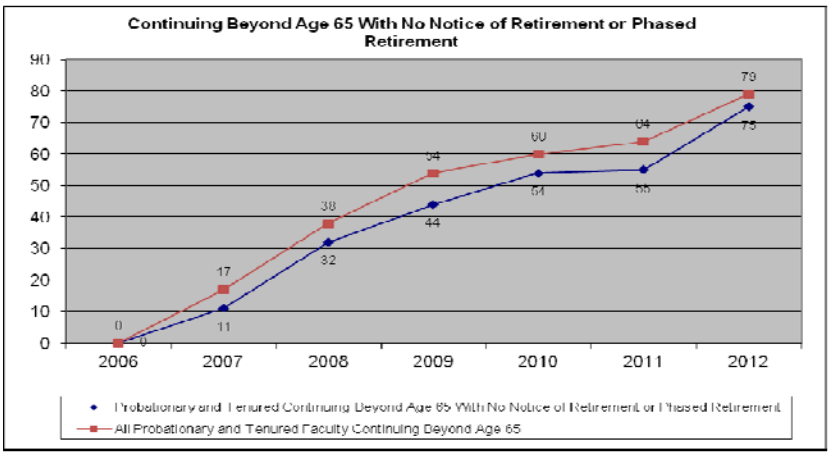
Source: Western Human Resources Information Systems

Probationary and Tenured Faculty at Western: Cohort Aged 60 or Greater

Age	2004	2005	2006	2007	2008	2009	2010
60	30	35	22	39	22	26	26
61	34	28	33	21	34	22	25
62	34	31	28	34	20	34	21
63	21	32	30	23	31	18	33
64	22	20	31	30	22	30	18
65	6	8	10	28	25	22	23
66	0	0	0	7	24	20	19
67	0	0	0	0	4	21	16
68	0	0	0	0	0	3	11
69	0	0	0	0	0	0	3
70	0	0	0	0	0	0	0
78	0	0	0	0	0	0	0
Total	**147**	**154**	**154**	**182**	**182**	**196**	**195**

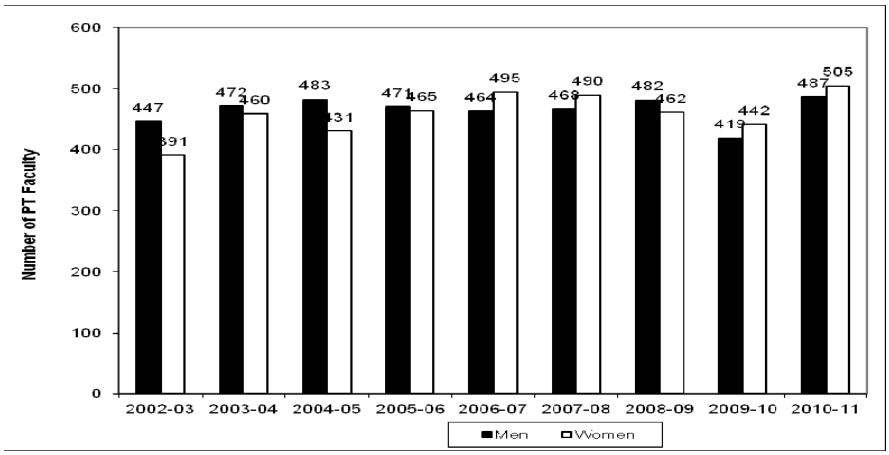
Source: UCASS

Probationary and Tenured Faculty at Western: Continuing Beyond Age 65



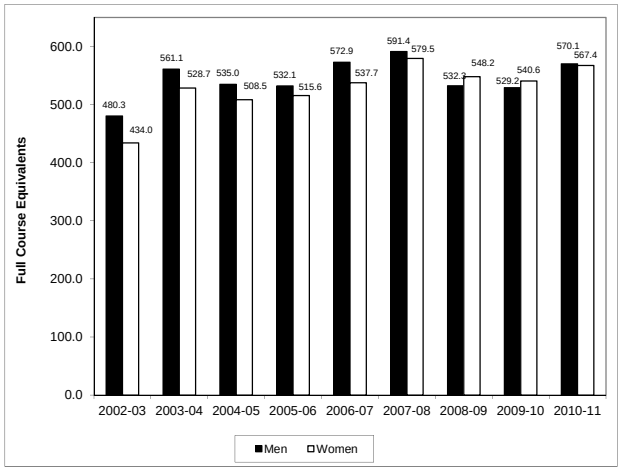
Source: Western Human Resources Information System

Number of Individuals with Part-Time Faculty Appointments: 2002-03 to 2010-11 (by Fiscal Year)



Source: Western Human Resources Information Systems

Degree Credit Course Teaching in FCEs by Part-Time Faculty: 2002-03 to 2010-11 (by Fiscal Year and Gender)

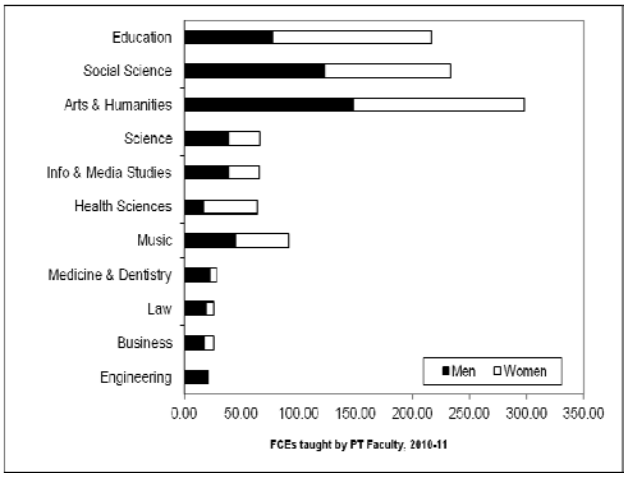


Source: Western Information Systems (appointment status and course data).

Note: Instructor data is unavailable for 3.7% of courses in 2002-03; 1.1% in 2003-04; 1.2% in 2004-05; 0.8% in 2005-06, 0 % in 2006-07, through 2010-11.

Course data for undergraduate, graduate and professional degree credit course teaching are included, with the exception of independent studies, directed research, exams, theses, clinical courses, etc.

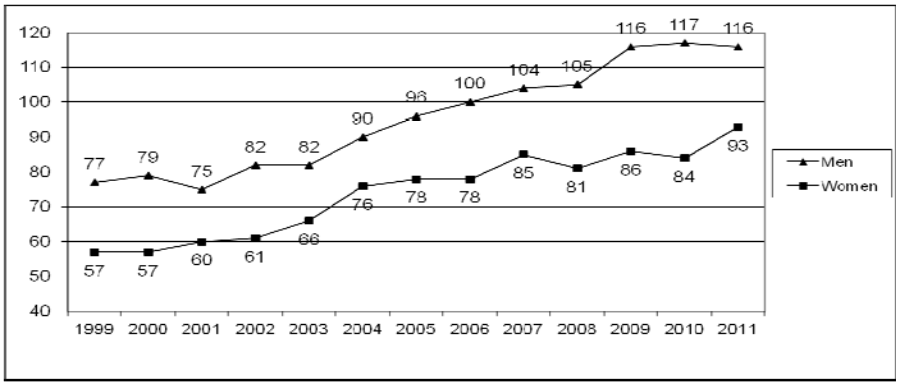
Degree Credit Courses taught by Part-Time Faculty in FCEs, by Faculty and Gender: 2010-11 (Fiscal Year)



Source: Western Information Systems (appointment status and course data).

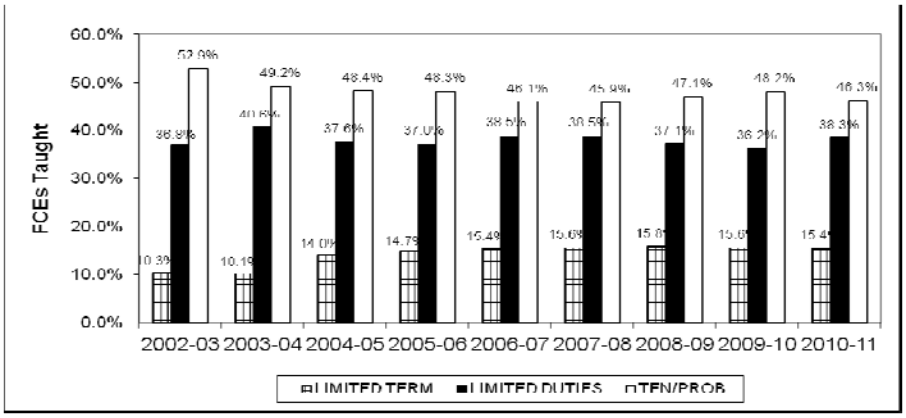
Course data for undergraduate, graduate and professional degree credit course teaching are included, with the exception of independent studies, directed research, exams, theses, clinical courses, etc. Course data for the Faculty of Education includes the Additional Qualification Courses.

Limited Term Appointments: 1999 to 2011



Source: UCASS Data 1999- 2007 (October).
Please note: a) Statistics Canada data includes faculty and appointment types that are outside of the UWOFA Collective Agreement; and b) the definition of limited term for Statistics Canada purposes has changed over time. Data may therefore not accurately reflect trends.
Source: Western's Human Resources Information Systems 2008 - 2011 (October)

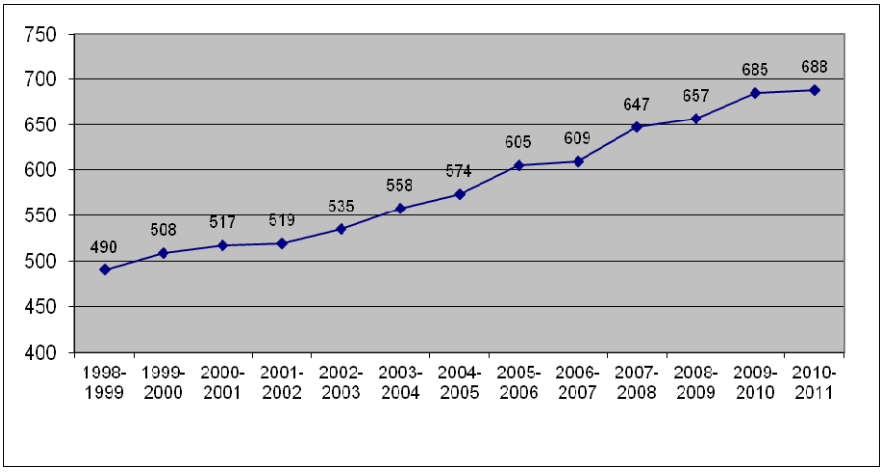
Degree Credit Courses Taught in FCEs, by Instructor Contract Type (by Fiscal Year)



Course data for undergraduate, graduate and professional credit course teaching are included, with the exception of independent studies, directed research, exams, theses, clinical courses, etc. The data does not include graduate student supervisions.

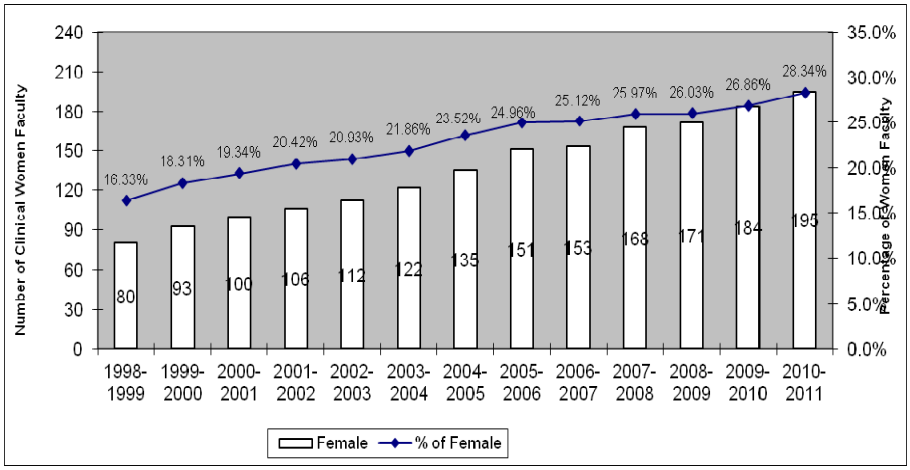
Note: Instructor data is unavailable for 3.7% of courses in 2002-03; 1.1% in 2003-04; 1.2% in 2004-05; 0.8% in 2005-06, 0% in 2006-07 through 2010-11.

Clinical Full Time Faculty (Physicians in Schulich) at Western, 1999 – 2011



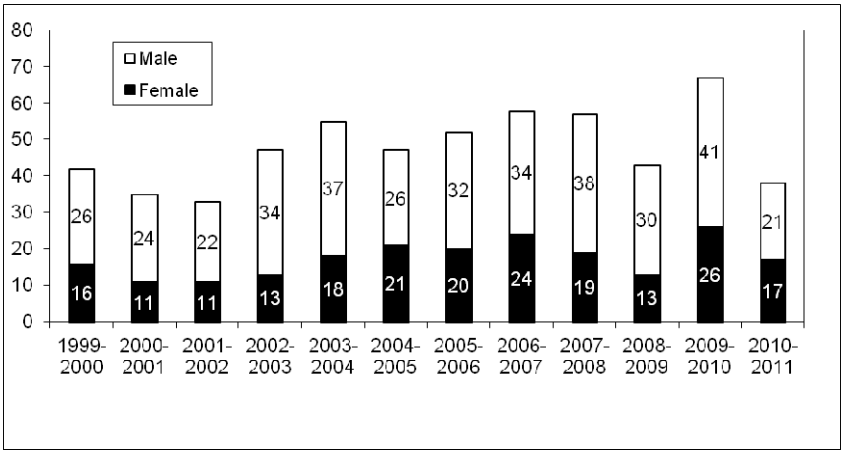
Source: Western Human Resources Information Systems

Clinical Full Time Women Faculty (Physicians in Schulich) at Western, 1999 – 2011



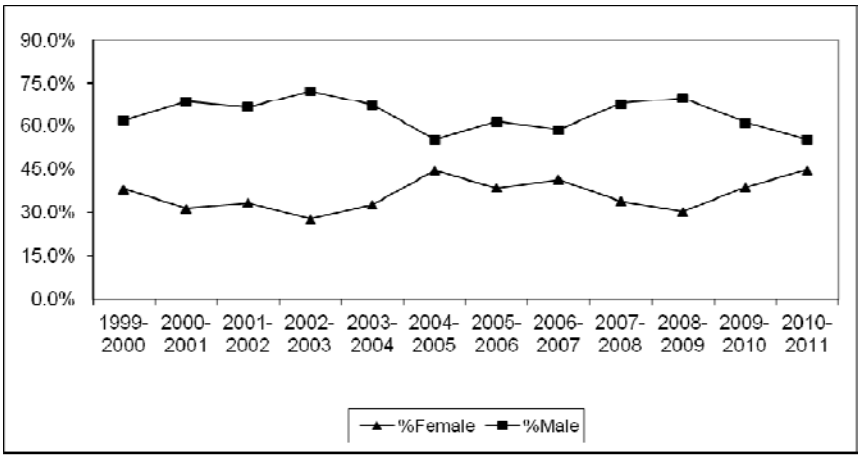
Source: Western Human Resources Information Systems

New Clinical Full Time Faculty (Physicians in Schulich) at Western by Gender: 2000 – 2011



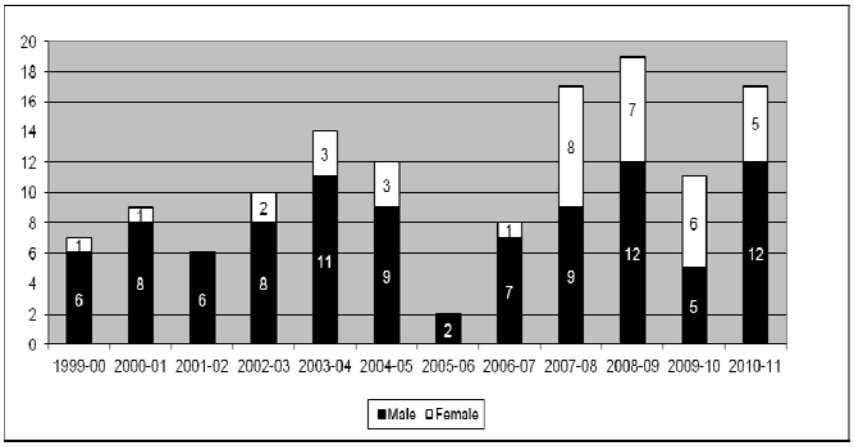
Source: Western Human Resources Information Systems

Percentage of New Clinical Full Time Faculty (Physicians in Schulich) at Western by Gender: 1999/00 – 2010/11



Source: Western Human Resources Information Systems

Clinical Full Time (Physicians in Schulich) Resignations by Gender, 1999/2000 – 2010/2011



Source: Western Human Resources Information System

Annual Report – 2011
Working Group on Information Security (WGIS)

The WGIS sub-committee consists of a multi-disciplinary team representing a broad cross-section of university leaders (for a list of members, see Appendix A). Recognizing that rapid changes in technology create challenges and opportunities, the WGIS team continued to pursue a strategy of proactive initiatives.

Initiatives this past year included: a continuing focus on information security awareness by addressing user behaviors that increase the risk of malware; continued efforts to mitigate the risks associated with "phishing" attempts, especially targeted "phishing" (*aka* spear-phishing); the continuation and expansion of the cryptography project; a focus on system security best practices, especially as prioritized by risk assessment efforts; and an effort to further increase perimeter security by restricting off-site connections to internal university resources.

The variety and frequency of computer security threats continues to evolve rapidly especially given the proliferation of personal mobile computing devices and ubiquitous computing platforms. The primary objective of WGIS was to predict vulnerabilities well in advance of problems and recommend protective measures for the university community. The secondary objective was to identify and successfully resolve new problems as soon as they were detected. Consistency in this strategy continues to be a key factor to maintaining a secure computing environment at Western.

Report Contents

Summary of Sub-Committee Activities 2
Information Security Awareness – eWellness 2
More Community Awareness 4
Western ROAMS & Service Protection Initiative 4
Policies, Procedures, and Best Practices 5
Policy Review 5
Payment Card Industry Compliance 5
Cryptography Initiative 6
Risk Assessment 7
Incident Response & Investigations 8
Conclusions & Future Efforts 8
Appendix A – List of Current WGIS Members as of End of 2011 9
List of Active WGIS Sub-Teams 9
Appendix B – Initial 2011 Risk Matrix 10
Appendix C – Updated EOY 2011 Risk Matrix & Priorities for 2012 11

Summary of Sub-Committee Activities

Information Security Awareness – eWellness

The Sub-Committee responsible for increasing Security Awareness on campus initiated a new awareness campaign this year and at the same time rebranded their efforts as 'eWellness (rather than Computer Wellness) to reflect the growing scope of technology and the security issues that need to be addressed.

Western's end-user computing community continued to be challenged throughout 2011 by a steady stream of both generic and targeted "phishing" (*aka* "spear-phishing") attempts by increasingly active internet-based malefactors who continue to evolve their efforts to acquire user credentials through both pure social engineering (*SE*) and blended SE/technical attacks.

Anti-phishing process enhancements put in place in 2010 to limit the exposure of Western users' credentials to such attacks has also continued to evolve, and together with increased uptake of ITS-provided spam-filtering technologies and an active Awareness campaign, resulted in an overall year-over-year reduction in the number of Western community users affected by such attacks, down to 70 from 87 in 2010 (reference Figure 1, below)

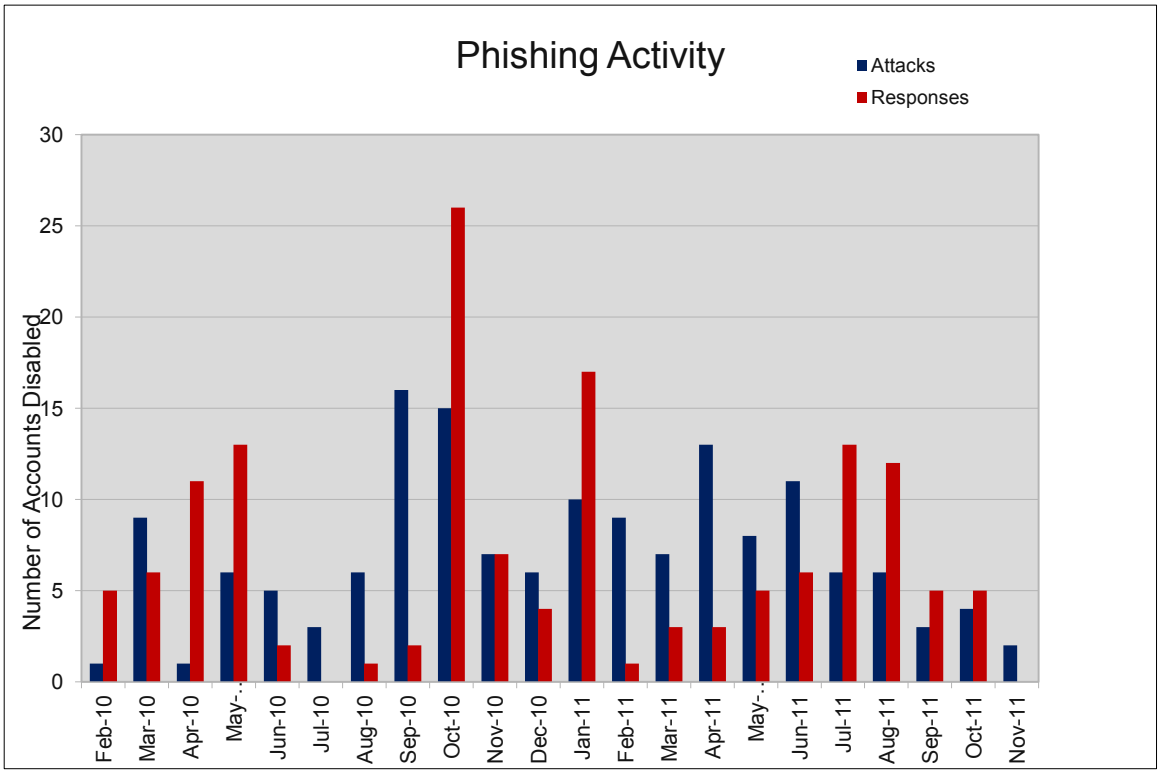


Figure 1 – Volume of targeted phishing attacks and "successful" responses

Nevertheless, 2011 continued to see effects of phishing on our community, as shown in Figure 2, below.

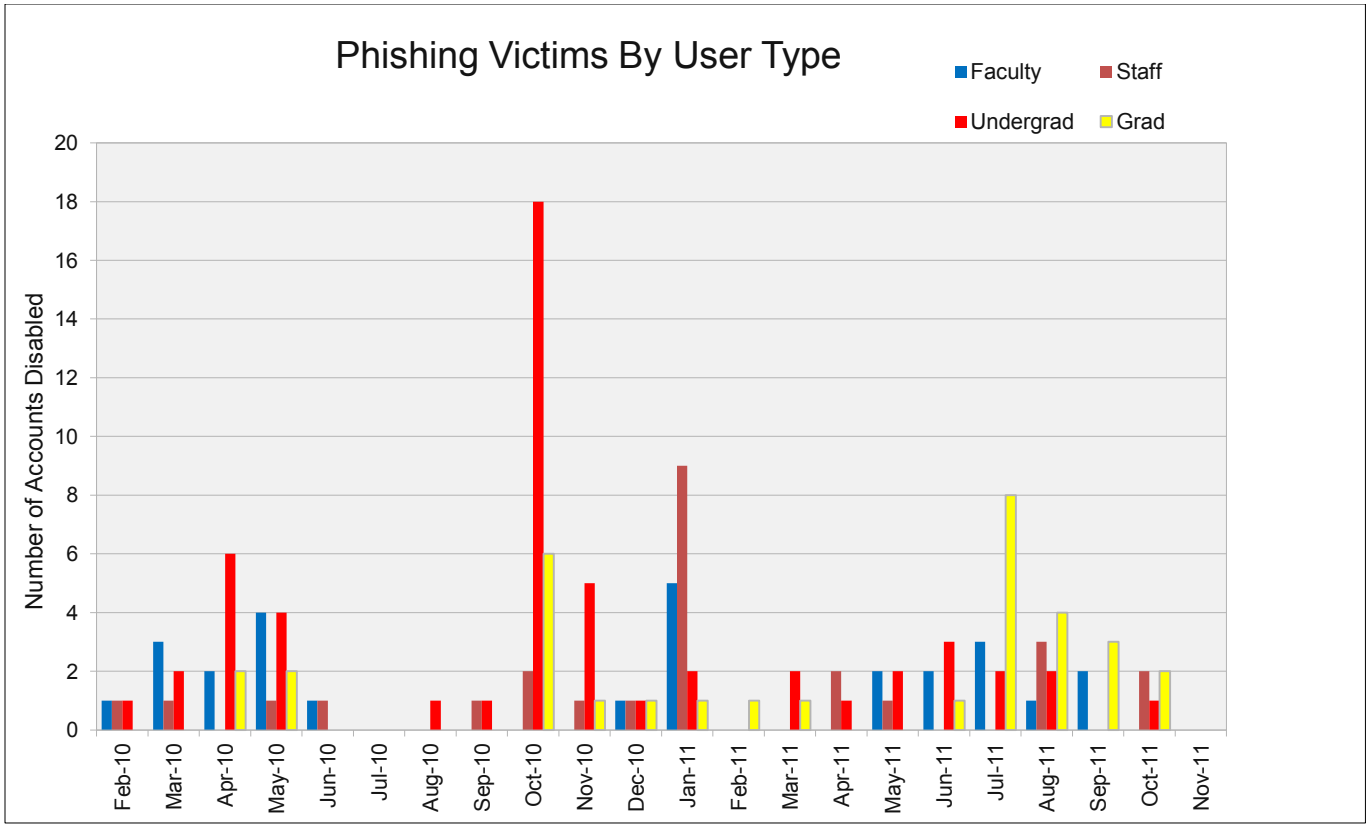


Figure 2 – Volumes of "successful" phishing responses by user type

Accordingly, one of the primary messages of the eWellness campaign this year was emphasizing the importance of protecting Western usernames and passwords.

WGIS 2012 eWellness campaign and ITS will continue to focus on communications and technical improvements aimed at further reducing the effects of such attacks, especially those associated with the aforementioned blended attacks that rely on a user clicking on links in unsolicited emails, where those linked websites expose the user to potential malware infections.

The eWellness Team was also engaged in encouraging faculty, staff and students of Western's community to transition from using Western's public (UWO) wireless network to Western's more secure (UWO-SecureV2) wireless network.

More Community Awareness

Awareness about information security issues within the university community has also been advanced through other WGIS and ITS activities in 2011.

With the continued involvement of the Non-Medical Research Ethics Board (NMREB) on the Data Classification and Encryption Sub-Committee, researchers are continuing to be guided toward inclusion in our deployment of Symantec's Pretty Good Privacy (PGP) as part of our cryptography deployment project, employing our PGP solutions and/or alternative cryptographic and/or procedural strategies to protect sensitive research-related information. Both the chairs of the NMREB and the Health Sciences REB are members of the Cryptography project, so as to continue furthering the opportunity for protecting research information through the application of appropriate cryptography technologies.

Finally, joint presentations by ITS and the University's Privacy Office on the topic of cryptography and privacy legislation (both generally, as well as detailing the Cryptography initiative) have been delivered to a number of Western groups including the Faculty of Health Science, Student Health Services, and Ivey. These talks included staff, faculty and key IT support personnel. Additional *ad hoc* inquiries have resulted from these sessions, seeking participation in the Cryptography project. Further such requests are continuing to be anticipated as the privacy liaisons continue to digest the information provided and identify immediate opportunities for cryptography-based security improvements in their respective areas of responsibility.

Western ROAMS & Service Protection Initiative

ITS continued to sustain communication efforts and drove associated process changes related to the rollout of *Western ROAMs* (Remote Office Access Management system). Increased awareness of remote secure access and increased demand for this service keeps pressure on ITS to continue migrating groups of end-users (typically by Faculty/Unit) into the new *Western ROAMs* model.

This model was designed to provide more granular network security management. It also allows for the reduction (and eventual elimination) of a substantial risk to end-user systems across campus by eliminating unauthorized access to the campus network through Remote Desktop Protocol (RDP). It re-established the principle of budget unit head approval for remote access to Western information.

The initiative to protect RDP continues and is expected to be completed in 2012. As of November 2011, the following Organizational Units are supported in the new *ROAMs* environment:

- Animal Care and Veterinary Services
- Department of Communications and Public Affairs
- Division of Facilities Management
- Division of Financial Services
- Division of Information Technology Services
- Faculty of Arts and Humanities

- Faculty of Education
- Faculty of Information and Media Studies
- Faculty of Law
- Faculty of Music
- Faculty of Social Science
- Office of Institutional Planning and Budgeting
- Office of the Registrar
- Schulich School of Medicine and Dentistry
- Western Bookstore
- Western Libraries

Migration of the above units to the new *ROAMs* model has produced measurable results.

Due to malefactors or the proliferation of the 'Morto' worm, attacks against the Remote Desktop Protocol (RDP) have risen above 1.5 million attacks per day. Even so, malicious attacks originating from off-campus against the RDP service in the above protected units have been reduced to zero, because moving them behind Western ROAMS makes them immune to malicious attacks.

This effort effectively mitigated risk to the RDP service from off-campus, and because placement behind *Western ROAMs* allows for the protection of additional services, this initiative was expanded to provide additional protection to ports below 1024. Internet protocol standards reserve the first 1024 ports for common and well known services (services such as Web, File Transfer Protocol, etc.) suggesting that this effort should protect these well-known services first. Within our environment, some of those ports are not being used, but are being attacked. Accordingly, services which reflected low or no use on end-user system or networked device were protected through restrictive network policy which prohibited connections from off campus. Services within the 1024 range which reflected heavy use, such as Web (port 80) and SSH (port 22) were left unfiltered.

This expanded initiative, branded "Service Protection" will continue into 2012, when development of ITS's network management tool (RAMP) is planned to provide Western's network administrators direct policy influence over protected services.

Policies, Procedures, and Best Practices

Policy Review

All Security Related Policies were reviewed to ensure they remained relevant and no significant modifications were required. No changes were required this year and the Policies were documented as reviewed.

Payment Card Industry Compliance

With several WGIS members actively involved in the PCI Compliance initiative (under the auspices of the Western Bank Card Committee and in support of MAPP 1.29 – Bank

Card Policy), WGIS remained aware and engaged in the progress of this major project and discussed best practices that may be used in other areas of security.

Originally all ecommerce servers and applications on campus pointed to the ITS provided 'stub' for secure transmission of credit card information. This year ITS migrated all of the E-commerce sites to take advantage of the new 'stub' offered directly on the merchant account site, removing the risk associated with managing this information.

The ecommerce ventures that have arisen on campus since Western achieved its PCI status continue to be directed through Western's Bank Card Committee.

Cryptography Initiative

As noted in the 2010 WGIS Annual Report, the pilot for PGP encryption technologies was concluded and was found to be suitable for deployment across Western for both the protection of research and corporate data.

Because the pilot was focused primarily on the development of end-to-end supporting processes for whole disk, email, and shared data (network drive/folder) within a central management framework a number of technologies were tested and additional lessons learned.

Thus, the PGP encryption pilot that was concluded in 2010 was formally re-launched as a post-pilot cryptography project designed to extend cryptographic support to encompass the broader community. The initial pilot suggested additional cryptographic strategies that are now being pursued. Such strategies include (but are not limited to):

- Continued development of a robust centralized key management capability;
- Inclusion of non-Symantec products under the same cryptographic umbrella;
- Planned operationalization of both the encryption deployments and the management of cryptographic keys; and
- Duplication of centralized key management servers into a cluster for service redundancy to ensure reliability

Some technical challenges exist, such as the inability to use existing technologies equally across all operating systems with full feature parity. Though these challenges have not hindered the progress in the cryptography project they will nevertheless require additional work to enable this project to have full benefit across campus. Progress continues to be made with respect to this.

Information Classification Initiative

With the increased use of cryptographic technologies to provide information confidentiality and data integrity, a natural problem became evident. People who had been provided with encryption/decryption ability discovered that not all data was equal; the risk to data is a function of its classification. This reinforced the need for an

Information Classification policy within Western to establish a common framework for assessing risk to different data types.

Accordingly, two separate initiatives were started. First, a sub-group of WGIS was struck to propose a high-level Information Classification Policy. Second, the WGIS Encryption Strategy Team was re-cast to look at Information Classification from the perspective of the Information Life-Cycle and tasked to:

- Compile an inventory of Western information assets
- Define levels of protection for information assets (based on current practices)
- Define information classification criteria
- Develop technical recommended information classification best-practices
- Define information handling and labeling procedures

This work is on-going.

Risk Assessment

A WGIS sub-committee remains responsible for reviewing and updating the Risk Assessment matrix.

This multi-disciplinary group (including individuals with technical, security, audit, and risk management skill sets) reviewed the risk management matrix, and with the input of WGIS as a whole reviewed the standing risk assessment for the purpose of continuing to identify immediate priorities for WGIS attention (reference **Appendix B** for this Initial 2011 risk matrix). That risk matrix also serves as a touchstone for a regular agenda item in WGIS meetings - the discussion of new technologies and new/evolving threats to existing technologies – in furtherance of WGIS' primary objective.

That effort confirmed the identification of risks which required continued priority attention: the exposure of end-user computing devices (desktops, laptops/tablets, and handheld devices) to external threats (targeted attacks, malicious websites, malicious email/spam, and malicious software). Collectively, efforts to address this set of risks are being referred to as "End-point Protection" strategies.

This risk assessment also confirmed the risks posed by the proliferation of mobile devices and ubiquitous computing services, such as 'Cloud Computing'. This resulted in an effort to begin grappling with strategies to manage this new risk.

ITS has initiated investigations of end-point protection:

1. Within the PDA Working Group, a security matrix has been maintained in order to identify the availability and options for security controls related to various "flavours" of handheld devices (iPhones, BlackBerrys, etc.). This PDA security matrix forms the basis for ongoing efforts by the PDA Working Group to identify best practices for securing such devices using existing capabilities, as well as gaps for which additional solutions may be required. Such gaps that have been identified are expected to drive further investigation (in 2012) into potential solutions.

2. The PGP encryption project is in direct support of end-point protection. This will grow to include encryption options for more devices and platforms.
3. The ROAMS project and Service Protect are also directly related to protecting the workstations on campus from RDP attacks.

Other activity throughout 2011, in addition to the efforts made on the priority topics identified by the Risk Assessment team and changes in both technology and threat landscapes, are reflected in the updated risk matrix attached as **Appendix C**. This is a living document that helps WGIS focus on areas of risk and changes regularly to reflect new knowledge of threats and new improvements to the Western Security environment. The latest Risk Matrix in Appendix C highlights the specific changes to the matrix this year, as well as the next priorities for attention in 2012.

Incident Response & Investigations

The Security Office dealt with 3 significant security-related incidents in 2011. Beyond that, ITS continues to operationalize the response to repeating security issues. The locking of computers on campus that have been compromised, the notification of copyright infringement, the management of Spear Phishing attacks and the detection of stolen laptops accessing our network have all been scripted and/or streamlined.

Non-routine incidents such as investigation and resolution of suspicious activity on the network, investigation and follow up on harassing or inappropriate email, or forensics in support of a police request continue at about the same rate this year as last year.

Conclusions & Future Efforts

In conclusion, 2011 has been another busy year for WGIS and its members, and 2012 is expected to follow suit.

Looking ahead to 2012, WGIS plans to focus efforts on two main areas, in addition to those items noted in the body of this report as continuing through 2012:

1. Completion of the Data Classification and Protection policy and expansion of the PGP cryptography project. The next year should see an increased number of end-point devices using encryption and a more complete set of tools supported.

2. Continued evolution and progression of the formal risk assessment and management processes. Along with the priorities identified throughout this document, WGIS uses this tool to introduce 2 new high priority topics for discussion. This allows flexibility to address emerging concerns and/or urgent security priorities.

Appendix A – List of Current WGIS Members as of End of 2011

Greg Moran gmoran2@uwo.ca (Chair)

Carac Allison cjalliso@uwo.ca (TUMS)
Craig Reed creed23@uwo.ca (TUMS)
David Wiseman magi@csd.uwo.ca (TUMS)
Jeffery Gardiner jgardi2@uwo.ca (ITS Central Information Security Officer)
Jeffery Grieve jeffg@uwo.ca (ITS designate)
Krishna Patel kpatel97@uwo.ca (Registrar designate)
Luiz Capretz lcapretz@eng.uwo.ca (Faculty member)
Peggy Wakabayashi peggy@housing.uwo.ca (Housing Designate)
Rob Brennan rbrennan@uwo.ca (Western Information Systems Group designate)
Steve Beauchemin sbeauche@uwo.ca (Faculty member)

Debbie Jones debbie@uwo.ca (Ex officio)
Sharon Farnell sfarnell@uwo.ca (Ex officio)
Steve Jarrett jarrett@uwo.ca (Ex officio)
Geoff Pimlatt gapimlat@uwo.ca (Ex officio)
Dan Sinai dsinai2@uwo.ca (Ex officio)

Ed Gibson egibson@uwo.ca (ITS, technical advisor)
Rich Whitcroft rwhitcro@uwo.ca (ITS, technical advisor)
Scott A May smay5@uwo.ca (Communications & Public Affairs, technical advisor)
Mike Mics mmics@uwo.ca (CCPS, technical advisor)

List of Active WGIS Sub-Teams

1. WGIS Encryption Strategy Team
2. WGIS Risk Assessment Team
3. WGIS eWellness Planning Team

Appendix B – Initial 2011 Risk Matrix

WGIS Risk Assessment Tool

Legend:	
	Sufficient Security controls in place
	Improvement opportunities exist in key security control areas
	Serious deficiences exist in key security control areas; short term focus required
	Not applicable

			Threats																
			Physical Threats			Western User Threats						External User Threats				Access Management Threats			
			Intrusion (on premises)	Theft or Loss (off premises)	Inadvertent Damage	Intentional Damage (Authorized User)	Intentional Damage (Unauthorized User)	Inadvertent Damage/Error (Authorized User)	Inadvertent Damage/Error (Unauthorized User)	Software Licensing & Copyright Violations	Social Networking	Targeted Attacks	Malicious Websites ("Drive By Hacking")	Malicious Email/Spam	Malicious Software	ID Sharing	Social Engineering	Remote Access	AM Process Control
Technologies	Personal Tools	Desktop PCs																	
		Laptops & Tablet PCs																	
		Handheld Devices (PDA/Smartphones)																	
		Cell Phones																	
		Portable Digital Storage Devices																	
		Personal ID Cards																	
		Local Printers																	
	Shared Tools	Credential Management Systems																	
		File Servers																	
		Databases/DB Servers																	
		Network Printers																	
		Network - Wired																	
		Network - Wireless																	
		Network Services (DNS, DHCP, etc)																	
		Email																	
		Web Services/Web Servers																	
		Western Directory																	
		Genlabs (Public use machines)																	
		HR Application (Employee records)																	
		HE Application (Student records)																	
		CR Application (Alumni/Donor records)																	
		Peoplesoft Finance																	
		Pension Application																	
		eCommerce Systems																	
		Cloud Computing (3rd party services)	For each cloud-based technology implementation, see relevant technology item risks, above																

Appendix C – Updated EOY 2011 Risk Matrix & Priorities for 2012

WGIS Risk Assessment Tool

Legend:	
	Sufficient Security controls in place
	Improvement opportunities exist in key security control areas
	Serious deficiences exist in key security control areas; short term focus required
	Not applicable

Technologies		Threats																	
		Physical Threats			Western User Threats						External User Threats				Access Management Threats				
		Intrusion (on premises)	Theft or Loss (off premises)	Inadvertent Damage	Intentional Damage (Authorized User)	Intentional Damage (Unauthorized User)	Inadvertent Damage/Error (Authorized User)	Inadvertent Damage/Error (Unauthorized User)	Software Licensing & Copyright Violations	Social Networking	Targeted Attacks	Malicious Websites ("Drive By Hacking")	Malicious Email/Spam	Malicious Software	ID Sharing	Social Engineering	Remote Access	AM Process Control
Personal Tools	Desktop PCs	Improvement opportunities exist in key security control areas	Improvement opportunities exist in key security control areas	Improvement opportunities exist in key security control areas	Serious deficiences exist in key security control areas; short term focus required	Serious deficiences exist in key security control areas; short term focus required	Improvement opportunities exist in key security control areas	Improvement opportunities exist in key security control areas	Serious deficiences exist in key security control areas; short term focus required	Serious deficiences exist in key security control areas; short term focus required	Serious deficiences exist in key security control areas; short term focus required	Serious deficiences exist in key security control areas; short term focus required	Improvement opportunities exist in key security control areas	Serious deficiences exist in key security control areas; short term focus required	Improvement opportunities exist in key security control areas	Improvement opportunities exist in key security control areas	Serious deficiences exist in key security control areas; short term focus required	Serious deficiences exist in key security control areas; short term focus required
Personal Tools	Laptops & Tablet PCs	Improvement opportunities exist in key security control areas	Improvement opportunities exist in key security control areas	Improvement opportunities exist in key security control areas	Sufficient Security controls in place	Serious deficiences exist in key security control areas; short term focus required	Improvement opportunities exist in key security control areas	Improvement opportunities exist in key security control areas	Serious deficiences exist in key security control areas; short term focus required	Serious deficiences exist in key security control areas; short term focus required	Serious deficiences exist in key security control areas; short term focus required	Serious deficiences exist in key security control areas; short term focus required	Improvement opportunities exist in key security control areas	Serious deficiences exist in key security control areas; short term focus required	Improvement opportunities exist in key security control areas	Improvement opportunities exist in key security control areas	Serious deficiences exist in key security control areas; short term focus required	Serious deficiences exist in key security control areas; short term focus required
Personal Tools	Handheld Devices (PDA/Smartphones)	Improvement opportunities exist in key security control areas	Improvement opportunities exist in key security control areas	Improvement opportunities exist in key security control areas	Serious deficiences exist in key security control areas; short term focus required	Serious deficiences exist in key security control areas; short term focus required	Serious deficiences exist in key security control areas; short term focus required	Serious deficiences exist in key security control areas; short term focus required	Serious deficiences exist in key security control areas; short term focus required	Serious deficiences exist in key security control areas; short term focus required	Serious deficiences exist in key security control areas; short term focus required	Serious deficiences exist in key security control areas; short term focus required	Improvement opportunities exist in key security control areas	Serious deficiences exist in key security control areas; short term focus required	Improvement opportunities exist in key security control areas	Improvement opportunities exist in key security control areas	Serious deficiences exist in key security control areas; short term focus required	Serious deficiences exist in key security control areas; short term focus required
Personal Tools	Cell Phones	Not applicable	Sufficient Security controls in place	Sufficient Security controls in place	Not applicable	Not applicable	Not applicable	Not applicable	Not applicable	Not applicable	Sufficient Security controls in place	Not applicable	Not applicable	Not applicable	Not applicable	Not applicable	Not applicable	Not applicable
Personal Tools	Portable Digital Storage Devices	Improvement opportunities exist in key security control areas	Improvement opportunities exist in key security control areas	Improvement opportunities exist in key security control areas	Improvement opportunities exist in key security control areas	Improvement opportunities exist in key security control areas	Improvement opportunities exist in key security control areas	Improvement opportunities exist in key security control areas	Not applicable	Not applicable	Not applicable	Not applicable	Not applicable	Improvement opportunities exist in key security control areas	Not applicable	Improvement opportunities exist in key security control areas	Not applicable	Not applicable
Personal Tools	Personal ID Cards	Sufficient Security controls in place	Sufficient Security controls in place	Sufficient Security controls in place	Sufficient Security controls in place	Sufficient Security controls in place	Sufficient Security controls in place	Sufficient Security controls in place	Not applicable	Not applicable	Not applicable	Not applicable	Not applicable	Not applicable	Sufficient Security controls in place	Sufficient Security controls in place	Not applicable	Sufficient Security controls in place
Personal Tools	Local Printers	Sufficient Security controls in place	Not applicable	Sufficient Security controls in place	Sufficient Security controls in place	Sufficient Security controls in place	Sufficient Security controls in place	Sufficient Security controls in place	Not applicable	Not applicable	Not applicable	Not applicable	Not applicable	Not applicable	Not applicable	Not applicable	Not applicable	Not applicable
Shared Tools	Credential Management Systems	Improvement opportunities exist in key security control areas	Not applicable	Not applicable	Improvement opportunities exist in key security control areas	Improvement opportunities exist in key security control areas	Improvement opportunities exist in key security control areas	Improvement opportunities exist in key security control areas	Improvement opportunities exist in key security control areas	Not applicable	Improvement opportunities exist in key security control areas	Not applicable	Not applicable	Improvement opportunities exist in key security control areas	Improvement opportunities exist in key security control areas	Improvement opportunities exist in key security control areas	Not applicable	Serious deficiences exist in key security control areas; short term focus required
Shared Tools	File Servers	Improvement opportunities exist in key security control areas	Not applicable	Not applicable	Serious deficiences exist in key security control areas; short term focus required	Serious deficiences exist in key security control areas; short term focus required	Serious deficiences exist in key security control areas; short term focus required	Serious deficiences exist in key security control areas; short term focus required	Improvement opportunities exist in key security control areas	Not applicable	Improvement opportunities exist in key security control areas	Not applicable	Not applicable	Improvement opportunities exist in key security control areas	Improvement opportunities exist in key security control areas	Improvement opportunities exist in key security control areas	Serious deficiences exist in key security control areas; short term focus required	Serious deficiences exist in key security control areas; short term focus required
Shared Tools	Databases/DB Servers	Improvement opportunities exist in key security control areas	Not applicable	Not applicable	Improvement opportunities exist in key security control areas	Improvement opportunities exist in key security control areas	Improvement opportunities exist in key security control areas	Improvement opportunities exist in key security control areas	Improvement opportunities exist in key security control areas	Not applicable	Improvement opportunities exist in key security control areas	Not applicable	Not applicable	Improvement opportunities exist in key security control areas	Improvement opportunities exist in key security control areas	Improvement opportunities exist in key security control areas	Improvement opportunities exist in key security control areas	Serious deficiences exist in key security control areas; short term focus required
Shared Tools	Network Printers	Improvement opportunities exist in key security control areas	Not applicable	Not applicable	Improvement opportunities exist in key security control areas	Improvement opportunities exist in key security control areas	Improvement opportunities exist in key security control areas	Improvement opportunities exist in key security control areas	Not applicable	Not applicable	Improvement opportunities exist in key security control areas	Not applicable	Not applicable	Improvement opportunities exist in key security control areas	Improvement opportunities exist in key security control areas	Improvement opportunities exist in key security control areas	Serious deficiences exist in key security control areas; short term focus required	Serious deficiences exist in key security control areas; short term focus required
Shared Tools	Network - Wired	Improvement opportunities exist in key security control areas	Not applicable	Not applicable	Improvement opportunities exist in key security control areas	Improvement opportunities exist in key security control areas	Improvement opportunities exist in key security control areas	Improvement opportunities exist in key security control areas	Not applicable	Not applicable	Improvement opportunities exist in key security control areas	Not applicable	Not applicable	Improvement opportunities exist in key security control areas	Improvement opportunities exist in key security control areas	Improvement opportunities exist in key security control areas	Improvement opportunities exist in key security control areas	Improvement opportunities exist in key security control areas
Shared Tools	Network - Wireless	Sufficient Security controls in place	Not applicable	Not applicable	Sufficient Security controls in place	Sufficient Security controls in place	Improvement opportunities exist in key security control areas	Improvement opportunities exist in key security control areas	Not applicable	Not applicable	Improvement opportunities exist in key security control areas	Not applicable	Not applicable	Improvement opportunities exist in key security control areas	Sufficient Security controls in place	Sufficient Security controls in place	Sufficient Security controls in place	Sufficient Security controls in place
Shared Tools	Network Services (DNS, DHCP, etc)	Improvement opportunities exist in key security control areas	Not applicable	Not applicable	Improvement opportunities exist in key security control areas	Improvement opportunities exist in key security control areas	Improvement opportunities exist in key security control areas	Improvement opportunities exist in key security control areas	Not applicable	Not applicable	Improvement opportunities exist in key security control areas	Not applicable	Not applicable	Improvement opportunities exist in key security control areas	Improvement opportunities exist in key security control areas	Improvement opportunities exist in key security control areas	Improvement opportunities exist in key security control areas	Improvement opportunities exist in key security control areas
Shared Tools	Email	Improvement opportunities exist in key security control areas	Not applicable	Not applicable	Improvement opportunities exist in key security control areas	Improvement opportunities exist in key security control areas	Improvement opportunities exist in key security control areas	Improvement opportunities exist in key security control areas	Improvement opportunities exist in key security control areas	Not applicable	Improvement opportunities exist in key security control areas	Not applicable	Serious deficiences exist in key security control areas; short term focus required	Improvement opportunities exist in key security control areas	Improvement opportunities exist in key security control areas	Improvement opportunities exist in key security control areas	Serious deficiences exist in key security control areas; short term focus required	Serious deficiences exist in key security control areas; short term focus required
Shared Tools	Web Services/Web Servers	Improvement opportunities exist in key security control areas	Not applicable	Not applicable	Improvement opportunities exist in key security control areas	Improvement opportunities exist in key security control areas	Improvement opportunities exist in key security control areas	Improvement opportunities exist in key security control areas	Improvement opportunities exist in key security control areas	Not applicable	Improvement opportunities exist in key security control areas	Not applicable	Not applicable	Improvement opportunities exist in key security control areas	Improvement opportunities exist in key security control areas	Improvement opportunities exist in key security control areas	Improvement opportunities exist in key security control areas	Improvement opportunities exist in key security control areas
Shared Tools	Western Directory	Improvement opportunities exist in key security control areas	Not applicable	Not applicable	Improvement opportunities exist in key security control areas	Improvement opportunities exist in key security control areas	Improvement opportunities exist in key security control areas	Improvement opportunities exist in key security control areas	Not applicable	Not applicable	Improvement opportunities exist in key security control areas	Not applicable	Not applicable	Improvement opportunities exist in key security control areas	Improvement opportunities exist in key security control areas	Improvement opportunities exist in key security control areas	Improvement opportunities exist in key security control areas	Improvement opportunities exist in key security control areas
Shared Tools	Genlabs (Public use machines)	Sufficient Security controls in place	Not applicable	Not applicable	Sufficient Security controls in place	Sufficient Security controls in place	Sufficient Security controls in place	Sufficient Security controls in place	Sufficient Security controls in place	Not applicable	Sufficient Security controls in place	Improvement opportunities exist in key security control areas	Serious deficiences exist in key security control areas; short term focus required	Serious deficiences exist in key security control areas; short term focus required	Sufficient Security controls in place	Improvement opportunities exist in key security control areas	Sufficient Security controls in place	Sufficient Security controls in place
Shared Tools	HR Application (Employee records)	Sufficient Security controls in place	Not applicable	Not applicable	Sufficient Security controls in place	Serious deficiences exist in key security control areas; short term focus required	Sufficient Security controls in place	Sufficient Security controls in place	Sufficient Security controls in place	Not applicable	Sufficient Security controls in place	Not applicable	Not applicable	Sufficient Security controls in place	Sufficient Security controls in place	Sufficient Security controls in place	Sufficient Security controls in place	Sufficient Security controls in place
Shared Tools	HE Application (Student records)	Improvement opportunities exist in key security control areas	Not applicable	Not applicable	Improvement opportunities exist in key security control areas	Serious deficiences exist in key security control areas; short term focus required	Improvement opportunities exist in key security control areas	Improvement opportunities exist in key security control areas	Improvement opportunities exist in key security control areas	Not applicable	Improvement opportunities exist in key security control areas	Not applicable	Not applicable	Improvement opportunities exist in key security control areas	Improvement opportunities exist in key security control areas	Improvement opportunities exist in key security control areas	Improvement opportunities exist in key security control areas	Sufficient Security controls in place
Shared Tools	CR Application (Alumni/Donor records)	Sufficient Security controls in place	Not applicable	Not applicable	Sufficient Security controls in place	Improvement opportunities exist in key security control areas	Sufficient Security controls in place	Sufficient Security controls in place	Sufficient Security controls in place	Not applicable	Sufficient Security controls in place	Not applicable	Not applicable	Sufficient Security controls in place	Sufficient Security controls in place	Sufficient Security controls in place	Sufficient Security controls in place	Sufficient Security controls in place
Shared Tools	Peoplesoft Finance	Sufficient Security controls in place	Not applicable	Not applicable	Sufficient Security controls in place	Serious deficiences exist in key security control areas; short term focus required	Sufficient Security controls in place	Sufficient Security controls in place	Sufficient Security controls in place	Not applicable	Sufficient Security controls in place	Not applicable	Not applicable	Sufficient Security controls in place	Sufficient Security controls in place	Sufficient Security controls in place	Sufficient Security controls in place	Sufficient Security controls in place
Shared Tools	Pension Application	Sufficient Security controls in place	Not applicable	Not applicable	Sufficient Security controls in place	Improvement opportunities exist in key security control areas	Sufficient Security controls in place	Sufficient Security controls in place	Sufficient Security controls in place	Not applicable	Sufficient Security controls in place	Not applicable	Not applicable	Sufficient Security controls in place	Sufficient Security controls in place	Sufficient Security controls in place	Sufficient Security controls in place	Sufficient Security controls in place
Shared Tools	eCommerce Systems	Sufficient Security controls in place	Not applicable	Not applicable	Sufficient Security controls in place	Serious deficiences exist in key security control areas; short term focus required	Sufficient Security controls in place	Sufficient Security controls in place	Sufficient Security controls in place	Not applicable	Sufficient Security controls in place	Not applicable	Not applicable	Sufficient Security controls in place	Sufficient Security controls in place	Sufficient Security controls in place	Sufficient Security controls in place	Sufficient Security controls in place
Shared Tools	Cloud Computing (3rd party services)	For each cloud-based technology implementation, see relevant technology item risks, above																

Risk Assessment Changes - 2011				
Cell ID	**Description**	**Was**	**Now**	**Justification for Change**
E15	Loss/Theft of Portable Digital Storage Devices	4 x 2	4 x 1	Fewer reports of Loss / Theft than with Laptops and Crypography
O11	Malicious Email/Spam - Desktop PCs	4 x 2	4 x 1	Fewer responses to Malicious Email in 2011 (Figure 1)
O12	Malicious Email/Spam - Laptops & Tablet PCs	4 x 2	4 x 1	Fewer responses to Malicious Email in 2011 (Figure 1)
O13	Malicious Email/Spam - Handheld Devices	4 x 2	4 x 1	Fewer responses to Malicious Email in 2011 (Figure 1)
M11	Targeted Attacks - Desktop PCs	4 x 3	4 x 2	Significant Reduction in RDP attacks
M12	Targeted Attacks - Laptop and Tablet PCs	4 x 3	4 x 2	Significant Reduction in RDP attacks
S21	Remote Access - Network Printers	4 x 2	4 x 1	Replacement of many Printers transferred into Private IP space

Risk Management Priorities for 2012	
2011*	Continued efforts on desktop/laptop/handheld config/patch management
2011*	Continued efforts to reduce threat by remote access by securing perimeter security (service protection)
1	Complete rollout of Western ROAMs, restriction of direct-from-internet remote desktop access, and (re)establishment of access approval/review processes
2	A focus on improved data protection, in particular data stored on end user devices (desktop/laptop/hand-held/mobile storage..)

* Activities begun in 2011, with efforts continuing through 2012