The Role of Cyber-Security in Information Technology Education

Dale C. Rowe Ph.D.
Brigham Young University
Information Technology Program
Provo, Utah
+1 (801) 422 6051
dale_rowe@byu.edu

Barry M. Lunt Ph.D.
Brigham Young University
Information Technology Program
Provo, Utah
+1 (801) 422 2264
luntb@byu.edu

Joseph J. Ekstrom Ph.D.
Brigham Young University
Information Technology Program
Provo, Utah
+1 (801) 422 1839
jekstrom@byu.edu

ABSTRACT
Recent reports indicate a shortage of approximately 20,000-30,000 qualified cyber-security specialists in the US Public Sector alone despite being one of the best financially compensated technology-related domains. Against ever evolving cyber-threats the need to graduate students skilled in the concepts and technologies of cyber-security is becoming a critical responsibility of academic institutions in order to help preserve the sovereignty of the US and her allies. This paper discusses the role of cyber-security in an IT education context and explains why IT programs should champion this topic. The relationship between Information Assurance and Security as a currently recognized discipline within IT and advanced cyber-security topics are presented. Recommendations for the placement and structure of a cyber-security emphasis within a curriculum are presented using an adaptable framework that we have named "Prepare, Defend, Act." We rationalize and discuss this framework along with teaching methods we have found to be effective in helping students maximize their cyber-security learning experience. Finally, four recommendations are proposed that we invite IT program-offering institutions to review.

Categories and Subject Descriptors
K.3.0 [Computers and Education]: General

General Terms
Security; Standardization

Keywords
Information Technology; Model Curriculum; Cyber Security; Information Assurance and Security

1. INTRODUCTION
Is cyber-security real and what is its role within Information Technology? What differences and relationships exist between Information Assurance and Security and cyber-security? These are questions that have recently been the topic of some research and analysis within Brigham Young University's IT Program.

The IT 2008 Model Curriculum [1] recognizes Information Assurance and Security as a key element of IT education with space both in the core and in the advanced curriculum. Within the pillars of IT education, it is placed appropriately across the top of the five topical pillars and described as a binding thread. Indeed, this is the approach desired by many academics to ensure that an awareness of the need for security is instilled in students in all major courses. In addition to being a self-contained principal subject, the IT 2008 Body of Knowledge includes security as a subtopic of Networking, Social and Professional Issues and Web Systems and Technologies. This pervasive cross-course instruction is part of the core education offered within Information Technology with more advanced topics and techniques recommended as advanced level material. Specifically, the model curriculum recommends that more advanced IAS material be covered in the fourth year as an integrative experience to bind the elements taught within each pillar.

Many government bodies have been long-time advocates of cyber-security and have recently devoted significant efforts and resources to strengthening their nations' cyber-posture. As a leader in this domain, the US recently announced their intention to categorize cyber-attacks as acts of war [2]; at the same time, the UK announced a new $1 billion (USD) initiative to develop advanced militarized cyber-security abilities [3]. These announcements follow a series of new cyber-security bills introduced in congress in May 2011 and accompany a 60 day 'Cyberspace Policy Review' [4, 5] which calls for increased collaboration between government, private sector and academia. Some may question why cyber-security has suddenly become such a hot discussion topic, while others may ask why have we waited so long? [6]

2. WHAT IS CYBER-SECURITY?
Despite the recent increase of public media coverage, cyber-security is not new and has been the subject of serious discussion in government, industry and academics for almost two decades. This said, there are some variations in the definition and scope of cyber-security that have been the cause of contention between authors.

Some experts claim the topic is over-hyped and artificially inflated by fear mongering, with terms such as 'cyber-warfare' designed to provoke an emotional rather than a rational response [7]. In a recent study by Intelligence^2 (Intelligence-squared), as many as 23 percent of professionals indicated that they believed

SIGITE'11, October 20–22, 2011, West Point, New York, USA.

the threat of cyber-war has been grossly exaggerated [8]. Concerns about civil liberty and electronic privacy erosion may indeed be valid [9, 10] however in the context of an academic learning environment, these are key concepts and discussion topics that can encourage independent thinking and research among students. Indeed, this type of discussion is proposed by many of those calling for caution such as security expert Bruce Schneier [11-15], who points out that many cybercrimes are the direct result of poor security rather than insufficient government powers of attribution. Likewise, president of the Electronic Privacy Information Center (EPIC) Marc Rotenberg argued against mandatory Internet identification requirements. He pointed out that in countries such as China, attribution requirements have resulted in censorship and international human rights violations [16]. Regardless of which view one may take, it is obvious that cyber-security is recognized as a very real topic and one worthy of discussion [17].

While this paper does not seek to establish a standardized definition of cyber-security for global acceptance, it does suggest some key elements for curricular inclusion in Information Technology programs. These are based on a variety of documents and reports many of which reside in the public sector. With the frequency of cyber-attacks on a constant rise, governments worldwide are taking proactive and preemptive action to reduce the risk of successful attacks against critical infrastructures. It is this connection between the physical and cyber domains that is of such concern. Indeed, recently a volunteer effort organized by the Cyber-security Forum Initiative reported on this effect and causality between real and cyber events in the current Libya conflict [18]. The relationship between military strikes on civilians and government-organized Internet blackouts was prevalent with actions in the physical world being preceded by cyber-events.

Many IT Professionals may be aware of recent events surrounding Supervisor Control and Data Acquisition (SCADA) systems following the STUXNET virus [19], yet almost two years after its first recognized appearance in 2009 there are still significant vulnerabilities. At the time of writing this paper (May 2011), independent security researchers Brian Meixell and Dillon Beresford along with NSS Labs canceled their Takedown 2011 Conference presentation "Hacking SCADA". The presentation was to show how to write "industrial-grade" SCADA malware using both inadequately patched vulnerabilities and new vulnerabilities. The presentation was voluntarily cancelled by the Meixell and Beresford due to "the serious physical, financial impact these issues could have on a worldwide basis" [20] and "negative impact to human life" [21]. The lack of security in these systems is particularly alarming given there is documented research of vulnerabilities dating back as far as 1999 [22-24].

Fortunately not all cyber-events are connected to human loss of life yet the economic impact to a society can still be hugely damaging. In the 2010 Fraud Report by Kroll [25], it was reported that information and electronic data theft surpassed all other fraud for the first time rising 9.3 percent from the previous year. This is in spite of a reduction in half of other fraud categories.

In 2006, the National Science and Technology Council released the Federal Plan for cyber-security and Information Assurance Research and Development [26]. The report identifies IT infrastructure supporting critical systems including power grids, emergency communications systems, financial systems and air-traffic control networks. Although many of these systems are owned by the private sector they represent critical homeland and economic interests and the government has a vested interest in their stability and security. The report's findings lead to ten recommendations for future cyber-security research and development.

In 2008, National Security Presidential Directive 54/Homeland Security Presidential Directive 23 [27, 28] was issued, formalizing the Comprehensive National Cyber-security Initiative (CNCI) [29]. The CNCI is the first in a series of stages to establish a broader, updated national U.S. cyber-security strategy with the following summarized goals: To (1) establish a front line of defense against today's immediate (cyber) threats, (2) defend against the full spectrum of threats and (3) strengthen the future cyber-security environment. These goals also underline the CNCI's initiatives.

Cyber-security is a challenge that extends beyond national boundaries and requires global cooperation with no single group, country or agency claiming ownership, according to a 2009 report by the US Department of Homeland Security [30]. The report proposes a Roadmap for Cyber-security Research. Building on the 2005 second revision of the INFOSEC Research Council (IRC) Hard Problem List [31], and in recognition of the aforementioned presidential directives [27, 28], the roadmap identifies research and development opportunities that are scoped to address eleven "hard problems". The list was established following a significant research effort and took 15 months to develop, with multiple 'real' and virtual workshops alongside online collaboration from a team of subject matter experts.

A recent Organization for Economic Co-operation and Development (OECD) report by two UK Professors discusses the relationship between cyber and physical warfare, claiming that although cyberspace is a war fighting domain, there is little prospect of a war being carried out solely in cyberspace [32]. They do however acknowledge that there are a few cyber-events with the capability to cause a global shock and many more that could create localized misery and loss. Their list of findings and recommendations is too exhaustive to cover in its entirety but focuses on risks from a multi-pronged attack using a variety of technological and social methods to achieve a mal-intentioned objective, such as cyber-espionage. Recently these attacks have become known as Advanced Persistent Threats or APTs [33].

The International Standards Organization are currently reviewing the final committee draft of ISO/IEC 27032: Guidelines for Cyber-security [34]. This defines cyber-security as the "preservation of confidentiality, integrity and availability of information in the cyberspace", with an accompanying definition of cyberspace as "the complex environment resulting from the interaction of people, software and services on the Internet by means of technology devices and networks connected to it, which does not exist in any physical form".

It is clear then, that cyber-security is an area of much debate, interest and attention. If there is any dispute about the importance of this as an academic training curriculum, one should consult recent reports indicating a dramatic (and growing) deficit of qualified professionals in the public sector [35-37]. Even given the importance of thorough Information Assurance and Security education throughout the Information Technology Model Curriculum [1], we suggest that a wider-reaching emphasis in cyber-security with advanced topics would add value to many existing IT Programs.

3. WHY INFORMATION TECHNOLOGY?

It is without question that all computing and technology programs have a responsibility to ensure a thorough and pervasive security curriculum within their courses. To do otherwise would not only disadvantage students, but has the potential to be dangerous in training students with advanced technical skills but lacking security awareness – such an omission would almost certainly result in systems designed or produced by graduates containing huge security vulnerabilities.

Yet we believe Information Technology programs are uniquely best-suited to an advanced cyber-security curriculum. Earlier we referred to the five pillars of an IT Curriculum as programming, networking, human computer interaction, databases and web systems.

These five pillars are each critical pre-requisites for cyber-security. Justification for this is provided below.

3.1 Programming

The ability to program a computer system to achieve a desired outcome is perhaps the most fundamental skill taught in an IT program and in all computing programs. Yet it is here that the potential for unintentionally crafting exploitable vulnerabilities lies. Programming security vulnerabilities are a common cause of computing security breaches. Even the best programmers can make mistakes, and a simple oversight can have far-reaching effects. Likewise it is in programming that the ability to rectify these vulnerabilities lies.

At the very least, conceptual programming knowledge is an essential cyber-security tool to understand how and why a software vulnerability may be exploited and begin to realize the impact of a successful attack.

3.2 Networking

The need for practical networking knowledge in cyber-security is obvious. "Cyberspace" is defined as a networked group of entities. Understanding the concepts, technicalities, protocols and vulnerabilities of computer networks are key pre-requisites of an advanced cyber-security education.

3.3 Human Computer Interaction (HCI)

In the context of cyber-security, HCI represents a huge "piece of the pie". Although declining, reports indicate that user error is the primary cause of security breaches [38]. Is this a result of poor user interface design or poor user education? In fact, both are likely to play a significant part. Information Technology professionals are described as user advocates [1] and effectively provide a human interface between technology and users. It is their responsibility to ensure the users can efficiently, securely and effectively realize their goals through the appropriate use of computer technology.

User education takes a significant role in user advocacy. Through proper training, users can be taught to recognize and avoid common security pitfalls such as phishing attacks, social engineering, malware and insecure browsing [39]. The benefit of these approaches has already been shown and as of 2009, user error is no longer the primary cause of security breaches [40, 41].

3.4 Databases

Databases are often primary targets in cyber-attacks. They represent a rich resource of information that is often commercially sensitive, contains sensitive user data, or both. While other computing programs may emphasize advanced database structure and design methods, Information Technology includes significant Database Management Systems (DBMS), and Database Administration (DBAdmin) content.

Although these are intended to help students be better able to integrate and manage systems from a theoretical and practical standpoint, the understanding of how a database management system functions and is administered are key skills in protecting information from cyber-theft or sabotage.

3.5 Web Systems

Web systems provide the external interface to many different types of computer systems. A website is typically the first publically accessible boundary that an attacker will communicate with in cyberspace. Websites are designed for a variety of purposes and often present a viable attack vector to an organizations internal network

A particularly prevalent and dangerous threat today is cross-site scripting (XSS). XSS is the placement of malicious code on an attacker-controlled website which exploits vulnerabilities in a legitimate and typically high-traffic website in order to inject client-side code (this is one method of drive-by infection – the infection of a victim's system without their knowledge or consent by using a client-side browser vulnerability). The danger of this type of infection is dependent on the nature of the malicious code and can vary from privacy invasions and information theft, to full remote control of a victim's system by the attacker. This is listed in the 2010 SANS Top 25 list as the number one most dangerous software error [42, 43].

Given the intentional public placement of websites, great care must be exercised to ensure their security. Vulnerabilities are frequently found by security experts and reported to vendors who produce patches, or security hotfixes. This evolutionary cycle appears to be without end and any organization with a web-presence should have clearly defined policies regarding the adoption and implementation of manufacturer fixes.

The web systems pillar of IT includes a strong security emphasis that discusses additional security topics such as the need for server hardening, firewalls and intrusion detection/prevention systems (IDS/IPS).

3.6 Summary of IT Fit

As shown, the five pillars of IT are well suited to cyber-security education. There already exists a pervasive security element throughout each pillar, which provides students with subject knowledge that is both conceptually and technically applicable within a security context. Additionally these same pillars provide key knowledge cornerstones that are pre-requisite to cyber-security education. This is discussed further in the Section 4.

We do not dispute that cyber-security education has elements residing in other disciplines [44]. In fact this diversity is to be encouraged and wherever possible leveraged into cross-disciplinary collaborative opportunities. The unique perspectives of Computer Science, Computer Engineering, Electronic Engineering, Information Systems, Mathematics and many other fields which share an interest in cyber-security, are able to contribute to making our digital society a safer place.

We do however assert that Information Technology presents a uniquely suited and ideal environment for cyber-security education that sets it apart from other disciplines. Indeed were

one to design a separate discipline specifically for cyber-security, we believe it would closely resemble an Information Technology program with a cyber-security emphasis.

4. A CYBER-SECURITY CURRICULUM

We have presented some definitions of a cyber-security in varying contexts and suitability of IT programs as an appropriate location for this topic. This section now discusses our proposition for an educational curriculum in advanced cyber-security. Continuing from Section 2, we demonstrate that even among the differing opinions and interpretations of cyber-security, it is possible to build a structured curriculum that should be both encompassing and unbiased to these definitions.

The Center for Education and Research in Information Assurance and Security (CERIAS) at Purdue University has published several papers on security education within computing programs and suggests a layered approach [45] to IAS education as: (1) Prerequisite Knowledge, (2) Information Assurance Body of Knowledge, (3) Higher Order Skills and (4) Job/Professional Level.

We propose that an advanced cyber-security curriculum is situated at the third of these layers as a higher order skill and wherever possible exposes students to level 4 as will be discussed in Section 5.

4.1 Outcomes

Establishing goals and outcomes is essential to develop an effective curriculum. These goals may be program specific and tailored to the educational and research objectives of the teaching institution. With this in mind, we will present five high-level outcomes that should be suitably generic to be adapted to most programs.

1. Students will be familiar with the multi-disciplinary and fast-paced nature of cyber-security and be prepared to learn and understand new technologies and contexts throughout their career.

This outcome is based on a paper by Ed Crowley who discusses curriculum development in Information Assurance and Security [44]. He discusses the multidisciplinary nature of IAS including psychology, sociology, law, computer science, engineering and management. In a cyber-security domain, these should also include an appropriate element of mathematics, physics and IT.

2. Students will acquire basic cyber-security skills with an emphasis on a professional path.

This outcome is adapted from a 1998 NCISSE presentation by Eugene Stafford at Purdue [46]. It emphasizes the need to align a programs skillset with the profession.

3. Students will understand the need for cross-disciplinary and cross-cultural collaboration in cyber-security and be able to communicate the domain to a variety of technical and non-technical audiences.

We present this outcome as our own objective from Brigham Young University's IT: Cyber-security emphasis outcomes. The need for students to be able to cross both cultural and academic divides to improve systems security and educate users is of paramount importance.

4. Students will be able to apply their knowledge of systems integration in lateral or 'out the box' thinking when working with cyber-security threats, attacks, incident response and defenses.

A further outcome from BYU's IT program, this emphasizes the need for cyber-security professionals to be able to think outside the box in order to "connect the dots". Being able to think as a potential attacker, relate to a cyber-victim and comprehend the bigger picture are important skills in cyber-security. For example, in an advanced persistent threat scenario, a cyber-security professional should be able to understand and correlate all attack vectors and use these in a form of root-cause analysis to determine the attack objectives, begin to derive attribution and implement an incident response plan that both minimizes service interruption and leads to future increased defensive abilities against attack.

One of the popular elements of BYU's Information Assurance and Security course introduction is where students are shown a short video (origin unknown) which depicts two government employees calling for help during an escalator failure [47]. The anecdotal clip serves as a visual reminder of our tendency to be obscured by our day-to-day routine and the importance of being aware of our surroundings that preempts lateral thinking.

5. Students will understand the ethical responsibilities of the cyber-security profession and will treat ethical, moral and privacy issues responsibly and with sensitivity.

As a final outcome from our emphasis, we underline the importance of cyber-security professionals being of high moral character. Other authors also highlight the importance of moral and ethical instruction in security related topics. [48, 49]

These five outcomes should not be seen as all-inclusive. They are merely provided to assist those responsible for course development as seed ideas in developing cyber-security program content.

4.2 Security Across The Curriculum?

Many academics have stated the need for security-across-the-curriculum in IT programs [48, 50-53]. The proposal of a cyber-security emphasis should not be seen as countering this research and we caution strongly against removing security content from IT topics in order to move it to defined cyber-security courses. The benefits of security across the curriculum have been proven in its implementation [53, 54]. However we feel there is still significant advanced content that would benefit undergraduates and help reduce the cyber-security professional deficit [35-37].

Some researchers assert that security topics are in fact drawn from a wide range of academic domains rather than being a separate study [55]. While it is true that cyber-security does indeed draw together various academic disciplines, this does not imply that it has no internal cohesiveness or innovative content. In fact as we illustrate, there are some topics that are simply not found in any other discipline. We believe that this is in part a contributory factor to the current lack of qualified professionals.

The Committee on National Security Systems produced in 1994 an educational reference framework listing the body of knowledge for an Information Security Curriculum [56] which unites security content from a variety of domains. Content areas within NSTISSI 4011 include: communications basics, security basics, NSTISS basics, system operating environment, NSTISS planning and management and NSTISS policies and procedures.

Although this provides a good baseline for Information Assurance and Security education, it does not address some cyber-threats currently faced.

We encourage institutions offering Information Technology or closely related topics to consider the inclusion of an advanced cyber-security curriculum that builds upon established foundations laid out in the IT Model Curriculum [1] and National Training Standard for Information Systems Security Infosec (NSTISSI) 4011 [56].

4.3 Topics

In 2003, before the IT Model Curriculum had been established, Ekstrom and Lunt presented a paper that attempted to define IT as an academic discipline that was more than a broad view of existing disciplines. Their research identified a significant area, "systems integration," that was not covered by the computing programs. Systems integration describes eloquently one of the prime focus areas of Information Technology [57].

As an academic discipline, IT has matured over recent years to cover in depth how different component technologies can be integrated to enable users. As the curriculum has been refined [58], this focal area has been maintained, yet there is still room for growth. By its nature the IT discipline is very much alive and connects with a variety of socio-technological fields including bio-informatics, social computing, technology education, technology innovation and cyber-security.

Given the variations in cyber-security standards, reports and documentation, it appears prudent at this stage to avoid adding any further complexity. In our experience, encouraging students to analyze these differences is a useful tool in promoting understanding. Following the principle of Occam's Razor [59], 'plurality should not be posited without necessity', we believe that simplifying cyber-security into a few key terms and their relationships will provide a flexible framework. This level of flexibility helps programs maintain a relatively 'open' academic structure that can cater to the 'shifting sands' [55] problems in cyber-security definitions, standards and frameworks.

We propose that an advanced cyber-security emphasis could be covered within three high-level categories which would follow a common pre-requisite of Information Assurance and Security [1]. These categories are: Prepare, Defend and Act

The initial inclination was to label the latter of these categories 'react' indicating a response to a cyber-incident. On reflection, this seemed inappropriate given the axiom 'it is better to act, than react'. The word react may conjure images of a knee-jerk careless reaction rather than a well-executed plan of action.

Each of these categories can be better contextualized through the following questions:

1. What cyber-threats are there and how can we prepare for, and minimize potential attacks? (Preparing)
2. How to design and maintain secure systems? (Defending)
3. What should be done in the event of a cyber-attack and how can one place attribution? (Acting)

Cyber-security preparation means that risks are understood. This requires a thorough understanding of the threat and its impact. It is important to note that these are not merely technical. A large part of preparation is in understanding the relationship between cyberspace and the real world. The primary technical topics are penetration testing, ethical hacking, and advanced persistent/evasive threats (APT/AET's).

Cyber-defense involves taking preventative measures to protect computer systems and again includes both technical and non-technical elements. We believe that this category is well suited to systems administration. Systems Administrators are responsible for the maintenance of systems and networks and the implementation of security policies. Other appropriate topics include networks and systems design all in a security context. Hardening, auditing, accreditation and user education all fall into the preventative defense category.

The act category is what to do in the event of a cyber attack. What are the signs of an active attack, what steps should be taken to assess potential impact, derive attribution, respond and restore service? Technical topics include digital forensics (live and offline) and incident response. Other areas include cultural and global standardization, legal issues, counter forensics, the theory of computer forensics and incident response, and understanding how different organizations have different methodologies and priorities.

Suggested course names for each category are: Cyber Threats and Penetration Testing, Cyber Defense and Systems Administration and Cyber Response and Forensics.

It may be noted that each topic is coupled with a more technical practice. This pairing intentionally scopes courses to deal with both the concepts of cyber-security as well as a 'practical skills toolbox' suitable for a cyber-security professional.

This relatively high level of topic abstraction should allow course instructors great flexibility in their content and the academic freedom to focus on a specific cyber-security model if desired. At the same time it emphasizes that cyber-security is not a new topic, rather a method of viewing and correlating existing knowledge to holistically analyze, understand, defend against and respond to cyber-threats. (An excellent mid-level summary of cyber-security topics and discussion points is presented in the OECD report 'Reducing Systematic Cyber-security Risk' [32] pp5-8).

Within BYU's IT program, these courses are taught at the senior/graduate level (500). While not all four-year programs offer graduate courses, we would advise that cyber-security courses are taught towards the end of a student's study after the necessary prerequisite material has been learnt.

5. EDUCATIONAL METHODS

Many researchers have provided excellent material on educational approaches for security topics [44, 48-50, 53-55]. We present some supplementary educational methods that have been found useful in our own program and hope that they may assist instructors in their own course design. This list is not exhaustive by any means and may be viewed as a basis for future research.

5.1 Hands-On Exposure

Research has shown hands-on experience to be an effective teaching tool [60]. Although there is a common belief that 'hands-on experience is at the heart of science learning' Nancy Nersessian emphasizes that labs should be explicitly directed towards conceptual instruction [61]. In 2006, Jing Ma and Jeffrey Nickerson reviewed different methods of laboratory instruction and concluded that laboratories can be an effective tool in both conceptual and design education [62].

There is no doubt in our minds that a well-designed lab can be very effective for student learning. Experience has shown that labs that encourage independent thinking and other higher cognitive functions are both effective and enjoyable for students. Cyber-security is a particularly appropriate topic for lab-based instruction as many labs are unscripted and 'open ended' allowing multiple correct solutions. Allowing students to select tools, methodology frameworks and operating systems to achieve a goal encourage student-led research and innovation.

Providing students with a cyber-security emphasis can be likened to military training regimes, according to David Dittrich [63], who goes on to discuss the significance of experience, and issues with rapidly dating technologies. In designing cyber-security labs, care must be taken to ensure that the work is not exclusively connected to a specific technology or piece of software, but focuses on concepts, methodologies and skills that will endure the test of time.

One technique that has shown significant success is that of cyber-security exercises, or cyber war-games. These place students in a competitive environment and allow them to hone their skills to achieve a specified objective. Such exercises are popular among hacking communities and government agencies. Gregory White describes a collegiate version of the exercises [64] which is subsequently held at the national level [65].

5.2 Collaboration

Working with industry and government in a teaching setting allows students to gain a unique insight into current cyber-security threats, trends and needs. Collaborative opportunities can be as simple as inviting cyber-security professionals to present, or more formal arrangements working with local businesses and institutions to expose students to real-world environments. Such collaboration need not be external, as one institution has demonstrated. Following a successful malicious compromise of their computer network, Dartmouth College established a cyber-security initiative in which students worked alongside the campus computing services to improve their security posture [66].

Several authors have also noted the need for information sharing in cyber-security [67, 68]. Through appropriate collaboration, students can gain an appreciation of the need for (and play a role in) community, private sector and government information sharing. The call for this type of collaboration was reciprocated in the recent Cyberspace Policy Review [5] which underlined the need for a variety of collaborative efforts between government, military, the private sector and academia.

Collaborative activities help expose students to professional level activities and can encourage professional certifications and qualifications throughout their future careers [45].

5.3 Case Studies

Case studies provide students and faculty an opportunity to engage in topical discussions of past cyber-security events. Recent events such as the Sony cyber attacks are estimated to have cost in excess of $3.2 billion (USD) [69]. Sony has recently suffered a series of attacks and security failures, the latest of which is the yet unverified claim by the Lulz Security hacker group on June 2, 2011, who claim to have stolen over one million user passwords from Sony Pictures [70].

In addition to studying successful attacks and failures, students should be encouraged to investigate thwarted attack attempts such as the recent Lockheed Martin attacks [71]. Analyzing why an attack succeeded or failed and an organization's approach to cyber-security highlights the importance of security in an organization-wide and global context.

A further area for case studies is in the critical assessment of current practices or approaches to cyber-security and their effectiveness [72]. Such topics are pivotal to the evolution of cyber-security and can help spot weaknesses in habitual behavior and procedures before a major exploitation occurs.

Through case studies, students can gain insight into motives, targets, threats, risk and incident response in the real world as well as an appreciation for the increasing relationship between 'real world' events and events in cyberspace. Students should be encouraged to conduct their own case studies through the course duration. Offering extra course credit for well-written case studies can often be an encouraging factor!

6. RECOMMENDATIONS

Our findings have shown IT to provide an excellent base upon which to build an advanced cyber-security curriculum and highlight the need for cyber-security education. In summary we would like to encourage IT programs to:

- Verify that they include a pervasive up-to-date security element throughout their curriculum.
- Familiarize students with the terminology of cyber-security.
- Evaluate their current advanced content in cyber-security related topics and where possible, teach such content in a cyber-security context.
- Where possible, introduce an advanced cyber-security emphasis based on the Prepare, Defend, Act model.

7. CONCLUSIONS

In this paper we have presented a summary of cyber-security and the current issues in an academic instructional context. The need for cyber-security education and training as a pervasive element in computing and other related programs is recognized as being an excellent method of building awareness in students.

It is clear however, that there are several aspects of cyber-security that are not covered within the standard IT curriculum. We believe that IT programs build an ideal foundational framework that is uniquely well suited to an advanced cyber security emphasis extending beyond the existing pervasive elements. In recognition of the model curriculum pillars of IT education, we encourage IT faculty to carefully analyze their programs security content with a view to increasing their coverage of this much needed topic.

A high level framework for the teaching of cyber-security has been proposed as an emphasis within IT. The elements of the framework have been defined as 'Prepare, Defend, Act'. We are aware of, and recognize the difficulty currently faced with substantial variances in standards, definitions and methods associated with cyber-security. The 'Prepare, Defend, Act' framework allows flexibility for institutions to impartially study these variations, or to align with a specific approach. This framework is currently being introduced within our own IT program as three 500 level graduate courses that are also available as undergraduate electives.

We have also shared methods that have been useful in enhancing our own cyber-security emphasis within BYU's IT Program and hope that this will become a basis for further research on effective methods.

In response to the recent events that have occurred during the preparation of this paper we acknowledge and appreciate the efforts of government [5], various private sector organizations, academia and open source research groups [18] in their efforts to promote a necessary awareness of cyber-security.

8. REFERENCES

[1] Lunt, B. M., Ekstrom, J. J., Gorka, S.*, et al.*, Information Technology 2008: Curriculum Guidelines for Undergraduate Degree Programs in Information Technology. *Association for Computing Machinery (ACM); IEEE Computer Society*, November 2008.

[2] BBC, US Pentagon to treat cyber-attacks as 'acts of war'. *British Broadcasting Corporation*, June 1, 2011. http://www.bbc.co.uk/news/world-us-canada-13614125 (Last Accessed: June 1, 2011).

[3] BBC, UK beefs up cyber warfare plans. *British Broadcasting Corporation*, May 31, 2011. http://www.bbc.co.uk/news/technology-13599916 (Last Accessed: June 1, 2011).

[4] Spacewar.com, White House proposes new cybersecurity bill. *Space War*, May 12, 2011. http://www.spacewar.com/reports/White_House_proposes_new_cybersecurity_bill_999.html (Last Accessed: June 1, 2011).

[5] Whitehouse, Cyberspace Policy Review. *Government Collaborative*, Washington DC, 2011. http://www.whitehouse.gov/assets/documents/Cyberspace_Policy_Review_final.pdf (Last Accessed: June 2, 2011).

[6] Herrera-Flanigan, J., Cyber Attention: Why Now? *Cybersecurity Report*, Nextgov, May 27, 2011. http://cybersecurityreport.nextgov.com/2011/05/cyber_attention_why_now.php (Last Accessed: May 30, 2011).

[7] Singel, R., Cyberwar Hype Intended to Destroy the Open Internet. *Wired*, March 1, 2010. http://www.wired.com/threatlevel/2010/03/cyber-war-hype/ (Last Accessed: May 30, 2011).

[8] Intelligence^2, The Cyber War Threat Has Been Grossly Exaggerated. June 8, 2010. http://intelligencesquaredus.org/index.php/past-debates/cyber-war-threat-has-been-grossly-exaggerated/ (Last Accessed: May 30, 2011).

[9] Mello, J. P., NSA Chief: Cyberwar Rules of Engagement a Policy Minefield. 15 Apr, 2010. http://www.technewsworld.com/story/69780.html?wlc=1279739450&wlc=1306808884 (Last Accessed: May 30, 2011).

[10] Lawson, S., Sow "Cyberwar" Rhetoric, Reap The NSA's "Big Brother". *The Firewall - The World of Security*, Forbes, July 8, 2010. http://blogs.forbes.com/firewall/2010/07/08/sew-cyberwar-rhetoric-reap-the-nsas-big-brother/ (Last Accessed: May 31, 2011).

[11] Schneier, B., Worst-Case Thinking. *Schneier on Security*, May 13, 2010. http://www.schneier.com/blog/archives/2010/05/worst-case_thin.html (Last Accessed: May 30, 2011).

[12] Schneier, B., Cyberwarfare Policy. *Schneier on Security*, 12 Dec, 2009. http://www.schneier.com/blog/archives/2009/12/cyberwarfare_po.html (Last Accessed: May 30, 2011).

[13] Schneier, B., U.S. Enables Chinese Hacking of Google. *CNN*, Jan 23, 2010. http://www.cnn.com/2010/OPINION/01/23/schneier.google.hacking/index.html (Last Accessed: May 30, 2011).

[14] Schneier, B., Crypto-Gram Newsletter: Cyberwar. *Schneier on Security*, 15 Jan, 2005. http://www.schneier.com/crypto-gram-0501.html#10 (Last Accessed: May 30, 2011).

[15] Schneier, B., North Korea Cyberattacks. *Schneier on Security*, July 13, 2009. http://www.schneier.com/blog/archives/2009/07/north_korean_cy.html (Last Accessed: May 30, 2011).

[16] Committee on Science and Technology, Planning for the Future of Cyber Attack Attribution. *U.S. House of Representatives*, Washington DC, 2010. http://epic.org/privacy/cybersecurity/EPIC_HouseSci_Testimony_2010-07-15.pdf (Last Accessed: May 30, 2011).

[17] Crews, C. W., Cybersecurity Theater vs. The Real Thing. *Wayne Crewes*, Forbes, Mar 16, 2011. http://blogs.forbes.com/firewall/2010/07/08/sew-cyberwar-rhetoric-reap-the-nsas-big-brother/ (Last Accessed: May 31, 2011).

[18] Souza, P. d., Rowe, D. C., Ali, A.*, et al.*, Cyber Dawn: Libya. *Cyber Security Forum Initiative (CSFI)*, May 2011.

[19] Falliere, N., Murchu, L. O. and Chien, E., W32.Stuxnet Dossier. *Symantec*, February 2011.

[20] Rashid, F., Siemens, DHS Ask Researcher to Cancel SCADA Vulnerabilities. *eWeek*, May 19, 2011. http://securitywatch.eweek.com/scada/siemens_dhs_ask_researcher_to_cancel_scada_vulnerabilities_talk.html (Last Accessed: May 30, 2011).

[21] Mills, E., SCADA hack talk canceled after U.S., Siemens request. *CNET*, May 18, 2011. http://news.cnet.com/8301-27080_3-20064112-245.html (Last Accessed: May 30, 2011).

[22] Posposil, R., The Next Y2K, *Utilities IT*, 2000.

[23] Naedele, M., Dzung, D. and Stanimirov, M., Network Security for Substation Automation Systems, *Lecture Notes In Computer Science*, Vol 2187, pp 25-34, 2001.

[24] Riptech, Understanding SCADA System Security Vulnerabilities. *Riptech Inc*, 2001.

[25] Kroll, Global Fraud Report. *Kroll Consulting*, USA, Fall 2010.

[26] NSTC, Federal Plan for Cyber Security and Information Assurance Research and Development. *National Science and Technology Council*, Washington DC, 2006. http://www.au.af.mil/au/awc/awcgate/nitrd/fed_plan_csia_rse.pdf (Last Accessed: May 30, 2011).

[27] NSPD-54, Cyber Security and Monitoring. *National Security Presidential Directive* 54, 8 Jan 2008.

[28] HSPD-23, Cyber Security and Monitoring. *Homeland Security Presidential Directive* 23, 8 Jan 2008.

[29] NSC, Comprehensive National Cybersecurity Initiative (CNCI). *National Security Council*, http://www.whitehouse.gov/cybersecurity/comprehensive-national-cybersecurity-initiative (Last Accessed: May 30, 2011).

[30] US-DHS, A Roadmap for Cybersecurity Research. *US Department of Homeland Security*, 2009.

[31] IRC, Hard Problem List. *INFOSEC Research Council (IRC)*, 2005.

[32] Sommer, P. and Brown, I., Reducing Systemic Cybersecurity Risk. *Organization for Economic Co-Operation and Development (OECD)*, 2011.

[33] Sterling, B., The Advanced Persistent Threat Attack. *Wired*, Jan 30, 2010. http://www.wired.com/beyond_the_beyond/2010/01/the-advanced-persistent-threat-attack/ (Last Accessed: May 30, 2011).

[34] ISO, Guidelines for Cybersecurity. *International Standards Organization*. 2011. http://www.iso27001security.com/html/27032.html.

[35] Hoffman, S., Lack of Cybersecurity Talent Could Leave U.S. Vulnerable: Study. *The Channel Wire*, CRN, July 22, 2009. http://www.crn.com/blogs-op-ed/the-channel-wire/218600240/lack-of-cybersecurity-talent-could-leave-u-s-vulnerable-study.htm (Last Accessed: May 30, 2011).

[36] Cacas, M., Feds Say Cybersecurity Staffing Needs to Double by 2015. *Armed Forces Communications and Electronics Association (AFCEA)*, May 11, 2011. http://www.afcea.org/signal/articles/templates/SIGNAL_Article_Template.asp?articleid=2615&zoneid=280 (Last Accessed: May 30, 2011).

[37] Auoub, R., The 2011 $(ISC)^2$ Global Information Security Workforce Study. *$(ISC)^2$*, 2011.

[38] Tucci, L., Fewer Security Breaches Blamed on Human Error. *TechTarget*, Sept 19, 2007. http://searchcio.techtarget.com/news/1273058/Fewer-security-breaches-blamed-on-human-error (Last Accessed: 30 May 2011).

[39] Dark, M., Security Education, Training, and Awareness from a Human Performance Technology Point of View, *Readings and Case Studies in the Management of Information Security*, 2007.

[40] Savage, M., Malicious Attacks Behind More Data Security Breaches than Human Error. *TechTarget*, Jan 11, 2010. http://searchfinancialsecurity.techtarget.com/news/1378614/Malicious-attacks-behind-more-data-security-breaches-than-human-error (Last Accessed: May 30, 2011).

[41] ITRC, Identity Theft Resource Center 2009 Breach List. *Identity Theft Resource Center*, June 1, 2010.

[42] Christey, S., Martin, B., Brown, M., *et al.*, 2010 CWE/SANS Top 25 Most Dangerous Software Errors v1.08. *CWE*, 2010.

[43] Lam, J., Top 25 series - Rank 1 - Cross Site Scripting. *SANS Software Security*, SANS, Feb 22, 2010. http://software-security.sans.org/blog/2010/02/22/top-25-series-rank-1-cross-site-scripting/ (Last Accessed: June 2, 2011).

[44] Crowley, E., Information System Security Curricula Development. *In Proceedings of the CITC4 '03: 4th Conference on Information Technology Curriculum*, (Lafayette, Indiana, USA), ACM, 2003.

[45] Dark, M. and Davis, J., A Curriculum Framework for the Emerging Discipline of Information Assurance. *In Proceedings of the American Society of Engineering Education North Midwest Conference*, (North Midwest), ASEE, 2003.

[46] Spafford, E., Teaching the Big Picture of INFOSEC. *In Proceedings of the 2nd National Colloquium for Information Systems Security Education (NCISSE)*, (James Madison University, VA), 1998.

[47] YouTube, Think Outside the Box. *Mooresetx2*, 2007. http://www.youtube.com/watch?v=C1yYB85ArHE (Last Accessed: 30 May, 2011).

[48] White, G. and Nordstrom, G., Security Across the Curriculum: Using Computer Security to Teach Computer Science Principles. *In Proceedings of the National Information Systems Security Conference*, NISSC, 1996.

[49] Dark, M. J., Epstein, R., Morales, L., *et al.*, A Framework for Information Security Ethics. *In Proceedings of the 10th Colloquium for Information Systems Security Education* (Adelphi, MD), June 5-8, 2006.

[50] Irvine, C. E., Chin, S.-k. and Frincke, D. A., Integrating Security into the Curriculum, *IEEE Computer*, Vol 31, Iss. 12, pp 25-30, 1998.

[51] Trimmer, K., Schou, C. and Parker, K., Enforcing Early Implementation of Information Assurance Precepts Throughout the Design Phase, *Journal of Informations Education Research (SIG-ED JIER)*, Vol 9, Iss. 1, 2007.

[52] Hentea, M., Dhillon, H. S. and Dhillon, M., Toward Changes in Information Security Education, *Journal of Information Technology Education*, Vol 5, pp 221-223, 2006.

[53] Dark, M. J., Ekstrom, J. J. and Lunt, B. M., Integrating Information Assurance and Security into IT Education: A Look at the Model Curriculum and Emerging Practice, *Journal of Information Technology Education*, Vol 5, pp 389-403, 2006.

[54] Null, L., Integrating Security Across the Computer Science Curriculum, *Journal of Computer Sciences in Colleges*, Vol 19, Iss. 5, pp 170-178, 2004.

[55] Shoemaker, D., Bawol, J., Drommi, A., *et al.*, A Delivery Model for an Information Security Curriculum. *In Proceedings of the Third Security Conference*, (Las Vegas, Nevada, USA), Information Institute, 2004.

[56] NSTISS, National Training Standard for Information Systems Security (INFOSEC) Professionals. *Committee on National Security Systems (CNSS)*, 1994. http://www.cnss.gov/Assets/pdf/nstissi_4011.pdf.

[57] Ekstrom, J. J. and Lunt, B. M., Education at the Seams: Preparing Students to Stich Systems Together; Curriculum and Issues for 4-Year IT Programs. *In Proceedings of the CITC4 '03 4th Conference on Information Technology Curriculum*, (New York, NY, USA), ACM, 2003.

[58] Lunt, B. M. and Ekstrom, J. J., The IT Model Curriculum: A Status Update, *SIGITE '08 Proceedings of the 9th ACM*

SIGITE Conference on Information Technology Education, 2008.

[59] Ockham's Razor. *Encyclopaedia Britannica*. 2011. http://www.britannica.com/EBchecked/topic/424706/Ockhams-razor (Last Accessed: May 30, 2011).

[60] Stohr-Hunt, P. M., An Analysis of Frequency of Hands-On Experience and Science Achievement, *Journal of Research in Science Teaching*, Vol 33, Iss. 1, pp 101-109, 1996.

[61] Nersessian, N. J., Conceptual change in science and in science education, *Synthese*, Vol 80, Iss. 1, pp 163-183, 1989.

[62] Ma, J. and Nickerson, J. V., Hands-on, simulated, and remote laboratories: A comparative literature review, *ACM Computing Surveys*, Vol 38, Iss. 3, pp 7, 2006.

[63] Dittrich, D., On Developing Tomorrow's "Cyber Warriors". *In Proceedings of the 12th Colloquium for Information Systems Security Education* (Dallas, Texas, USA), June 2-4, 2008.

[64] White, G. B. and Williams, D., Collegiate Cyber Defense Competitions. *In Proceedings of the Ninth Colloquium for Information Systems Security Education* (Atlanta, Georgia), The ISSA Journal, October 2005.

[65] White, G. B. and Williams, D., The National Collegiate Cyber Defense Competition. *In Proceedings of the Tenth Colloquium for Information Systems Security Education* (Baltimore, MD), June 2006.

[66] Goldstein, A. and Bucciero, D., The Dartmouth Cyber Security Initiative: Faculty, Staff, and Students Work Together, *IEEE Security and Privacy*, Vol 7, Iss. 6, pp 57-59, 2009.

[67] White, G. B. and DiCenso, D. J., Information Sharing Needs for National Security. *In Proceedings of the System Sciences, 2005. HICSS '05. The 38th Annual Hawaii International Conference on*, 03-06 Jan. 2005.

[68] Sandhu, R., Krishnan, R. and White, G. B., Towards Secure Information Sharing models for community Cyber Security. *In Proceedings of the Collaborative Computing: Networking, Applications and Worksharing (CollaborateCom), 2010 6th International Conference on*, 9-12 Oct. 2010.

[69] Lah, K., Sony Loses Billions Amid Consumer Rage. *CNN*, May 26, 2011. http://www.cnn.com/video/?/video/business/2011/05/26/lah.japan.sony.woes.cnn (Last Accessed: June 2, 2011).

[70] Aamoth, D., New Sony Hack Claims Over a Million User Passwords. *Time*, June 2, 2011. http://techland.time.com/2011/06/02/new-sony-hack-claims-one-million-user-passwords/ (Last Accessed: June 2, 2011).

[71] BBC, US defence firm Lockheed Martin hit by cyber-attack. *British Broadcasting Corporation*, May 30, 2011. http://www.bbc.co.uk/news/world-us-canada-13587785 (Last Accessed: May 30, 2011).

[72] Harrison, K. and White, G., An Empirical Study on the Effectiveness of Common Security Measures. *In Proceedings of the 43rd Hawaii International Conference on System Sciences* (Hawaii, USA), IEEE Computer Society.