E-Business Curricula and Cybercrime: A Continuing Error of Omission?

Marcelline Fusilier[1,*], Charlie Penrod[2]

[1]College of Business and Economics, American University of Kuwait, Safat 13034 Kuwait
[2]School of Business, Northwestern State University of Louisiana, Natchitoches, Louisiana,71497, USA
*Corresponding Author: mfusilier@auk.edu.kw

Abstract   The growth of e-business has been accompanied by even faster increases in losses from security breaches, legal problems, and cybercrime. These unnecessary costs inhibit the growth and efficiency of e-business worldwide. Professional education in e-business can help address these problems by providing students with coursework aimed at them. The present study extends research begun in 2007 on course coverage of law, security, and ethics in e-business master's programs. Data were collected from university web sites in 2010 on 104 e-business master's curricula worldwide and compared with 2007 data. Results suggest no significant coverage changes and a majority of program curricula still lack courses in law, security, or ethics. Coverage of these topics did not apparently increase from 2007 to 2010 despite the rapid acceleration of cybercrime during the same period. However the change in coverage of topics related to cybercrime varied by region of the world in which e-business degree programs are based.

Keywords   e-Business, Cybercrime, Higher Education

1. Introduction

The financial impact of cybercrime on e-business and business in general has escalated dramatically in recent years, apparently the fastest growing type of crime (1,2). Businesses all over the world are disrupted, lose sensitive information, and experience productivity declines as a result of cybercrime (3).Results of the 2010/2011 Computer Crime and Security Survey indicate that 67 percent of respondents experienced malware infection (2). According to the Internet Crime Complaint Center 2012 report (4), losses from Internet crime are up 8.3 percent over the previous year. Despite the cost and pervasiveness of cybercrime, a survey of over 9,300 business and technology executives in 128 countries found that businesses' use of key technology safeguards are on the decline and fewer than half have security awareness training programs for employees (5).

Zhao and Zhao (6) identified various security vulnerabilities on up to one-third of Fortune 500 corporations' retail e-commerce. It is therefore not surprising that 40 percent of e-commerce customers sampled in a recent study expressed concerns about the security of web sites (7).This may reduce online shopping (8).

The 2011 Cyber Security Watch Survey report (9) concluded that employees need greater skills to address such problems. The Comprehensive National Cyber security Initiative(10) of the U.S. government has been expanded by President Obama to include a major goal to increase education focused on security (Initiative 8).In a review of legal harmonization on cybercrime, Clough (11) argued that education and technological solutions are as important as legal regulation in addressing the challenges of cybercrime. The paper's next section reviews the literature on the extent to which topics aimed at addressing cybercrime have been covered by educational programs intended to prepare professionals for e-business.

2. Literature Review

Law (12), security (13), and ethics (14) are necessary foundations for effective e-business. These factors can help to promote trust among e-consumers and prevent cybercrime. The Economist Intelligence Unit report in 2009 [15] recognized the importance of law by adding a legal component to estimate countries' e-readiness. Blythe (16) tracked the development and spread of electronic signature law around the world to promote security of Internet transactions. Abyad (17) contended that trust is more critical in e-commerce than in traditional shopping because it involves more uncertainty and risk. E-business security measures can help to build consumer trust (17,18,19).Shahibi and Fakeh (13) reported that technology concerns such as virus protection during online transaction and safe online payment were viewed by consumers as important determinants of e-commerce providers' security.

Ethics in e-business can take the form of privacy policies and clearly stated return policies (17).Maury and Kleiner (20) pointed out the need to build ethical values into e-business to

improve consumer confidence.Bruce and Edgington (21) reported that ethics education in MBA programs can influence students' beliefs and behavior.Harris et al. (22) argued that "instruction in ethics should be a core component of the curriculum" (p. 187) and include a particular focus on cybercrime. Together, these studies suggest that ethics education may be basic to achieving the goals of improved security practices, legal compliance, and customer trust. Moreover, coursework in the areas of law, security, and ethics may serve to create an awareness of the dimensions of the cybercrime problem as well as prevent it. Fusilier and Penrod (23) reported that education programs for e-business professionals do not appear to provide sufficient preparation for preventing e-business legal and security problems even though evidence indicates that law, security, and ethics are necessary for enabling e-business.

2.2. Law, Security, and Ethics in e-business Education

Cybercrime is not viewed with the same ethical certainty as other types of crime such as robbery or assault (24).Incorporating cyber ethics into curricula for youth is increasingly seen as a means for prevention (24).McCrohan, Engel, and Harvey (25) demonstrated that it is possible to change security behaviors of Internet users through training. In spite of this, evidence suggests that e-business degree programs in higher education include: (a) ethics courses in fewer than five percent of curricula (26,27), (b) law and/or security courses in zero to 50 percent of curricula (28,29,30,31), and (c) e-business security courses in only 54 percent of the graduate and undergraduate e-business programs (32).A contrary finding was reported by Mechitov, Moshkovich, and Olson (33) that 70 percent of the masters of science in electronic commerce programs sampled had security and law course(s). However that result was based on a sample of only 10 programs.In a study of 163 e-business master's programs, Fusilier and Penrod (23) found law, security, and ethics courses offered in 47, 33, and 10 percent of e-business master's programs respectively. Two studies took a different approach to assessing curriculum content by coding e-business course syllabi (34,35). Results suggested that fewer than half of the syllabi included topics on legal issues, ethics, or privacy. Slightly over half of the syllabi included security as a topic. No previous studies were found that reported the existence of courses on prevention of cybercrime.

2.3. Purpose of the Study

It seems that the increase in cybercrime in recent years would necessitate more courses in e-business curricula to address the problem. Previous literature indicates a baseline underrepresentation of courses in e-business curricula focused on addressing cybercrime.Has this changed in recent years?The present study explored the responsiveness of universities to the wave of cybercrime. A repeated measures

analysis was conducted to explore the extent of law, security, and ethics courses in master's degree e-business programs worldwide from 2007 to 2010. The purpose is to investigate whether cybercrime education has improved during this period as cybercrime has dramatically increased. Only e-business programs were studied which provides a focused test of curricular efforts regarding factors related to cybercrime. This type of program seems likely to include cybercrime prevention coursework because cybercrime is a serious threat to online business and the consumer trust so critical for e-business to thrive.

3. Method

3.1. e-business Programs

The list of e-business master's programs used in the Fusilier and Penrod (23) study was obtained. The list included e-business master's programs that existed in 2007.The web sites of the schools offering the programs were checked in 2010 to determine whether each program was still being offered at that time. It is not unusual for e-business programs to be revised or canceled (36). Fifty-nine of the 163programs included in the earlier study were no longer listed on the web sites of the schools that had offered them in 2007. This suggested that 59 programs had been canceled. The present study therefore focused on the remaining 104 programs that had been analyzed by Fusilier and Penrod (23) in 2007 and were still operational in 2010. The list of courses comprising the curriculum of each program was accessed on the web site of the school offering it. Web sites in languages other than English were either translated by the authors or by an Internet translation site.

3.2. Course Categories

The online title and description for every course in the 104 e-business curricula were examined to determine whether the course appeared to cover the topic of (1) business law, (2) e-business law, (3) ethics, or (4) security. Each of these topics served as a category for courses. A course was included in a category if its title and description indicated that it mainly covered the topic of the category. For example, if a course mainly covered business law, it would be assigned to the business law category. Courses that did not cover any of the four topics of interest to the present study were not included in the categories. For example, a general finance course would not fit with any of the categories because its main focus was not on any of the four topics of interest.

After assigning courses to categories, the total numbers of courses in each of the four categories could be tabulated for all of the 104 e-business program curricula. The specific procedure used for placing courses into categories was:

1.Business Law: This category was for course titles and descriptions that indicated coverage of the topic of general

business law. Examples of titles of courses that were included in this category were: "Survey of Business Law" and "Legal Environment of Business."In a few cases, legal issues and ethics were included in the same course (four incidents). Descriptions of these combination courses indicated a predominant emphasis on legal topics. They were therefore coded as business law or e-business law, whichever was most appropriate. No courses were counted in more than one coding category.

2.e-business Law: Courses were assigned to this category if their title and description indicated that they covered law in the context of e-business. Examples of such course titles included "Cyber law" and "e-business Intellectual Property."

3.Ethics:Courses with titles that concerned ethics were coded into this category. "Business Ethics and Society" and "Applied Ethics" were examples of course titles that were included in the category for ethics.

4.Security: The security category was for courses that covered topics such as security, cryptography, encryption technology, risk analysis, firewall technology, intrusion detection system, handling computer viruses, etc. Two example course titles are: "Electronic Payment and Security" and "Computer Security for e-commerce."

The procedure of using course titles as a measure of topic coverage is consistent with previous research (23,28,32,30,37). Courses in the present sample were also designated as being required or elective in thee-business curriculum of which they were a part.

4. Results

Of the 104 e-business masters programs analyzed in the present study, forty-six were based in North America (Canada [5], USA [40], and Mexico [1]), 23 in Australia/New Zealand [21 and 2, respectively], 27 in Europe, and 8 in Asia. Table 1 shows the current findings on representation of law (business or e-business), security, and ethics courses in the master's e-business curricula as well as the previous results of Fusilier and Penrod (23).For each of the three categories, fewer than half of the programs included even one course, required or elective. The 2010 data suggest that 61 percent of the programs did not include a single business law course while 64 percent did not offer a course dedicated to security. Nearly 90 percent of the programs did not include a course clearly focused on ethics. Repeated measures ANOVA for the 2010 and 2007 data did not show significant differences between the years for any of the required course types: Business law (Wilks' Lambda = 0.976, $F(1,96) = 2.344$, $p = 0.129$), e-business law (Wilks' Lambda = 0.993, $F(1,96) = 0.639$, $p = 0.426$), and security (Wilks' Lambda = 0.994, $F(1,96) = 0.585$, $p = 0.446$). This suggests that course offerings did not change from 2007 to 2010.Figure 1 graphically displays the percentages of programs offering various numbers of each type of course.

Table 1. Frequencies and Percentages of e-Business Master's Programs According to Law, Security, and Ethics Courses Offered – The Present Study's 2010 data and 2007 percentages from Fusilier and Penrod (23)

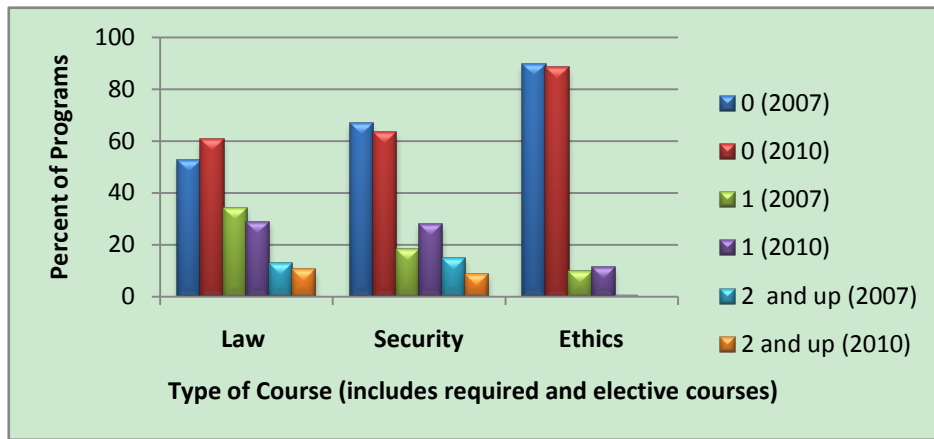| Courses in program	Law (includes all required and elective business and e-business law)			Security (includes required and elective courses)			Ethics (includes required and elective courses)		
	2010 Programs	2010 Percentage	2007 Percentage	2010 Programs	2010 Percentage	2007 Percentage	2010 Programs	2010 Percentage	2007 Percentage
0	63	60.6	52.8	66	63.5	66.9	92	88.5	89.6
1	30	28.8	34.3	29	27.9	18.4	12	11.5	9.8
2	7	6.7	9.2	7	6.7	8.6	0	0	0.6
3	1	1.0	2.5	0	0	4.3	0	0	0
More than 3	3	3.0	1.2	2	1.9	1.8	0	0	0
Total Programs	104	100	100	104	100	100	104	100	100

Figure 1. Numbers of Law, Security, and Ethics Courses offered in e-business Master's Programs, 2007 versus 2010(Percentages of programs offering each number of courses were calculated within each year)

4.1. Interactions

Interaction terms were computed to explore changes in course offerings across the years by world region. Results of this analysis could address the question of whether the findings differ according to where the programs are located. Programs based in North America were compared to those based in the rest of the world. This approach was used because there were more programs based in North America than on any other continent. Dividing the sample this way allowed more equal sized groups to be formed. Statistically significant interaction terms were detected for required courses in business law, e-business law, and security. Each is explained below.

Results for required business law courses are displayed in Table 2 and graphed in Figure 2(Wilks' Lambda = 0.938, F(1,96) = 6.309, p = 0.014).To determine the nature of the interaction, three paired sample t-tests were computed comparing the years within the: (a) North American sample and (b) rest of the world. An independent samples t-test was also computed to check for differences between North America and the rest of the world for each year. There was a statistically significant difference for the number of required business law courses offered in North America between 2007 (mean = 0.27) and 2010 (mean = 0.11) [t(44) = -2.461,

p = 0.018]. There was no significant difference between 2007 and 2010 for the programs based in the other parts of the world. A difference was detected for 2007 between the North American programs (mean = 0.27) and those based in other parts of the world for 2007 (mean = 0.04) [t(55) = 2.919, p = 0.005]. Equal variances could not be assumed for this test of the 2007 means (Levine's test for equality of variance, F = 49.621, p = .001). Findings suggest the interaction effect comes from the apparent decrease in business law course offerings in the study's North American programs from 2007 to 2010 and the difference between the world regions in 2007.

A different result can be seen for required e-business law courses in Table 3 and Figure 3(Wilks' Lambda = 0.961, F(1,96) = 3.915, p = 0.051).The average number of required e-business law courses appeared higher in 2010 (mean = .016) than in 2007 (mean = 0.07) for the North American sample [t(44) = 2.072, p = 0.044].No difference was apparent between years for the programs based in the rest of the world. Likewise no differences were detected for either year between the world regions. The interaction effect apparently comes from the greater number of e-business law courses required in 2010 than in 2007 for the programs based in North America.

Table 2. Results of Interaction Test, Year x Geographic Region, on Required Business Law Course Offerings - Repeated Measures ANOVA

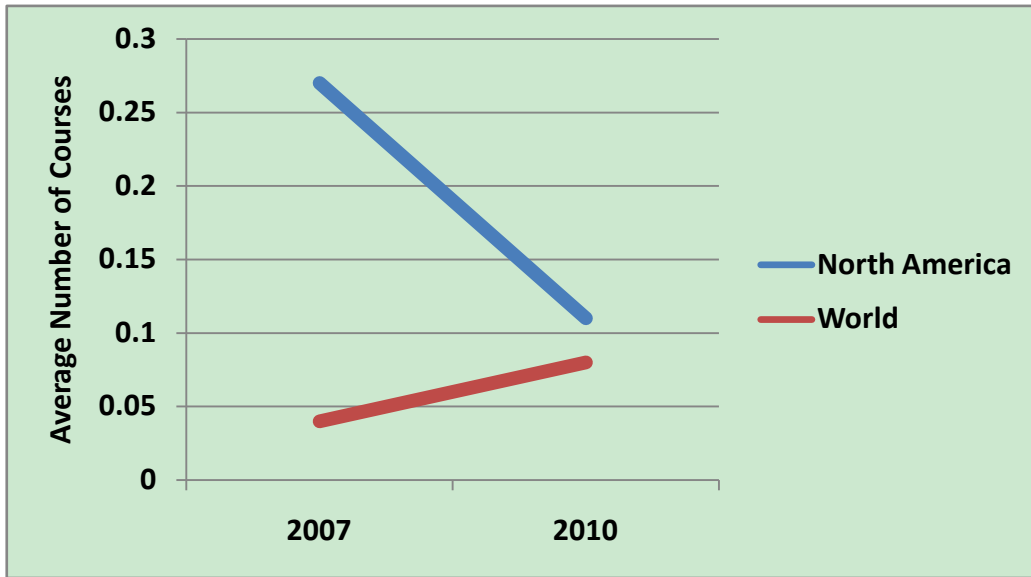| Source	Type III Sum of Squares	df	Mean Square	F	Sig.
Year	.169	1	.169	2.344	.129
Year x North America and World	.455	1	.455	6.309	.014
Error	6.918	96	.072		

Figure 2.   Interaction Effect - Year x Geographic Location of Program on Required Business Law Courses

Table 3.   Results of Interaction Test, Year x Geographic Region, on Required e-Business Law Course Offerings - Repeated Measures ANOVA

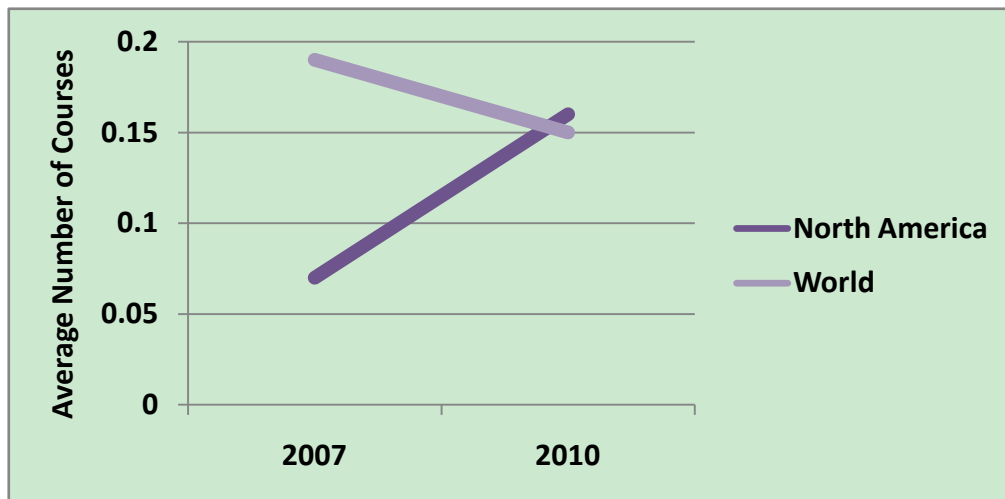| Source	Type III Sum of Squares	df	Mean Square	F	Sig.
Year	.032	1	.032	.639	.426
Year x North America and World	.195	1	.195	3.915	.051
Error	4.784	96	.050		

Figure 3. Interaction Effect - Year x Geographic Location of Program on Required e-Business Law Courses

Table 4.Results of Interaction Test, Year x Geographic Region, on Required Security Course Offerings - Repeated Measures ANOVA

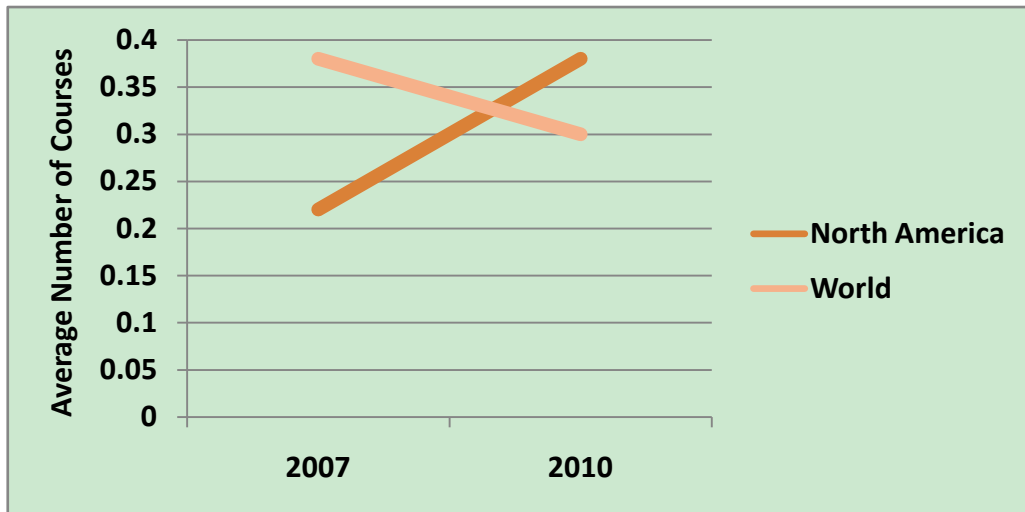| Source	Type III Sum of Squares	df	Mean Square	F	Sig.
Year	.078	1	.078	.585	.446
Year x North America and World	.649	1	.649	4.869	.030
Error	12.805	96	.133		

Figure 4. Interaction Effect - Year x Geographic Location of Program on Required Security Courses

See Table 4 and the graph in Figure 4 results of the interaction effect on required security course offerings(Wilks' Lambda = 0.952, F(1,96) = 4.869, p = 0.03).More security courses appeared to be offered in the North American programs on average in 2010 (mean = 0.38) than in 2007 (mean = 0.22) [t(44) = 2.006, p = 0.051].Again, no differences were apparent between years for programs based outside of North America or between world regions for either year.

5. Discussion

Previous research has documented low representation of law, security, and ethics coursework in e-business education from the beginning of the past decade (e.g.,30,31).The present study's data do not indicate improvements in this low-representation pattern: changes in the percentages of programs including law, security, or ethics courses from 2007 to 2010 are not significant. If instruction in these topics is strongly related to awareness, prevention, and remedies for cybercrime, then their absence from university e-business programs might help to explain the growth of cybercrime with the spread of e-business.

The present data suggest that e-business programs in North America have increased their e-business law and security course offerings from 2007 to 2010 however this increase is not enough: the average number of courses per program is still less than 1.0.The decrease in business law courses in the sample's North American programs might be explained by a decision to focus more courses specifically on e-business law. The business law course requirement may have been shifted to e-business law, accounting for the increase in the latter area.

There is a clear need for cyber-security education. The present study found that 63.5 percent of the programs in the 2010 sample included no security course at all, either required or elective. This corroborates the Kim et al. (32) conclusion of a general deficiency in security coursework. The apparent lack of security coverage in degree programs may strongly contribute to the widespread security problems in e-business today. Liu and Mackie (38) provide details for teaching security for e-commerce.

Ethics coursework also appears needed. Evidence suggests that requiring an ethics course in an MBA curriculum contributes to students' views of effective coverage of ethics in the program (21). However 88.5 percent of the programs reviewed in the present study offered no courses obviously devoted to ethics.

E-business has tremendous potential for positive economic impact and appears more recession resistant than retail sales in general. Despite the global economic downturn, e-commerce is currently surging with a more than 15.2 percent increase over last year's sales (39).It has shown consistent rapid global growth and improved delivery of goods and services while potentially reducing the impact of doing business on the natural environment (40). However,

cybercrime can undermine these benefits. Technology changes rapidly and teaching students to have an orientation toward security, ethics, and legal issues will allow them to stay in touch with developments regarding cybercrime. Such instruction may also help e-business professionals to build ethical organizational cultures that can curtail internal criminal activity. It is incumbent on universities to include coursework on this issue. Academic studies recommending revision of curricula, however, do not seem to be enough. More than ten years of research findings and recommendations appear to have had no significant impact on e-business curricula regarding law, security, and ethics coursework.

Fusilier and Penrod (23) used regulatory focus theory to explain the relative neglect of courses in business curricula that focus on loss prevention, such as law, security, and ethics. These authors argued that business schools tend to emphasize coursework that promotes students' ability to attain gains, such as higher revenue or market share. Coursework focused on gains, such as marketing, were found to be more prevalent in business school curricula than the prevention-focused courses of law, security, and ethics. However, ongoing economic uncertainty may impose pressures on business schools to provide more balanced coverage between activities that address attainment of gain and prevention of loss.

University characteristics may also be partially to blame. Financial pressures and bureaucratic, unresponsive organizational structures may result in curricula that do not address the needs of society and students. Armour (41) contended that e-business programs are being designed more to attract enrollment rather than to effectively equip students to cope with the demands of an e-business career. This is consistent with Gumport's (42) observation that many universities are abdicating their roles as social institutions and instead taking on a profit orientation through increased enrollments. Unfortunately, such a role shift might result in neglect of universities' social and educational responsibilities. Universities must address cybercrime as leading social institutions regardless of economic imperatives. Activities consistent with this goal should include instruction in areas that bear on the issue.

5.1. Limitations of the Study and Directions for Future Research

The present study did not address the connection of university instruction in law, security, and ethics to actual behaviors directed at preventing and managing cybercrime. Future research could relate curriculum coverage of these topics to graduates' behaviors directed at addressing cybercrime. Another potential shortcoming concerns the extent to which course coding is based solely on course titles and descriptions represent course content. Studies could investigate course content in a variety of course titles to determine the extent to which law, ethics, and security might be infused into other academic subjects. King et al. (34) and

Rezaee et al. (35) have already developed coding procedures for e-commerce syllabi, and these procedures could be applied in studies of course content. Additionally, degree programs in related areas, such as computer science, might be studied to see if topics related to cybercrime are meaningfully covered in such curricula. If so, e-business degree programs could use these practices as a guide for improvement.

6. Conclusion

Tracking more than 100 e-business programs over a recent three-year period found no discernible university education changes in response to the growing incidence and seriousness of cybercrime. Accordingly, the present findings strongly suggest including more law, security, and ethics courses in e-business master's programs. Generally, it appears that curricula should be more responsive to stakeholder needs and the events that can impact e-business. Educational initiatives to address cybercrime can add to the other management and prevention approaches currently being implemented such as legal remedies that extend across national borders. Although governmental and administrative limitations often constrain master's programs on the numbers of courses they can include, having even one course in each area would be an improvement for a majority of the programs. Offering courses dedicated to each topic could assure coverage of these vital subjects and also streamline program assessment.

REFERENCES

[1] Ponemon Institute (2010). First annual cost of cybercrime study. Available online at http://www.arcsight.com/collateral/whitepapers/Ponemon_Cost_of_Cyber_Crime_study_2010.pdf(Accessed July 18, 2013).

[2] R. Richardson(2010). 2010/2011 CSI Computer Crime and Security Survey.Available online at: http://gocsi.com/survey/(Accessed July 18, 2013).

[3] Ponemon Institute (2012). The Impact of Cybercrime on Business. Available online at: www.checkpoint.com/products/downloads/whitepapers/ponemon-cybercrime-2012.pdf (Accessed July 18, 2013).

[4] Internet Crime Complaint Center (IC3) Internet Crime Report (2012).Available online at: http://www.fbi.gov/news/pressrel/press-releases/ic3-2012-internet-crime-report-released (Accessed July 18 2013).

[5] Global State of Information Security Survey (2013). Available online at: http://www.pwc.com/gx/en/consulting-services/information-security-survey/download.jhtml (Accessed July18, 2013).

[6] J.J. Zhao, S.Y. Zhao. Retail e-commerce security status among Fortune 500 corporations, Journal of Education for Business, Vol. 87, No. 3, pp. 136-144, 2012.

[7] K.T. Smith (2011). Consumer perceptions regarding e-commerce and related risks.B>Quest, 2011 issue, 1-20.Available online at: http://www.westga.edu/~bquest/2011/ecommerce11.pdf(Accessed July 18, 2013).

[8] S.K. Jain, M Jain.Exploring impact of consumer and product characteristics on e-commerce adoption: A study of consumers in India, Journal of Technology Management for Growing Economies, Vol. 2, No. 2, pp. 35-64, 2011.

[9] 2011 CyberSecurity Watch Survey (2011). Available online at: www.cert.org/archive/pdf/CyberSecuritySurvey2011Data.pdf (Accessed July 18, 2013).

[10] Comprehensive National Cybersecurity Initiative (2012). Available online at: http://www.whitehouse.gov/cybersecurity/comprehensive-national-cybersecurity-initiative(Accessed July 18, 2013).

[11] J. Clough. Cybercrime, Commonwealth Law Bulletin, Vol. 37, No. 4, pp. 671-680, 2011.

[12] M.J. Taylor, J.McWilliam, D.Gresty, M. Hanneghan. Cyber law: Case studies in the SME environment, Systems Research and Behavioral Science, Vol. 22, No.3, pp. 261-267, 2005.

[13] M.S. Shahibi, S.K.W. Fakeh. Security factor and trust in e-commerce transactions. Australian Journal of Basic and Applied Sciences, Vol. 5, No.12, pp. 2028-2033, 2011.

[14] A.M. Adam, A. Aderet, A. Sadeh. Do ethics matter to e-consumers? Journal of Internet Commerce, Vol. 6, No. 2, pp. 19-34, 2007.

[15] Economist Intelligence Unit. e-readiness rankings 2009. Available onlineat:http://graphics.eiu.com/pdf/E-readiness%20rankings.pdf(Accessed July 18, 2013).

[16] S.E. Blythe. Improving cyber-security in Turkey via refinements in e-commerce law.International Journal of Management, Vol. 28, No.2, pp. 478-487, 2011.

[17] A. Abyad. Consumer trust in e-commerce.Middle East Journal of Business, Vol. 6, No. 3, pp. 3-6, 2011.

[18] A. Angriawan, R. Thakur.A parsimonious model of the antecedents and consequence of online trust: An uncertainty perspective,Journal of Internet Commerce,Vol. 7, No. 1, pp. 74-94, 2008.

[19] G. van Noort, P. Kerkhof, B.M. Fennis.Online versus conventional shopping: Consumers' risk perception and regulatory focus,CyberPsychology& Behavior, Vol. 10, No.5, pp.731-733, 2007.

[20] M.D. Maury, D.S. Kleiner.E-commerce, ethical commerce?Journal of Business Ethics, Vol. 36, No.1/2, pp. 21-31, 2002.

[21] G. Bruce, R.Edgington.Ethics education in MBA programs: Effectiveness and effects, International Journal of Management and Marketing Research, Vol. 1, No.1), pp. 49-69, 2008.

[22] A.L. Harris, M. Lang, D.Yates, S.E. Kruck. Incorporating ethics and social responsibility in IS education, Journal of Information Systems Education, Vol. 22, No.3, pp. 183-189, 2011.

[23] M. Fusilier, C. Penrod. E-crime prevention: An investigation of the preparation of e-commerce professionals,Journal of Internet Commerce,Vol. 8, No.1-2, pp. 2-22, 2009.

[24] J.J. Baum. CyberEthics: The new frontier,TechTrends,Vol. 49, No. 6, pp. 54-55, 2005.

[25] K.F.McCrohan, K. Engel, J.W. Harvey. Influence of awareness and training on cyber security,Journal of Internet Commerce,Vol. 9, No.1, pp. 23-41, 2010.

[26] S. Davis, K. Siau, K.Dhenuvakonda.A fit-gap analysis of e-business curricula vs. industry needs,Communications of the ACM,Vol. 46, No.12, pp. 167-177, 2003.

[27] E.Y. Li,H.J.R.Yen,C.Y.J. Cheng. A fit-gap analysis of e-business curricula and job demand in Taiwan and the U.S.,Computers& Education,Vol. 51, No. 3, pp. 969-987, 2008.

[28] J. Burkey.The evolution of electronic commerce education,Journal of Education for Business,Vol. 82, No. 5, pp. 276-281, 2007.

[29] J. Chen, B. Panigrahi, E.G. Zapatero.Undergraduate e-business curricula at the AACSB accredited business schools in the U.S., Review of Business Research, Vol. 8, No. 2, pp. 71-77, 2008.

[30] K.A.Dunning, B.S.Vijayaraman, R. Krovi, P.S. Kahai. Graduate e-business program design and evaluation, Journal of Computer Information Systems, Vol. 42, No. 1, pp. 58-64, 2001.

[31] H.L.Ethridge, K.H.Y.Hsu, T.E.Wilson, E-business education at AACSB-affiliated business schools: A survey of programs and curricula,Journal of Education for Business,Vol. 76, No. 6, pp. 328-331, 2001.

[32] H. Kim, Y. Han, S. Kim, M. Choi.A curriculum design for e-commerce security,Journal of Information Systems Education,Vol. 16, No.1, pp. 55-62, 2005.

[33] A.I.Mechitov, H. Moshkovich, D.L. Olson. The master's degrees in e-commerce: A survey study,Journal of Computer Information Systems,Vol. 42, No. 4, pp. 29-34, 2002.

[34] C.G.King,S.L.Frank, R.G. Platt. E-commerce courses: Overview of nature and content,Journal of Education for Business,Vol. 76, No. 6, pp. 332-337, 2001.

[35] Z. Rezaee, K.R.Lambert,W.K. Harmon. Electronic commerce education: Analysis of existing courses,Accounting Education: An International Journal,Vol. 15, No.1, pp. 73-88, 2006.

[36] M. Fusilier, S. Durlabhji.Troubling turnover: An investigation of discontinued e-commerce master's degree programs,Proceedingsof the Northeast DSI Annual Conference, Brooklyn, NY, USA, March 28-30, 2008.

[37] J.E. Novitzki. E-business education: A quantitative review of program attributes and offerings, Proceedingsof the 17th Annual Conference of the International Academy for Information Management, December 13-15, Barcelona, Spain, 2002.

[38] C. Liu, B.G. Mackie. Teaching security techniques in an e-commerce course, Journal of Information Systems Education, Vol. 17, No.1, pp.5-10, 2006.

[39] U.S. Census Bureau News Quarterly retail e-commerce sales 1st quarter 2013, May 15, 2013. Available online at: http://www.census.gov/retail/mrts/www/data/pdf/13q1.pdf (Accessed July 18, 2013).

[40] R.H.Gay, R.A.Davis, D.T.Phillips, D.Z. Sui. Modeling paradigm for the environmental impacts of the digital economy,Journal of Organizational Computing & Electronic Commerce,Vol. 15, No. 1, pp. 61-82, 2005.

[41] S. Armour. Degrees in e-commerce seem less dazzling. USA Today, January 16, 2001. Available online at http://www.usatoday.com/careers/news/2001-01-16-dotcom degree.htm (Accessed July 19, 2013).

[42] P.J. Gumport. Academic restructuring: Organizational change and institutional imperatives,Higher Education,Vol. 39, No. 1,pp. 67-91, 2000.