CAPTURE THE TALENT: SECONDARY SCHOOL EDUCATION WITH CYBER SECURITY COMPETITIONS

Hanif Mohaddes Deylami[1, 2], Mahsa Mohaghegh[1], Abdolhossein Sarrafzadeh[1]
Michael McCauley[1], Iman Tabatabaei Ardekani[1] , Tamsin Kingston[1]

[1]Department of Computing and Information Technology, Unitec Institute of Technology, Private Bag 92025, Victoria Street West, Auckland 1142, New Zealand.
[2]School of Computer Science, Faculty of Information Science and Technology, Universiti Kebangsaan Malaysia, 43600 UKM Bangi, Malaysia.

ABSTRACT

Recent advances in computing have caused cyber security to become an increasingly critical issue that affects our everyday life. Both young and old in society are exposed to benefits and dangers that accompany technological advance. Cyber security education is a vital part of reducing the risks associated with cyber-threats. This is particularly important for current and future youth, who are the most technology-literate generations. Many research studies and competitions have been undertaken around the world to emphasize and identify the significance of cyber security as a relevant and pressing research area. Cyber security competitions are great means of raising interest in the young generation and attracting them to educational programmes in this area. These competitions show the need for cyber security to be taught as a formal subject in secondary schools to enhance the effectiveness of computer science concepts in cyber space. This paper presents an effective educational approach, justifying such competitions as a means of introducing cyber security as a computer science subject for New Zealand secondary school students, and also presents methods of implementation.

KEYWORDS

Cyber security education, Cyber space, Live security competition, Capture the flag.

1. INTRODUCTION

In recent years, cyber security has become a critical issue affecting many aspects of our lives. As a result, many research centers, institutes, and universities have increased focus on security topics within relevant courses. Most of these courses use standard educational tools such as notebooks, PowerPoint slides, and academic articles to convey security concepts. Student performance is usually evaluated by assignments, multiple choice tests, and exams. These are mostly paper-based, with an emphasis on theoretical concepts. While some courses teach using a practical approach, there are significant difficulties associated with this teaching method, and as such this approach is not commonly used. To overcome these difficulties, cyber security competitions could be used to support educational institutions by evaluating students' prior knowledge of this topic. One of the earliest efforts in this area took place in Feb 2004 [1] in San Antonio, Texas, involving secondary school students, their teachers, IT professionals, and companies, and government. The result of this was a real time cyber security competition not very different to a competition that took place between students of US military academies. They provided a report, which attempted to represent the concepts of a cyber security competition, elaborating the

framework and resources, and the related issues of hosting a cyber security competition. Overall they presented the potential structure for such competitions, and became one of the first roadmaps for secondary school-specific cyber security competitions.

The growth of computer security was rapid, and governments had little time to up skill to prepare the basic structure for educating the next generation. Significant problems were faced even in simply adding cyber security as a subject at secondary school level, given the lack of resources, and the fact that teachers had limited time to learn relevant security principles [2]. Educational institutes are faced with the need to fully develop cyber security as part of their educational curriculum, and within this to decide between a theoretical approach, a practical approach, or a balance between the two. Significant effort is required from both teachers and institutes in terms of addressing a comprehensive set of practical security techniques without getting lost in the details of each technology required. There must be a careful selection of the topics, and particularly the way the topics are presented at secondary school level [3]. Focused training in computer science as a subject for secondary school students began in 2011 in New Zealand [4], after it was considered important that students be more than just users of computational technology. As a result, several tertiary institutions in New Zealand have realized the need for developing cyber security programs, and also cyber security competitions to close the skill gap between educational environment and the industry. One of these is Unitec Institute of Technology in Auckland, who have developed a number of programs at all levels of tertiary education [4] and have made significant steps by being the first to organize a cyber security Capture the Flag (CTF) competition exclusively for secondary school students, to challenge them with real-world problems in cyber security, including hacking, pattern identification, and creative thinking. CTF competitions (also called live security competitions) are practical competitions comprising attack and defense components in a virtual environment, where multiple participants attempt to attack the platform in various ways in order to collect points. A great deal of work goes into organizing competitions like this.

The structure of this paper is as follows: Section 2 provides a brief background and history of the development of Cyber Security Education in New Zealand, and discusses several examples of school competitions in New Zealand, the Uk and the United States. Section 3 expands on Unitec's Cyber Security Competition being the first CTF security competition in New Zealand targeting only secondary school students. This section also discusses different topics in cyber security such as ethical web hacking, network forensics, and cryptography. Section 4 shows practical results from data obtained during the live security competition held in Unitec Institute of Technology in September 2015. Section 5 presents some conclusions, and outlines potential future work regarding cyber security education in New Zealand secondary schools, based on Unitec'sCTF competition results and data.

2. BACKGROUND AND HISTORY

Recently we have witnessed numerous technological innovations and developments, a number of which have involved information technology (IT) infrastructure. Society is becoming increasingly dependent on technology and its accompanying cyberspace, and as such there is significant need for education in order to protect technology users. Unfortunately, although cyberspace provides many benefits and advantages to its users, it has also exposed them to multiple dangers. It is important that this raises awareness and equips participants with protection against such dangers in an environment that the use of technology is increasing at a fast pace.

Traditionally, the younger generation has looked to their parents and teachers to educate them about how to deal with risks and dangers. However in the case of technology-related danger, parents and teachers are often less digitally-literate than the younger generation. As a result they

are seldom equipped to teach them cyber safety and cyber security. This makes it necessary for the government educational system to create and formalize information technology and cyber security education.

2.1. Cyber Security Educationin New Zealand (NZ)

Cyber security is a complex matter, and any approach to solving the issues related to cyber security involves physical, procedural and logical forms of protection against threats [5]. Cyber security education is vital in preparing people to implement cyber security practices. Traditionally, formal cyber security education programs have primarily targeted organisational audiences. However recent government regulations and cyber awareness programs such as the Department of Prime Minister and Cabinet's connect smart program in NZ [6], the similar programs in the UK [7], and the USA [8] have targeted businesses and the general public, including younger generations.

In 2011 [6], New Zealand's cyber security strategy recognized several key objectives, one of which was to work with educators and institutes to meet the demand for graduates skilled in cyber security (a response to which could be to arrange cyber security competitions). The current strategy [6] will be reviewed in the end of 2015 to ensure that the government's resources and approach to cyber security are up to date. Figure 1 represents the most current government and non-government based cyber security groups, events and meetings in NZ.

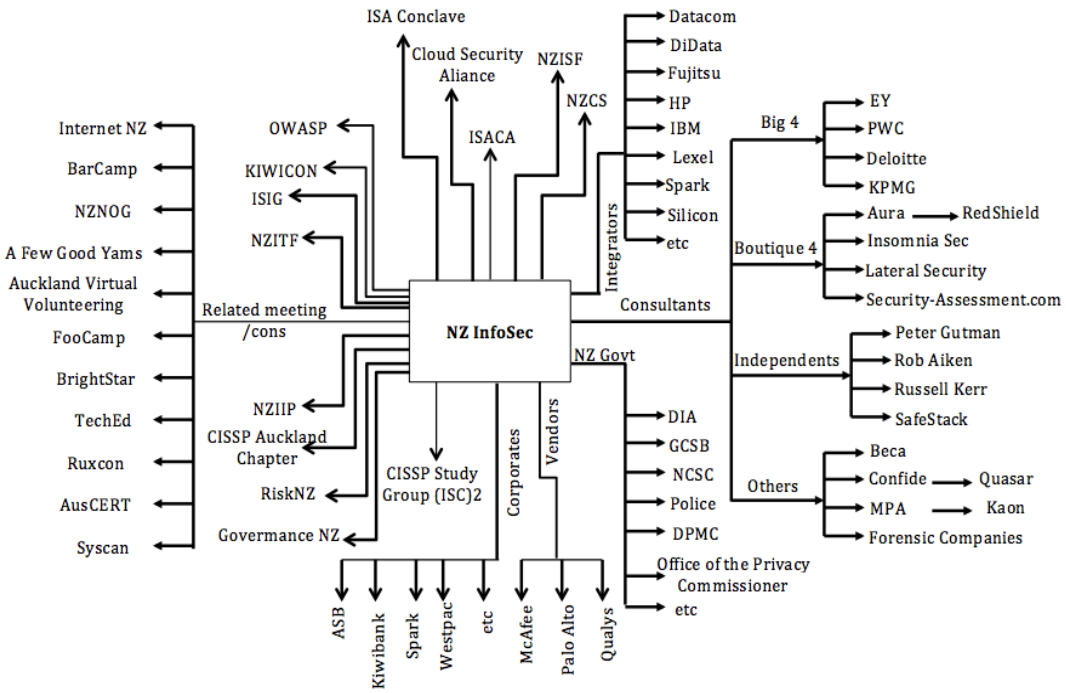

Figure 1. List of New Zealand Information security groups and events

Source: The information collected from different events and meetings related to the cyber security in New Zealand. More information you can find in Acknowledgements and also Tabel 4.

In February 2011 [9], computer science was added as a formal teaching standard, and as such began to be taught at all secondary schools in NZ.New Zealand secondary schools are generally divided into two categories: primary school level (years 1-8), and secondary school level (years 9-

13). The National Certificate of Educational Achievement (NCEA) is the main qualification for secondary school students between years 11 to 13. It is a flexible certificate and can be achieved through different pathways depending on a combination of standards that students pass [9].Unfortunately, although cyber security is an interesting and relevant topic, it is seldom addressed in current NZ secondary school environments. There are a number of issues which contribute to its absence. Adequate facilities must be prepared, as well as up to date hardware technology [10]. Teachers must be up skilled in this area, and courses must be designed and balanced among the numerous other computer science subjects. As a result, cyber security is only gradually being introduced to younger audiences in NZ secondary schools. The choice of teaching approach and material is critical in these early stages of development, and is primarily governed by two aspects: the age and level of the target students, and the projected growth of cyber technology.

Many educational and private centers are developing programs aimed at highlighting the need to develop cyber security subjects in New Zealand schools with the main focus being on years 11-13 although this is has not happened yet. One of the main centers working to promote cyber security at this level is Unitec Institute of Technology in Auckland. Since 2013, Unitec has run several professional development workshops for secondary school teachers, giving them the opportunity to improve their knowledge and skills in particular areas of IT, including cyber security and cyber space safety. Since 2011, Unitec has also filled skills gaps in various areas by developing a number of programs at all levels of higher education, and have also collaborated with various cyber security centers in Japan (NAIST and NICT) in an effort to form sustainable structures that enable the recognition of young people who possess exceptional talent and interest [4].

Unitec'scyber security program, developed within the Centre for Computational Intelligence for Cyber Security at Unitec, includes the Undergraduate degree pathway in Cyber Security, Graduate Diploma pathway in Cyber Security, Master of Computing - Cyber Security Endorsement, Doctor of Computing (professional doctorate), and the dual doctorate–offered by Nara Institute of Science and Technology (Japan) and Unitec [4]. In 2015 they also offered New Zealand's first cyber security CTF competition exclusively for secondary school students at years 11-13, in order to raise awareness of cyber security issues within youth in NZ. Material and concepts that were addressed in this competition included general creative thinking problems, ethical web hacking, network forensics, encoding and cryptography (see Figure 2).

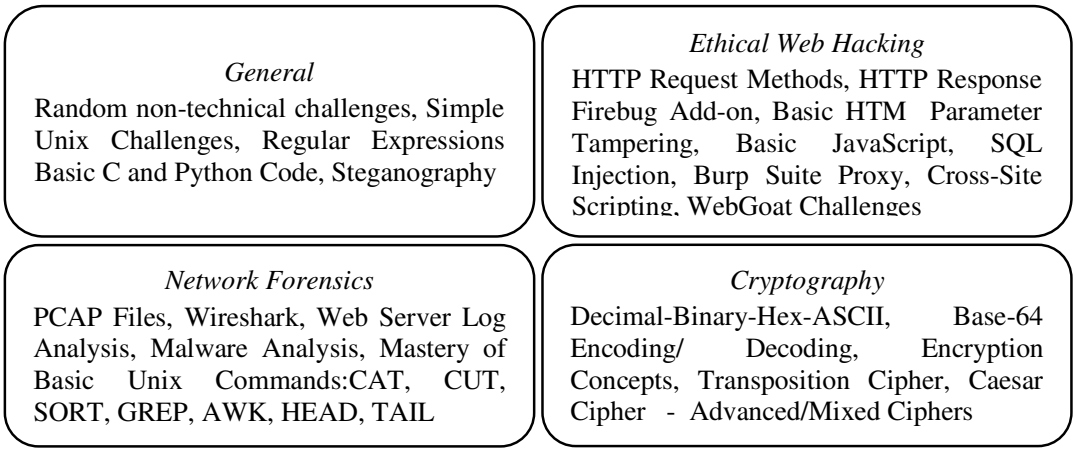

Figure 2.Infographic of concepts covered in Unitec's 2015 Cyber Security Competition

2.2. Existing Cyber Security Competitions for Secondary School Students

In recent years, cyber security competitions have become an increasingly significant topic in the field of computing, since they cater well to the practical nature of cyber security problems. The following table (see Table 1) lists three cyber security competitions held in New Zealand, the US and UK for secondary school students.

Table1. Cyber Security Competitions for Secondary School Student

#	*Competition Name*	*Organiser*	*Age Group*	*Date*	*Frequency*
1	Cyber Security Competition - CTF	Unitec Institute of Technology, New Zealand	Secondary School Students (Year 11-13)	12th-13th Sep. 2015	Annual
2	Cyber Security Awareness Week (CSAW)- CTF	New York University, USA	Secondary School Students	12th-14th Nov. 2015	Annual
3	Cyber Security Challenge Schools Programme	Cyber Security Challenge UK	Primary and Secondary School Students	13th-15th Nov. 2015	Annual

2.2.1. Cyber Security Competition - Unitec Institute of Technology, New Zealand[(1)]

After establishing the first cyber security research centre in New Zealand in 2012, Unitec Institute of Technology has since gone on to develop courses in cyber security at Bachelors, Masters, and Doctoral degree level, as well as forging strong research partnerships with top research institutes overseas. Unitec has been successful in encouraging high school students to realize the significant demand in cyber security and the growing need for skilled cyber security graduates. Unitec's 'Capture the Flag' Competition is an opportunity for high school students to participate in a competition that involves solving real-world problems in cyber security by hacking, identifying patterns, and employing creative and critical thinking processes. It is the first competition of this sort as it goes beyond programming (which most other competitions focus on) and was the first competition focussed solely on secondary school students.

2.2.2. Cyber Security Awareness Week (CSAW) - New York University, USA[(2)]

The NYU School of Engineering has been a pioneer in developing cyber security programs, launching its Master degree in cyber security in 1999, and offering numerous cyber security courses and extracurricular opportunities for undergraduates.
Cyber Security Awareness Week (CSAW) is supported by the NYU School of Engineering's Information Systems and Internet Security Laboratory, The lab is a student run environment with advice provided by hackers-in-residence and industry partners. The school's Enterprise Learning Unit, New York Information Security Meetup, and Peerlyst also provide support.

2.2.3. Cyber Security Challenge Schools Programme–UK Cyber Security Challenge[(3)]

Launched in 2010, the Cyber Security Challenge UK runs a national programme of competitions designed to attract and inspire that untapped talent into the cyber security profession. Backed by over 50 organisations from government, industry and academia, the challenge sets competitions

(1) Further information at: http://cybersecuritycompetition.unitec.ac.nz/
(2) Further information at: https://csaw.engineering.nyu.edu/
(3) Further information at: http://cybersecuritychallenge.org.uk/education/schools/

that test existing cyber security skills, runs cyber camps to help people develop new skills, and provides information through networking events and its website to offer guidance on career opportunities.

3. UNITEC'S CYBER SECURITY COMPETITION 2015 – CAPTURE THE FLAG

The significant and rapid growth in the utilization of the internet creates possibilities for cyber criminals to hack and hijack information and data for financial profit and other illicit activity on the black market. Cybercrime - malware and network intrusion, financial crime, and abuse – is currently one of the fastest growing areas of crime, and one of the leading issues in cyberspace.

In September of 2015, Unitec's Department of Computing organized and ran the first cyber security competition in New Zealand that was targeted exclusively at secondary school students. The primary goal of this competition is to promote interest in, and educate secondary students about practical computer security. The competition was structured around defending and attacking a web application server, with the target system consisting of a Linux, Apache, MySQL, and PHP software stack.

3.1. Workshop in April 2015

In order to help prepare potential participants, and to aid in promoting the competition, the Department of Computing opened a public call and invited all secondary school students to an informal meeting in April2015. An overview of the competition was presented, with the format of the CTF challenge, eligibility rules for participants, and the prizes for each winner.

These activities were of particular value to students who were planning to participate in the competition, and also those who were considering computer security as a career path for the future. Three specific topics were focused on in the workshop: ethical web hacking, network forensics, and encoding and cryptography. Various activities including ethical web hacking were provide. With network forensics, students were introduced to Wire Shark, basic log analysis commands in Unix, web server log analysis, and PCAP files. The encoding and cryptography part of the workshop explored basic concepts in encoding, encryption binary encoding examples, and encryption cipher examples.

3.2. Topics Coveredin Unitec's Cyber Security Competition

The four subsections below elaborate on the cyber security related topics which were covered in Unitec's Cyber Security Competition. Note that the enumeration below is not exhaustive. It should rather be seen as a set of recommendations for cyber security competitions, and suggests a general direction for the future of secondary school CTF competitions in New Zealand.

3.2.1. General Topics in Cyber Security

The use of competitions to practical cyber security concepts is recognised as an effective educational means. However the design, implementation, and execution of a complex, large-scale education system requires a substantial amount of effort. In cyber security courses, students examine the fundamental vulnerabilities of various operating systems and software in personal computers, and how to fix them. In addition to becoming familiar with firewalls and related concepts they also learn and gain practical experience with worms and viruses, and how to detect and remove them.

Unitec Institute of Technology has created a course which provides a basic overview of cyber security management in a corporate setting. Students examine introductory topics such as assurance principles, risk management issues, and organizational plans, along with the various types of security tools available.

To facilitate the growth of the cyber security profession, Unitec Institute of Technology is dedicated to introducing the cyber security material to secondary school students in NZ, especially those who are interested in cyber security and computer subjects. From there, secondary school students who are already interested in the field will have the opportunity to further develop their cyber-skills, and learn about how they can practically apply these abilities in the field. Through Unitec's cyber security competition and the related workshop, students at different interest and knowledge levels have direct experience to uniquely learn about cyber security from a variety of perspectives. With this early understanding of the field, Unitecis offering cyber security material as a part of computer science courses for secondary school students in New Zealand.

3.2.2. Ethical Web Hacking

Ethical web hacking is the process of evaluating the security of a computer system by simulating an attack by a malicious hacker. There are significant job opportunities for ethical hackers as companies become increasingly aware of security risks.

Ethical web hacking has the potential to be a useful computer science subject for secondary school students, as it enables them to use their existing knowledge of programming, databases, networks and web development, and to teaches them to think like a hacker. Such experience would provide them with a deep understanding of security issues, and could lead to excellent employment opportunities in the future. With this subject being taught in such a way, students would benefit from an active teaching group with a growing reputation, based on industry links and knowledge transfer projects, delivered in a project based, entrepreneurial culture, and thus provide them with a deep understanding of security issues and concerns.

Unitec is the only institute in New Zealand that offers different levels of cyber security in its programs, and the graduate students from this institute are passionate about their subject area and developing their knowledge. They aim to present a useful structure for New Zealand secondary school students in order to develop the mindset of a hacker, and are determined to make a contribution to improving security in the world of computing. This is the primary reason for their initiative in running their CTF competition for secondary school students, and focusing on important material such as HTTP request methods, HTTP response, Firefox Firebug add-on, basic HTML, SQL injection, basic JavaScript, Burp Suite proxy, parameter tampering, WebGoat challenges, and Cross-site scripting in an ethical web hacking environment.

3.2.3. Network Forensics

Network forensics is a topic that falls under digital forensics. It deals with the capture, recording, and analysis of network events in order to discover the source of security attacks, legal evidence, or other problem incidents [11]. Analysis of network traffic may include tasks reassembling of files, searching for keywords, and parsing such things as emails or chat sessions [12, 13].

We suggest inclusion of topics such as network intrusion detection/prevention systems, wireless traffic analysis, web server log analysis, malware analysis, network tunnelling, and a mastery of basic Unix commands such as CAT, CUT, SORT, GREP, AWK, HEAD, and TAIL, for filtering out information from log files, specifically web server logs in the curriculum. They strongly

suggest adding this topic as a formal option within computer science courses for secondary school students in New Zealand, since they believe that a mastery of network forensics will teach secondary school students how to follow attackers' footprints and analyse evidence from a network environment.

3.2.4. Cryptography

Transmitting messages is an important practical problem. Cryptography ensures that messages are unreadable to anyone other than the intended recipient. Cryptography is basically writing in secret code. In data and telecommunications, cryptography has specific security requirements, such as authentication, privacy or confidentiality, message integrity, and non-repudiation of information. There are two basic types of ciphers used: the symmetric key cipher, which uses the same key for the same message, and the asymmetric key cipher, which uses different keys for encoding and decoding the same message. Cryptography is another topic suggested by Unitec for inclusion within computer science courses in New Zealand secondary schools. They have formed useful framework to teach this topic in, and cover the basics of information theory so that students can have an overview of message encoding before addressing various classical ciphers. They also plan to create the following sub-topics in order to properly introduce secondary school students to cryptography:

Unit 1: Introduction into Cryptography
Unit 2: Classical Cryptography
Unit 3: Block Ciphers
Unit 4: Hash Functions
Unit 5: The RSA Cryptosystem and Factoring Integers
Unit 6: Elliptic Curve Cryptography
Unit 7: Digital Signature and Entity Authentication

This course explains the inner workings of cryptographic primitives, and how to correctly use them. Students will learn how to reason about the security of cryptographic constructions and how to apply this knowledge to real-world applications. The course begins with a detailed discussion of how two parties who have a shared secret key can communicate securely when a powerful adversary eavesdrops and tampers with traffic. We will examine many deployed protocols and analyze mistakes in existing systems. It's also discusses public-key techniques that let two or more parties generate a shared secret key. Throughout the course students will be exposed to many exciting open problems in the field.

4. DATA ANALYSIS

During the competition, students were presented with a survey letter, which is containing four main questions related to the lessons presented in the cyber security workshop and live competition. These questions were asked before and after the competition activity to determine whether there had been a change in the secondary school student's knowledge and response. The results showed a definite positive trend which confirmed that the learners had gained knowledge relevant to fundamentals of cyber security. The results showed a definite positive trend which confirmed that the participants had gained knowledge relevant to cyber security concepts (see Table 2).

Table 2. Aggregated learner survey results

#	Question	Knowledge before running the competition (%)				Knowledge after running the competition (%)			
		Low	*Fair*	*High*	*Very High*	*Low*	*Fair*	*High*	*Very High*
1	General information about Cyber security	40	20	33.33	6.67	0	33.33	60	6.67
2	Ethical Web Hacking	46.66	26.66	13.33	13.33	0	40	40	20
3	Network Forensics	60	33.33	6.66	0	13.33	60	26.66	0
4	Cryptography	33.33	40	20	6.67	6.66	20	60	13.34

The survey questions were intended to determine whether the students believed the cyber security competition to be an effective teaching tool, and whether they believed they were more knowledgeable of the topics covered in the competition after it was complete(see Figure 3).

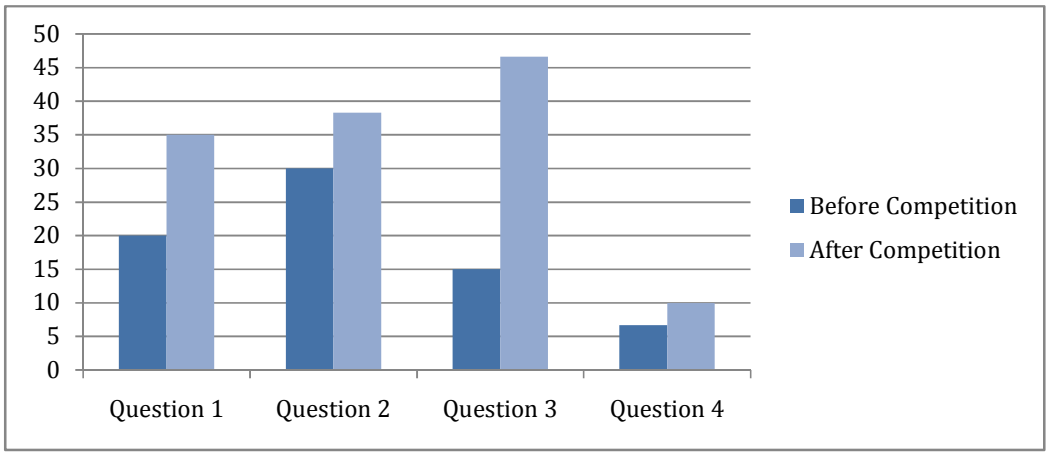

Figure 3. The result of survey questions

The survey also asked three questions regarding the overall level of computer science taught in participants' schools, and their evaluation of the depth of their teachers' knowledge of computer science as a subject (see Table 3).Further research with a larger sample size should be undertaken to further improve the accuracy of the results.

Table 3. Overall view of survey results

#	Question	Owerall view (%)				
		Very Low	Low	Fair	High	Very High
1	How satisfied are you overall with the level of computer science taught in your school?	0	20	46.66	20	13.34
2	At your school, how confident are you in your teacher's knowledge of computer science?	0	0	33.33	40	26.67
3	How important do you think it is to have cyber security taught in secondary schools?	0	0	33.34	33.33	33.33

Survey results suggested that the learners had undergone small behavior changes that indicated an increased awareness of the issues. Finally, the students all concluded that they believed competitions to be an effective education tool for addressing the subject of cyber security.

5. CONCLUSION AND FUTURE WORK

Computer science education is necessary for our educational system, especially considering the increase in digital activity by today's youth. New Zealand is among those countries which have taken steps in introducing computer science courses to the secondary school educational system [14, 15]. The current design of computer science courses requires certain changes regarding the structure of material considering two main issues. Firstly, computer science as a subject was introduced over a very short time span from planning to implementation in New Zealand's educational system. The New Zealand government's educational department was quick to implement the subject and begin having it delivered in secondary schools. Unfortunately this did not give sufficient time to prepare hardware equipment or ensure that teachers were adequately equipped and prepared to address the new standards. The second issue necessitating change is the fact that IT technology has been growing fast in the past decade, and continues to change at an ever-increasing rate. Courses must be constantly assessed and updated to reflect emerging technology and digital advance within cyber space.

This case study has shown how current computer science courses would be enhanced by adding cyber security as a subject, and also how live competitions in cyber security are able to support secondary school students to better understand the concepts of this topic. The Unitec CTF competition was a great learning experience both for the students involved and for the organizers. We believe that this exercise helped the secondary school students understand the intricacies of practical computer security, highlighted their strengths and weaknesses in computer security skills and generally increased their interest and desire to learn more about this area. It is therefore the conclusion of these authors that cyber security as a subject, including the four main areas discussed (fundamentals of cyber security, ethical web hacking, network forensics, and cryptography),is a viable option for the education of the future generation, specifically secondary school students.

We intend to recommend cyber security subjects to the New Zealand Ministry of Education, and also continue this competition by encouraging creation of reading groups focused on practical computer security, and by running similar CTF competitions in upcoming years, incorporating the feedback from this year's participants.

ACKNOWLEDGEMENTS

This research is outcome of a research collaboration opportunity funded by Unitec's Department of Computing, and also Research and Enterprise Office of Unitec Institute of Technology. The authors would like to thank all supportive Unitec Cyber Security Capture The Flag (CTF) 2015 Competition team members, especially Dr.HinneHettema, and MostafaBiglari-Abhari. Moreover, the first author would like to thank Dean Carter (Technical Director-Information Security, Beca, New Zealand) for his great information about Cyber Security organizer, and related events in New Zealand.

REFERENCES

[1]. Lance J. Hoffman, Daniel Ragsdale (2004). Exploring a National Cyber Security Exercise for Colleges and Universities.The George Washington University Cyber Security and Policy Research Institute (Report No. CSPRI-2004-08) and United States Military Academy Information Technology and Operations Center (Report No. ITOC-TR-04001), August 24.

[2]. Bishop, M. (1997). The state of INFOSEC education in academic: Present and Future Direction. In proceedings of National Colloquium on Information System Security Education, page 19-33. Keynote address, Linthicum, MD.

[3]. Bishop, M. (1999). What Do We Mean By "Computer Security Education"?.In Proceedings of the 22nd National Information Systems Security Conference, Arlington, VA.

[4]. Leon Fourie, AbdolhosseinSarrafzadeh, Shaoning Pang, Tamsin Kingston, HinneHettema, Paul Watters (2014).The Global Cyber Security Workforce - An Ongoing Human Capital Crisis. Global Business and Technology Association Managing In AnInterconnectedWorld: Pioneering Business and Technology Excellence, ISBN: 1-932917-10-1.

[5]. Atkinson, S., Furnell, S., Phippen, A. (2009). Securing the next generation: enhancing esafety awareness among young people. Computer Fraud & Security.

[6]. NZ Government.New Zealand's Cyber Security Strategy (2011). Retrieved from: http://www.dpmc.govt.nz/sites/all/files/publications/nz-cyber-security-strategy-june-2011_0.pdf

[7]. The UK Cyber Security Strategy-Protecting and promoting the UK in a digital world (2011).

[8]. White House: The National Strategy to Secure Cyberspace (2003).

[9]. Tim Bell, Peter Andreae, Anthony Robins (2012).Computer Science in NZ High Schools: The First Year ofthe New Standards. SIGCSE'12,Raleigh, North Carolina, USA, February 29 - March 3.

[10]. Fitzpatrick, A. (2012).Cyber security experts needed to meet growing demand, The Washington Post. Retrieved from: http://www.washingtonpost.com/business/economy/cybersecurity-experts-needed-to-meetgrowing-demand/2012/05/29/gJQAtev1yU_story.htm

[11]. Gary Palmer (2001). A Road Map for Digital Forensic Research, Report from DFRWS 2001, First Digital Forensic Research Workshop, Utica, New York, Page(s) 27–30, August 7-8.

[12]. Erik Hjelmvik, Passive Network Security Analysis with NetworkMiner. Retrieved from: http://www.forensicfocus.com/passive-network-security-analysis-networkminer

[13]. SimsonGarfinkel, Network Forensics: Tapping the Internet (2002). http://www.oreillynet.com/pub/a/network/2002/04/26/nettap.html

[14]. Bell, T., Duncan, C., Jarman, S. and Newton, H. (2014).Presenting Computer Science Concepts to High School Students.Olympiads in Informatics Journal 8: 3-19.

[15]. Bell, T., Andreae, P. and Robins, A (2004).A case study of the Introduction of Computer Science in NZ schools. ACM Transactions on Computing Education (TOCE) 14(2): 10:1-10:31.

Table 4. The list of acronyms and abbreviations for Figure 1

#	Acronym	Definition of acronym	#	Acronym	Definition of acronym
1	NZ InfoSec	New Zealand Information Security	14	NZISF	New Zealand Information Security Forum
2	Govermence NZ	Govermence New Zealand	15	NZCS	New Zealand Computer Society
3	NZNOG	New Zealand Network Operators Group	16	NZ Govt	New Zealand Government
4	TechEd	Technology Education	17	Datacom	Data Communications
5	Syscan	Symposium on Security for Asia Network	18	Insomnia Sec	Insomnia Security
6	AusCERT	Australian Computer Emergency Response Team	19	NZ Gov DIA	New Zealand Government Department of Internal Affairs
7	OWASP	Open Web Application Security Project	20	NZ GCSB	New Zealand Government Communications Security Bureau

8	CISSP	Certified Information Systems Security Professional	21	NZ Gov NCSC	New Zealand Government National Cyber Security Centre
9	ISIG	Information Security Interest Group	22	NZ Gov Police	New Zealand Government Police
10	NZITF	New Zeland Investment Trust	23	NZ Gov DPMC	New Zealand Government Department of the Prime Minister and Cabinet
11	NZIIP	New Zealand Institute of Intelligence Professionals	24	ISA Conclave	Internet Security and Acceleration Conclave
12	RiskNZ	Risk New Zealand	25	ISACA	Information Systems Audit and Control Association
13	Internet NZ	Internet New Zealand	26	KiwiCon	KiwiConference