Teaching Advanced Computing Technologies to Managers, Engineers and Other Professionals

Ljiljana Brankovic, Stephan Chalup and Mark Wallis
The University of Newcastle
Corresponding Author Email: Ljiljana.Brankovic@newcastle.edu.au

CONTEXT Nowadays most businesses in Australia maintain a website to advertise their products and services and some to also conduct online sales and payments. Many have an additional Facebook page or utilise other on-line tools and phone apps. Data is now considered to be one of the most valuable assets of companies, and many are using Cloud services for safe storage and data processing. With the rapid growth of the volume and diversity of collected data, and its increasing importance for strategic planning, many businesses have started using big data analytics techniques to extract knowledge from data to support their decisions. All of the above technologies require formal security management or otherwise they can become a weak link which can create security vulnerabilities and expose company assets. While some of the computing tasks and their associated security can be outsourced to specialised IT companies, it is crucial that business managers and professionals have sufficient conceptual understanding of these topics in order to make quality decisions and ensure the survival of their business in the modern world.

PURPOSE The question studied it this paper is how best to teach advanced computing technologies to business managers, engineers and other professionals with different prior experience and educational backgrounds.

APPROACH We describe a curriculum for teaching the most relevant computing technologies to professionals working in various branches of industry and business, mostly based on a Graduate Certificate in Advanced Computing Technologies for Business, currently being taught in an intensive weekend mode. A similar program could also be taught online with one intensive face-to-face session per course.

RESULTS The limited analysis possible during the first run of the program indicates that the delivered courses were well-received by the students who have been able to successfully master the curriculum presented in an intensive weekend delivery mode.

CONCLUSIONS While virtually all Australian universities have programs for training IT professionals, apart for a few isolated courses, few universities provide opportunities for other graduates to learn the most relevant computing technologies. Such programs should be developed and included in engineering and business coursework Masters programs and made available to middle and senior business managers.

KEYWORDS Cloud Computing, Big Data, IT Security.

Introduction

Nowadays virtually all businesses in Australia and the Western world maintain an online presence. Some use it only to announce their contact details and opening hours, others to advertise their product and services, while a growing number use their websites for e-commerce, including on-line payment systems. While having an online presence offers businesses exposure to customers that they would have otherwise not be able to reach and convenience of electronic commerce, companies' Web servers also represent a gateway for hackers and malware that could potentially infect and compromise the computer system of the company (Stallings, 2017). This year alone we have witnessed an alarming number of businesses falling victim to ransomware, such as WannaCry (Symantec Security Response 2017), malicious software that encrypts all data files on the server and where the decryption key is made available only after a ransom has been paid to the attackers. The yearly cost of ransomware in Australia has been conservatively estimated to a billion Australian dollars (Belot & Borys, 2017) while the global cost of cybercrime has been expected to reach six trillion US dollars in 2021 (Morgan, 2016).

Not surprisingly, there is shortage of cybersecurity personnel, with around one million new cybersecurity jobs in 2016 (Morgan, 2016). Possibly more importantly, businesses are still reluctant to invest into cybersecurity, thus bearing unnecessarily high cost of data breaches, averaging 1.3 million US dollars for enterprises and 117,000 US dollars for small business per incident in North America in 2017 (Kaspersky Lab, 2017). In this context, the role of universities in Australia and worldwide is not only to establish degrees to graduate a sufficient number of cybersecurity specialists but also to provide cybersecurity courses and programs suitable for business managers, engineers, IT and other professional, so as to raise awareness of importance of cybersecurity and facilitate better informed decision making.

The situation is similar in other areas where technology meets business. For example, for many years Data Mining has been a subject that involved a solid education in machine learning, applied statistics and relevant database techniques. Recently the field experienced a massive boom due to the availability of an abundance of data on the internet, the success of Google's search engines, the availability of GPU computing and the so called "Big Bang of Artificial Intelligence". The latter occurred in about 2012 when it was suddenly recognised that artificial neural networks, after some design changes that added several hidden layers of neurons, can solve many challenging pattern recognition and control tasks that the community and relevant industries have been struggling with for the past twenty years (Krizhevsky et al., 2012). This new paradigm, called "Deep Learning", made headlines on all machine learning blogs for the past five years (Goodfellow et al., 2016). The majority of papers at all major machine learning conferences currently involve deep learning.

Major companies such as Facebook and Google have already made substantial investments into deep learning (for example, Google acquired DeepMind Technologies in 2014) and other companies now massively investing in this field including social media, finance and the transforming automotive industry, hoping to tap into possibilities presented by deep learning. There is a high demand for competent graduates in data analytics from industry. Student numbers in classes on AI and machine learning have increased by factors of 2-4 at many Australian Universities. However, what currently is missing are courses and programs suitable for managers and other professionals.

Cloud Computing is another area experiencing high growth. Managers are increasingly becoming required to understand concepts of scalability and resource management so they can direct IT resources within their organisations. There is a lack of courseware currently available that is able to teach highly technical concepts such as how the Cloud works to non-technical audiences.

In this paper, we explore opportunities for cross-disciplinary courses and programs teaching advanced computing technologies to business managers, engineers, IT and other professionals. We present a curriculum mostly based on the Graduate Certificate in Advanced Computing Technologies for Business that is currently running in an intensive weekend mode to accommodate students who are working full time.

Curriculum

The following curriculum combines modules in the acutely important domains of IT security, Cloud Computing and Big Data Analytics. The aim of the program is to provide managers and professionals with the necessary conceptual knowledge to lead teams of data scientists, security and privacy experts and storage specialists, and to be able to make informed decisions. None of the modules requires specific prerequisites and all the modules have the aim to educate students about the most important concepts and tools in the domain. The delivery mode can be either face-to-face intensive mode, preferably on weekends to accommodate full-time working students, or online mode with occasional face-to-face sessions.

The assessment is similar for all modules and includes online quizzes, a research report and a presentation. The purpose of the online quizzes is to examine the knowledge and deeper understanding acquired in the module, as well as the students' ability to continue independent learning. The quizzes consist of a combination of multiple-choice questions, short answers and mini projects. For the research report, the students independently explore a given topic and describe their findings in a report, and present it orally in the class. Such assessment is more suitable for the cross-disciplinary student cohort and takes them away from the rigidity of the classical exam.

We next outline the various modules as presented in the graduate certificate program.

Privacy

Table 1: Privacy topics

What is privacy? • Definition • Examples of privacy breaches
Privacy history • Did people enjoy privacy throughout history or is it a modern invention?
Psychological aspects • Do we, as individuals, need privacy for our mental wellbeing?
Privacy and human rights • Privacy International
Privacy laws, regulations and acts in different countries • Australia (Privacy Act and its amendments; Australian Privacy Principles) • USA • European Union
Security vs privacy • Understanding the relationship between security and privacy
Data collection, publishing and mining, and associated privacy issues • Privacy preserving data publishing (k-anonymity, differential privacy, etc.) • Balance between privacy and utility
Privacy-enhancing technologies and tools • Virtual Private Networks • Communication anonymisers, private browsing and search engines • Encrypt your emails - PGP • Private Messaging

Understanding privacy principles and privacy obligations towards clients is very important for those business and government sectors that collect and manage any kind of personal data. The students are taught their legal obligations in terms of handling such data. The students are also invited to explore privacy as individuals, from a socio-psychological perspective, to be able to fully understand the point of view of organisational clients. In Table 1, the privacy topics are grouped into socio-psychological, legal and technological aspects and coded as yellow, red and blue, respectively, while their overlaps are presented in orange and purple.

Computer Crime

In the computer crime module, the students gain systematic knowledge of types and techniques using in computer crime, as well as the most important counter-measures.

Table 2: Computer crime topics

What is computer crime? • Definition • Examples of computer crime
Types of Cybercrime • Computers as targets • Computers as storage devices • Computers as communications tools
Cybercrime Techniques • Hacking (unauthorized access) - Computer Emergency Response Teams (CERTs). • Malware (Types of malware: viruses, worms, Trojan horses, logic bombs, trapdoors, zombies (bots), etc.; antivirus software) • Distributed Denial of Service Attack (DDoS) and DDoS Countermeasures • Spam • Phishing • Social Engineering
Cybercrime classification • Fraud, Online Scams and Other Theft • Illegal/unauthorized Advertising • Extortion/Threat • Espionage and Cyberwarfare
Cybercrime and the Internet of Things • Examples
Cost of Computer Crime
Intellectual Property (IP) • Copyrights; trademarks; patents

Computer Ethics

Table 3: Computer ethics topics

What is ethics? • Definition; examples
Ethical theories • Metaethics • Nominative Ethics o Utilitarianism; Deontology; Virtue Ethics • Applied Ethics
Computer Ethics • What are the specifics of computer ethics
Examples
Code of Conduct • ACM, IEEE and AITP codes; Google, Lego, Uber

On successful completion of this module, students are able to understand basic ethical concepts and theories, and design principles of conduct that can guide ethical decision making in various contexts. Students first learn the basic ethical theories and then learn about specific contexts created by the proliferation of computer and networking technologies.

Computer Security

This module prepares students to understand a variety of IT security attacks, mechanisms and services, apply fundamental technical skills to assess security threats, vulnerabilities and risks, and apply the necessary skills for bridging the gap between managers and technical personnel to enable efficient communication and decision making. The students were taught the basic principles of cryptography, network security, malware, intrusion and firewalls. After each topic we conducted a hands-on workshop where they broke ciphers, and with our industry partners they performed some basic ethical hacking and studied a piece of malware specially created for the use in the class.

Table 4: Computer security topics

Security attacks, services and mechanisms
Classical ciphers
Breaking classical ciphers hands-on
Breaking classical ciphers hand-on workshop
Modern Cryptography • Stream and block ciphers • Public key cryptography • MAC and hash function • Digital signature
Network Security • Message authentication • Evolution of Networks and Network Security • TCP/IP Security • Wireless Network Security
Ethical Hacking hands-on workshop
Malware • Intruders • Firewalls • Usable Security • Malware
Malware hands-on workshop

Security Risk Management

On successful completion of this module, students are able to understand the theory of and different approaches to risk management, and communicate risk to IT professionals and senior managers to facilitate decision-making.

Table 5: Security risk management topics

What is Risk?
Exposure to Risk
Risk Management Standards
Risk Management Process
Risk Assessment
Risk Reporting

Cloud Computing

In this module the students learn the basics of cloud computing and how it can benefit an organisation in terms of computing power, storage and applications.

Table 6: Cloud computing topics

A review of classic storage systems
What is the Cloud?
How business can leverage the Cloud for storage.
A review of Open and Commercial Cloud offerings
Greenfields vs Migration to the Cloud
Hands-on computer experiments in guided lab workshops

We specifically ask students in this module to apply their domain knowledge and how Cloud Computing can be used in areas they are familiar with. There is a focus on both introducing the technologies used within the Cloud as well as use-cases of common Cloud deployments.

The students were given the task of providing a cost/benefit analysis of a particular common issue with Cloud Computing where they had the opportunity to research and expand upon the course learnings further.

Big Data Analytics

The Big Data Analytics module teaches students the most important concepts and tools that are required to understand the opportunities and challenges that Big Data Analytics faces in the current development of the field and in close connection to relevant aspects of privacy, security and storage technologies.

The offerings of the module in 2016 and 2017 had several students from engineering management degrees but also IT professionals. While most students were sufficiently technically competent and open to receive the technical aspects of the course they were specifically interested in topics that were socially and ethically critical. For example, big data analytics provides enormous new opportunities and power to companies such as Facebook, Google, Netflix and Amazon where the full extent of impact and future consequences for the global society are still unknown.

With the increasing power and abilities of data analytics tools comes also a higher risk with respect to privacy and security and increasing challenges for networking and storage. This module combined topics in all three domains.

Table 6: Big data analytics topics

Introduction to Machine Learning and Data Mining
Introduction to Deep Learning
Big Data case studies; Storing Big Data and Security Issues
Big Data case studies; Hands-on Work in Python and Machine Learning Applications

Data analytics algorithms, their evaluation and the correct interpretation of results can involve advanced mathematical concepts. A challenge in course delivery was the diverse, and for some course participants non-existent, mathematical background in basic statistics, calculus and vector geometry. Therefore, a mode of Tailored Blended Learning (TBL) was applied where each student could be individually mentored during the intense face-to-face sessions on the weekends and via on-line communication while working on assignments during the week.

Due to TBL a satisfying program of topics at AQF level 8 could be selected for each individual student and her/his course project.

Among the concepts and topics to be addressed were some of the basic and fundamental concepts of machine learning such as supervised classification, generalisation, cross-validation, hyperplane geometry, perceptrons, evolutionary algorithms, support vector machines. Further required was knowledge of potential issues that can cause errors such as overfitting and the curse of dimensionality. This was paired with teaching techniques and concepts for classifier evaluation and quality assessment of outcomes such as precision and recall and receiver operating characteristics.

With respect to practical tutorials the course included a brief introduction to Python, Scikit-Learn, Tensorflow and Keras (Géron, 2017). These were taught and practiced using Jupyter notebooks. For accelerating the Deep Learning exercises and allowing a TBL approach for larger classes we plan to employ the UON GPU facilities in future offerings.

Next to a general understanding of data analytics technologies, associated potential pitfalls and quality assurance techniques a practical experience with deep learning (Goodfellow et al., 2016) was a major learning goal of the course. Knowledge of the disruptive impact that deep learning currently has on businesses that use Big Data Analytics is particularly important for start-ups in this domain.

Discussion

From an educational perspective, there is a challenge for Australian Universities to adjust quickly enough to provide all the graduates that industry requires to stay up-to-date with the extremely fast pace of technological development in big data analytics, storage and security. For relevant industries in this sector these technologies are critical to survive and take advantage of the associated industrial transformations, for example, in the automotive sector, medical imaging and many other application domains of big data analytics.

A student who previously was educated to become a “Data Miner” will now be called a “Data Scientist”. The name change could be regarded as an upgrade that reflects the changes of a field that has grown rapidly and now involves advanced techniques not only from applied statistics and traditional data mining, but also statistical physics, topology, differential geometry, logic, neuroscience and various other scientific domains. However, in practice, the name upgrade could also be seen as an attempt to cover-up or counter-balance the many challenges that education in this area faces. The pressure of fast education in this area has to combat the traditionally slow adjustment of educational institutions and the difficulty to acquire appropriate computing equipment and course materials fast enough.

While most Australian universities have programs for training IT professionals, several universities have specialised cybersecurity undergraduate programs, including Edith Cowan University, Deakin University, and University of South Australia. Some universities offer multidisciplinary degrees such as Bachelor of Cyber Security and Behaviour at Western Sydney University or Master of Cybersecurity (Law, Business Ops & IT) at Latrobe University.

However, apart for a few isolated courses, few universities provide opportunities for other graduates to learn the most relevant computing technologies. Such programs should be developed and included in engineering and business coursework Masters Programs and made available to middle and senior business managers.

References

Belot, H., & Borys, S. (2017). Ransomware attack still looms in Australia as Government warns WannaCry threat not over. ABS News. Retrieved on 2 October 2017, from http://www.abc.net.au/news/2017-05-15/ransomware-attack-to-hit-victims-in-australia-government-says/8526346

Géron, A. (2017). *Hands-On Machine Learning with Scikit-Learn and TensorFlow: Concepts, Tools, and Techniques to Build Intelligent Systems*. O'Reilly Media.

Goodfellow, I., Bengio, Y. & Aaron Courville (2016). *Deep Learning*. MIT Press.

Kaspersky Lab. (2017). Kaspersky Lab Survey: Cyberattacks Cost Large Businesses in North America an Average of $1.3M, Retrieved on 2 October 2017, from https://usa.kaspersky.com/about/press-releases/2017_kaspersky-lab-survey-cost-of-cyberattacks-for-large-businesses-in-north-americ

Krizhevsky, A., Sutskever, I., & Hinton, G. E. (2012). ImageNet Classification with Deep Convolutional Neural Networks. In: Pereira, F., Burges, C. J. C., Bottou, L. & Weinberger, K. Q. Advances in Neural Information Processing Systems 25 (NIPS 2012), pp.1097-1105, Curran Associates, Inc.

Morgan, S. (2016). Hackerpocalypse: A Cybercrime Revelation. A 2016 report from Cybersecurity Ventures sponsored by Herjavec Group. Retrieved on 2 October 2017, from https://cybersecurityventures.com/hackerpocalypse-cybercrime-report-2016/

Stallings, W. (2017). *Cryptography and Network Security – Principles and Practice*. 7th Edition, Pearson Education.

Symantec Security Response. (2017). What you need to know about the WannaCry Ransomware. Retrieved on 2 October 2017, from https://www.symantec.com/connect/blogs/what-you-need-know-about-wannacry-ransomware