The Case for Inclusion of Competitive Teams in Security Education

Anthony Serapiglia
Anthony.Serapiglia@stvincent.edu
CIS Department
St. Vincent College
Latrobe, PA 15650

Abstract

Through industry news as well as contemporary reporting, the topic of computer security has become omnipresent in our daily lives. Whether the news is about corporate data breaches, international cyber espionage, or personal data compromises and identity theft – EVERYONE has had to deal with digital security in some way. Because of this, one of the fastest growing areas of need in the CIS discipline and workforce is for skilled and knowledgeable security workers, and a gap has formed that has left hundreds of thousands of jobs unfilled possibly compromising overall security even more. While nothing trumps actual experience, it is possible to instill some experience into undergraduate students through simulations and especially cyber-security competitions. Inclusion of a competitive team in a second level security course is shown to increase student satisfaction with the course material, instructor effectiveness, and student perception of preparedness in the field.

Keywords: Security, Hacking, CyberSecurity, Competition, Curriculum, Pedagogy

1. INTRODUCTION

"Never trust a dynamiter who has all his fingers…." Old railroad saying…

In the early 2000's, the path to a security job in computing/information assurance/networking was through experience. It was common to see job postings that required 10 years of experience or more for anything that related to security. The positions of Chief Security Officer (CSO) and Chief Information Security Officer (CISO) simply did not exist. In 2015, by modest estimates, more than 209,000 cybersecurity jobs in the U.S. are unfilled, and postings are up 74 percent over the past five years (Carapezza, 2015; Resa, 2014).

According to the United States Department of Labor, the job outlook for Information Security Analysts predicts a growth rate of close to 40% through the year 2022. (BLS, 2014) In a changing atmosphere of perception and understanding of how pervasive security must be within organizations, what used to be categorized as an entry level Systems Administrator position is now often categorized as a security job. The growth in need for workers who are ready to fill these positions has far outstripped the pool of those with ten years of experience. This gap has presented to Computer and Information Science (CIS) programs a common problem facing many disciplines, how best to take the "ten years of experience" and instill that knowledge in a usable form into our students. The purpose of this paper is to highlight how the inclusion of a competitive team participating in an interscholastic cyber-security competition into an advanced security course affected student course evaluations in six categories: "Course work contributes to objectives", "Feel challenged and motivated", "Stimulates interest", "Makes me feel involved", "Effective Instructor", and "Successful course" while also providing practical experience in cybersecurity and information systems management.

2. ENVIRONMENT REVIEW

The year of 2014 saw an unprecedented wave of computer/information/network security events in the headlines and international news. Security breaches at retailers continued to a point where generic headlines became 'fill in the blank' templates of store name and how many personal records were compromised. After the Target point of sale (POS) breach during the holiday shopping season of late 2013 (Vijayan, 2014), so many other retailers were compromised; from Home Depot (Krebs, 2014) and Neiman Marcus (Katz, 2014) to UPS (Hardekopf, 2014) and the State of New York (Virtanen, 2014); that Forbes magazine began a running web listing of the top 20 data beaches of 2014 (Forbes, 2014).

Internationally, the Attorney General of the United States took the unprecedented step of charging five Chinese military hackers for "Cyber Espionage against U.S. corporations and a labor organization for commercial advantage (DOJ, 2014)." In November of 2014, Sony Pictures Entertainment became the victim of a hacking campaign that saw reportedly 100 terabytes of data stolen and public release of many sensitive and embarrassing documents and e-mails in retaliation for "The Interview" a movie lampooning an assignation attempt of Kim Jong-un the leader of North Korea. While some debate still remains on North Korea's direct involvement (Zeter, 2014; Kopan, 2014), Director of Homeland Security Jeh Johnson, FBI Director James Comey, and U.S. Secretary of State John Kerry all have made statements condemning North Korea for the "provocative and unprecedented attack (Kerry, 2014)" with eventual economic sanctions levied by the United States against North Korea because of the attack (Lederman, 2015). From an individual standpoint, 2014 also saw "The Fappening", a breach of Apple's cloud services that led to over 500 private pictures and videos of celebrities made public through a targeted attack of their phone backups held in cloud storage (Alexander, 2014; Hamil 2015).

With so many incidents affecting so many different areas, from government to corporate to individuals, 2014 seemingly became the year in which the "black hats" had a decisive edge against the "white hats".

3. ORGANIZATIONAL EFFORTS

Security is amazingly amorphous in how hard it is to define directly and with precision. While its presence today is ubiquitous in our collective consciousness and daily routine, it is also ever sifting in the form that threats take and the severity to which they expose us. Once mocked and criticized, Donald Rumsfeld's statement on collecting data in support of existence of state sponsored terrorism in Iraq has become much used in risk assessment (Girard, 2014; Neve, 2014):

> "Reports that say that something hasn't happened are always interesting to me, because as we know, there are known knowns; there are things we know we know. We also know there are known unknowns; that is to say we know there are some things we do not know. But there are also unknown unknowns -- the ones we don't know we don't know. And if one looks throughout the history of our country and other free countries, it is the latter category that tend to be the difficult ones." (Rumsfeld, 2002)

While many may have thought this quote to be simply political doublespeak, many who deal in computer and information security simply nodded their heads in understanding. It is always easy to break down any computing issue into a binary form: one or zero, on or off, true or false, protected or unprotected, known or unknown… However, 'in the field' experiences have shown that there is often a shade of grey between the two ends. Often there is an unknown unknown lurking that cannot be prepared for directly. Intuition, experience, hunches can all come into play in preparation and response when that third option inserts itself into the binary world. Unfortunately for those either looking to break into the world of security, or for those trying to fill security positions, those skills are not easily come by quickly or in a classroom.

David Sanger, New York Times Chief Washington Correspondent is an expert on cybersecurity. "The hardest thing about teaching anything about cybersecurity is the same thing that's the hard part about writing and reporting about cybersecurity, which is, it's moving so fast," Sanger explains (Carapezza, 2015). A Harvard graduate, he is a senior fellow and adjunct lecturer now teaching a course on cybersecurity, national security, strategy, and the press that draws from today's headlines in his lectures and case studies (Harvard, 2015). This approach is not uncommon. One of the issues that has always added complexity to Computing, Information Science, and Information Systems curriculum development has been that these programs exist in multiple different schools which by nature focus

on different outcomes whether the program is housed in a Business School, Communications School, Library Science School, Engineering School, or even a Mathematics School.

The Association for Computing Machinery (ACM) has provided model curriculum guidelines since the 1960s. The 2013 model curriculum is the latest update. In it Information Assurance and Security is broken out into it's own Knowledge Area (KA) for the first time. In defining the KA, industry standards of CIA (Confidentiality, Integrity, and Availability) are used in conjunction with providing for authentication and non-repudiation. Broadening the scope, CS2013 acknowledges that both assurance and security concepts are needed to ensure a complete perspective, "Information assurance and security education, then, includes all efforts to prepare a workforce with the needed knowledge, skills, and abilities to protect our information systems and attest to the assurance of the past and current state of processes and data (ACM, 2013)."

The model curriculum guidelines for Information Systems version 2010 lists security and risk management as one of a group of five high level IS capabilities. Under the heading of Understanding, Managing and Controlling IT Risks, this is more clearly defined as, "IS graduates should have strong capabilities in understanding, managing, and controlling organizational risks that are associated with the use of IT-based solutions (e.g., security, disaster recovery, obsolescence, etc.). At the undergraduate level, the emphasis should be on in-depth understanding of a variety of risks. Because IT solutions are so closely integrated with all aspects of a modern organization, it has become essential to manage the risks related to their use in a highly systematic and comprehensive way (ACM, 2010).

Other organizations have become leaders in defining what professional certifications should encompass. The International Information Systems Security Certification Consortium, $(ISC)^2$, was formed in 1989 as a group to determine a Common Body of Knowledge (CBK) that has become the basis for what has been the leading security certification for years, the Certified Information Systems Security Professional (CISSP) certification. As of 2015 the CBK includes eight domains of focus: Security and Risk Management, Asset Security, Security Engineering, Communications and Network Security, Identity and Access Management, Security Assessment and Testing, Security Operations, and Software Development Security (ISC2, 2015) One of the hallmarks that sets the CISSP certification apart from others has been the added requirement that not only do candidates have to pass an exam related to the CBK, but they must also show that they possess a minimum of five years of direct full-time security work experience in two or more of the security domains. However, one of the critiques of the CISSP certification as the industry has matured, is that the CBK is "an inch deep and a mile wide" with this phrase even becoming the title of a popular website devoted to helping candidates prepare for the test (https://inchdeepmilewide.wordpress.com).

The alternative to the CISSP certification is offered by the EC-Council (The International Council of Electronic Commerce Consultants) with their flagship certification being the Certified Ethical Hacker (CEH). The CEH certificate has been offered since 2003 (Goldman, 2012) and is heavily centered on practical skills education and specifically penetration testing techniques. The name itself has been controversial, becoming both an asset and a possible hindrance to the organization and certificate holders (D'Ottavi, 2003; Olson, 2012). The word "hacker" has carried multiple meanings through the years and has not always been looked favorably and more conservative executives are wary of the negative association.

The other leading organization in developing curriculum and certification programs is the SANS Institute (the name is derived from SysAdmin, Audit, Networking, and Security). Founded in 1989, the organization created their Global Information Assurance Certification (GIAC) in 1999. GIAC tests and validates the ability of practitioners in information security, forensics, and software security. SANS as an organization has grown to provide training seminars on ground and online, with the SANS Technology Institute was granted regional accreditation by the Middle States Commission on Higher Education and now offers two Masters of Science degree programs (SANS, 2014). The SANS Reading Room - a research archive of information security policy and research documents delivers over one million downloads per year to professionals globally.

A common thread amongst these organizations in their curriculum models and certification paths, is that although both the CISSP and CEH require proof of field experience, these organizations have had a focus on providing support materials for the classroom and promoting standards of what should be included and expected of the students/certificate candidates.

4. COMPETITIONS

Security is at its very heart a competition. Any activity that pits one entity against another can be considered competition. Competitions take many forms and occur at many levels of intensity and consequence. Some are recreational, contested for fun. Others are blood sport, grave consequences of life and death at stake. So it is with security. Actions that were once considered fantasy only possible in movies such as War Games (1983), aggressive digital attacks have occurred causing physical damages with lasting global ramifications. The success of Stuxnet (Gross, 2011; Langer, 2011; Zetter, 2014) proved that state sponsored cyber-attacks could be as successful in the 21st century as the clandestine saboteurs of the World Wars in the 20th century was in disabling factories and other machines of war. On one hand, one country can say an act of war occurred. On another, some could say the slowing or stopping the production of a weapon of mass destruction saved countless lives.

As a training ground for education, competitions provide a fertile field for enabling students to gain experience quickly in a focused and controlled environment. This concept is not new, flight simulators have been used to train pilots for decades, and with technological innovations the use of simulators have grown to include sport and race car drivers to law enforcement and combat training. In the cybersecurity world, "capture the flag" (CTF) competitions are the simulated crucible in which the curriculum lessons are tested and validated by the students. Instead of a playing field with physical flags to capture, Red teams and Blue teams defend and attack computer networks and the flags are data and services that are either preserved or disabled.

University of California Santa Barbara (UCSB) has grown a series of live exercises in their Computer Science department into the iCTF – International Capture the Flag competition which claims to be the largest and longest running having started in 2001. Starting as a local onsite competition, it has grown to international scope and has developed an open source framework for hosting virtual networks to facilitate the hosting of other competitions (UCSB, 2015).

Perhaps the best known of the CTF competitions is the one held in conjunction with the annual DEFCON event in Las Vegas. Started in the fourth year of the conference, 1996, it has been a prominent feature of each edition since. The CTF "game" at DEFCON has evolved and grown through the last 20 years and has become a model from which many others are patterned. "At its core CTF is meant to test computer and network security. To some, that seems to be a fairly narrow focus area, but most Defcon attendees realize that "cyber security" is actually a very large and diverse field. Services range from poorly implemented or configured crypto, SQL-injection, cross-site-scripting, buffer overflows, timing attacks, heap exploits, malformed network constructs, custom interpreters, the list is truly endless. (DEFCON, 2015)."

5. INTEGRATING COMPETITIONS

'College A' is a small Catholic Liberal Arts college in the Mid-Atlantic region. Overall enrollment at the college is approximately 1,200 with a range of 60 to 70 Computing Information Science (CIS) majors. In the past four years, enrollment in the CIS program has grown nearly 30%. With limited resources, several courses are offered on every other year cycle. The Security track is one of these. During the 2012/2013 academic year a redesign of the first and second level security courses was undertaken. The first level course was organized to be in line with the $(ISC)^2$ Common Body of Knowledge (CBK) associated with the CISSP certification. As an introductory course, the "inch deep, mile wide" coverage of the security world is utilized to introduce students to width and breadth of the entirety of the security world. The second level course was redesigned to be more in line with the outcomes defined in the Certified Ethical Hacker (CEH) certification path, with more in depth coverage of networking, cryptography, penetration testing, and forensics.

The first level course received a good reception from the students. The general response was an eye opening experience to the wider CBK and the eight different domains. While positively received, there was a definite gap between book material and skills material that was recognized by the students. This was expressed in at least two of the comments in the course end student evaluations: "The idea of computer security is such a broad spectrum of information. I feel that I have learned a lot, but still don't know if I could handle such tasks in the work environment." And "I definitely learned a lot more about security than I thought I would. Intellectual fulfillment for me is top notch for this course, as I feel my eyes have been opened significantly. I wish there was a more interactive way to teach this, but I do also understand that to get through 10 domains, PowerPoints and lecturing are necessary. I

particularly enjoyed the hands-on labs, so if more of those can be integrated without losing time to cover all of the material, then I would highly recommend that."

One of the challenges in developing the second level course was the choice of text. With a broad range of topics, the problem was encountered that no one text book was as in depth in any one of the topics as multiple texts devoted to the specific topics would be. Multiple texts would be burdensome to the students and the prevailing culture of the school would not allow a course with no formally stated required text. A decision was made to go with one text that had good coverage of two of the topics, with supplemental materials from the SANS Institute and other Internet sources on the other topics. Opinions varied on the overall success of the course. While most responses of the student surveys were positive in their comments, the survey numbers for several student evaluation categories showed a decrease between the two courses.

	1st Level F2012 (n=16)	2nd Level S2013 (n=8)
Course work contributes to objectives	5.3	5.0
Feel challenged and motivated	5.12	5.0
Successful course	5.5	5.1
Stimulates interest	5.44	5.1
Makes me feel involved	5.06	4.9
Effective Instructor	5.31	4.9

Fig 1. Student Course Evaluation Scores comparing 1st semester intro class to second semester 'advanced' class

In addressing the drop in numbers between the two courses, it was determined that the material simply needed to be brought together in a more cohesive manner that showed the interconnected nature of the disparate topics. With limited time and resources, as well as cost to student concerns, it was decided that the best course of action was to incorporate an interscholastic cyber-security competition into the course.

MACCDC

Since the mid 2000's, several groups have come together to help fill the gap between the curriculum and course material side of security education and the practical skills and experience side. In combination, the National Cyberwatch Center, The Collegiate Cyber Defense Competition (Mid-Atlantic division, MACCDC), and the National Cyber League have formed a robust environment that provides support materials, training 'gymnasiums' with practice and exploration opportunities, and a hosted high level competitive CTF style event. Participation in the NCL cost $20 per student, and registration for a team in the MACCDC competition cost $250.

During the second half of the fall semester in the first level course, students were made aware that there would be a competition team as part of the second level course in the spring. As preparation for the competition, exercises could be worked through on a volunteer basis through the NCL website.

During the spring semester, the focus of the course materials in the second level class was much the same as it had been in the previous delivery of the course two years prior. The general topics of focus were the same, with much based on the CEH path of certification. Topics related to networking, Systems Administration, and penetration testing were focused upon early as the preliminary stages for the MACCDC competition were schedule halfway through the semester.

An early concern was how to select students for the team, or whether to field two teams for the competition. For better or worse, this decision was moot, as the scheduling of the preliminary rounds fell during the time of spring break. The rules of the MACCDC call for a team no greater than eight, and eight was the number of students that would still be available to be on campus to participate.

The preliminary round was held virtually with each team/school logging into a hosted virtual environment. For the qualifying session, each team was given access to four virtual servers, two Windows based instances and two LINUX instances. Each had several services running including a SQL server, Active Directory, a web server, and a software PBX instance. From the start of the competition clock, the student team was given 15 minutes to familiarize themselves with the environment and to take any preliminary hardening actions they could. After 15 minutes a "Red Team" of aggressors comprised of event coordinators and administrators began to try and disrupt the services and functions of the servers. Scoring was comprised of three different areas: service uptime, 'flags' found (discovery questions answered about the system), and 'injects' or work orders that were given at intervals during the three-hour time period.

During the 2015 MACCDC, 30 schools participated. These schools comprised a wide variety of shape and size from large state universities, to small private liberal arts colleges, to several regional community colleges. As a first time participant, the team fielded by this school had a goal of discovery as much as competition. While not scoring in the top ten, the team did not finish last.

Observing the team during the competition showed how this crucible brought out the best, and unfortunately the worst, in the students. Three groups formed in focusing on separate tasks. One overall 'captain' was able to organize efforts, but eventually struggled to keep track of everything. Four students who had previous Sys Admin experience through internships and side projects became leaders and took charge of the individual groups. Only two sophomores threw up their arms in overwhelmed defeat.

Comments from the students highlighted their experience directly after; "I think I learned more in that three hours than I have in my previous three years…" and "Thank you for putting in the time and getting everything together and giving us the opportunity to compete. I enjoyed doing this and feel I learned some pretty cool things. At the very least it gave us a guide of what to learn and put time into."

In class after break, the team participants gave a presentation to the full class detailing the experience and highlighting some of the essentials of what they learned. Amongst the list were command and control issues such as ensuring you have multiple avenues of access into a machine and the use of the whiteboards to make sure everyone was on the same page with status reports. Other notes included the importance of your "go to" list of reference sites for basic shell/terminal commands, the importance of prioritizing your discovery to essential services, and above all else – first step, change the admin passwords!

Results

Even though only half of the students in the course were able to participate in the actual competition, all of the students benefitted by the focus of how the course materials fit the idea of the competition. The materials did not change significantly in their content or presentation from the previous delivery of the course. These positive effects were shown in the student course evaluations as compared to the same course two years earlier.

	2nd Level S2013 (N=8)	2nd Level S2015 (N=16)
Course work contributes to objectives	5.0	5.67
Feel challenged and motivated	5.0	5.60
Successful course	5.1	5.38
Stimulates interest	5.1	5.38
Makes me feel involved	4.9	5.44
Effective Instructor	4.9	5.56

Fig 2. Student Course Evaluation Scores comparing 'advanced' class scores from 2013 without competition, and 2015 with competition

Even though the number of students in the course doubled, metrics associated with student satisfaction levels, students' perceptions of the success of the course, and the instructor all increased.

6. CONCLUSIONS

Through industry news as well as contemporary reporting, the topic of computer security has become omnipresent in our daily lives. Whether the news is about corporate data breaches, international cyber espionage, or personal data compromises and identity theft – EVERYONE has had to deal with digital security in some way. Because of this, one of the fastest growing areas of need in the CIS discipline is for skilled and knowledgeable security workers. A gap has formed that has left hundreds of thousands of jobs unfilled, possibly compromising overall security even more. While nothing trumps actual experience, it is possible to instill some experience into undergraduate students through simulations and especially competition.

Several organizations, including ACM, ISC2, the EC-Council, SANS Institute, etc. have outlined model curriculums with input from leading educational and industry experts. These organizations have developed materials and provided testing infrastructure to certify students in the discipline. However, another area is needed to validate skill sets and working knowledge of the material, and that is being filled by the organizations that are developing and hosting competitions. Just as Shotokan Karate is broken into three parts – kihon (basic instruction), kata (practice of patterns of moves), and kumite (sparring) – the discipline of cyber security should encompass three parts of equal measure – basic

instruction, practice, and finally a testing bed of competition.

Incorporating the third area of competition into an existing second level security course produced significant increases in student satisfaction with the course and the instructor. As one student summed it up, "This class made me feel confident that I know more about security than most people my age. I feel I have learned more in his classes than anywhere else, because you get tossed into a situation and you need to figure it out. Problem Solving skills are some of the most important skills someone in our field can have, and this course helps us develop those skills."

9. REFERENCES

Alexander, E. (2014, September 1). Jessica Brown Findlay: Downton Abbey star is linked to list of celebrities targeted by hackers. Retrieved June 2, 2015, from http://www.independent.co.uk/news/people/jessica-brown-findlay-downton-abbey-actress-is-linked-to-list-of-celebrities-targeted-by-hackers-9704785.html

Bureau of Labor Statistics, U.S. Department of Labor, Occupational Outlook Handbook, 2014-15 Edition, Information Security Analysts, on the Internet at http://www.bls.gov/ooh/computer-and-information-technology/information-security-analysts.htm (visited May 22, 2015).

Carapzza, Kirk. "With More than 200,000 Unfilled Jobs, Colleges Push Cybersecurity." PBS. January 22, 2015. Accessed April 27, 2015.

Central Challenges of American National Security, Strategy, and the Press. (2015). Retrieved June 4, 2015, from http://www.hks.harvard.edu/degrees/teaching-courses/course-listing/iga-211

Computer Science Curricula 2013: Curriculum - ACM. (2013, December 20). Retrieved February 1, 2015, from http://ACM.ORG

"Condemning Cyber-Attack by North Korea". United States Department of State. December 19, 2014. Retrieved December 24, 2014.

DEF CON Hacking Conference: CTF History. (n.d.). Retrieved June 3, 2015, from https://www.defcon.org/html/links/dc-ctf-history.html

D'Otavi, A. (2003, February 3). Interview: Marcus J. Ranum, the "father" of the firewall. Retrieved June 4, 2015, from http://www.infoservi.it/interview-marcus-j-ranum-the-father-of-the-firewall/1057

Girard, John; Girard, JoAnn (2009-06-01). A Leader's Guide to Knowledge Management: Drawing on the Past to Enhance Future Performance. Business Expert Press. pp. 55–. ISBN 9781606490198. Retrieved 10 February 2014.

Goldman, J. (2012, May 2). How to Become a Certified Ethical Hacker. Retrieved April 5, 2015, from http://www.esecurityplanet.com/hackers/how-to-become-a-certified-ethical-hacker.html

Gross, M. (2011, April 1). A Declaration of Cyber-War. Retrieved June 1, 2015, from http://www.vanityfair.com/news/2011/04/stuxnet-201104

Hamil, J. (2015, June 12). How did hackers get their paws on up to 600 celebs' sexy selfies? Retrieved June 1, 2015, from http://www.mirror.co.uk/news/technology-science/technology/fappening-sexy-celeb-selfie-hacker-5871352

Hardekopf, Bill. "UPS Reveals Data Breach in 51 Stores." LowCards. August 21, 2014. Accessed June 7, 2015. http://www.lowcards.com/ups-stores-reveals-data-breach-51-stores-26855.

Information Systems Curricula 2010: Curriculum - ACM. (2010, May 20). Retrieved February 1, 2015, from http://ACM.ORG

International Information Systems Security Certification Consortium. (n.d.). Retrieved June 14, 2015, from https://www.isc2.org

Katz, Karen. Security Info at Neiman Marcus. June 15, 2014. Accessed March 16, 2015. http://www.neimanmarcus.com/NM/Security-Info/cat49570732/c.cat?icid=topPromo_hmpg_ticker_SecurityInfo_0114.

Kopan, T. (2014, December 29). U.S.: No alternate leads in Sony hack. Retrieved April 16, 2015, from http://www.politico.com/story/2014/12/fbi-briefed-on-alternate-sony-hack-theory-113866.html

Krebs, Brian. "Krebs on Security." Krebs on Security RSS. September 14, 2014. Accessed June 3, 2015. http://krebsonsecurity.com/2014/09/home-depot-hit-by-same-malware-as-target/

Langer, R. (2011, March 1). Cracking Stuxnet, a 21st-century cyber weapon. Retrieved June 2, 2015, from http://www.ted.com/talks/ralph_langner_cracking_stuxnet_a_21st_century_cyberweapon?language=en

Lederman, Josh (January 2, 2015). "US slaps sanctions on North Korea after Sony hack". Associated Press. San Francisco Chronicle. Retrieved January 5, 2015.

Neve, Geert de; Luetchford, Peter (2008). Hidden Hands in the Market: Ethnographies of Fair Trade, Ethical Consumption, and Corporate Social Responsibility. Emerald Group Publishing. pp. 252–. ISBN 9781848550582. Retrieved 10 February 2014.

Olson, P. (2012, July 31). Exploding The Myth Of The 'Ethical Hacker' Retrieved June 3, 2015, from http://www.forbes.com/sites/parmyolson/2012/07/31/exploding-the-myth-of-the-ethical-hacker/

Resa, Dan. "The Growth of Cybersecurity Jobs." Growth of Cybersecurity Jobs. March 1, 2014. Accessed May 16, 2015. http://www.burning-glass.com/research/cybersecurity/.

Rumsfeld, D. (2002, February 12). United States Department of Defense. Retrieved February 5, 2015, from http://www.defense.gov/transcripts/transcript.aspx?transcriptid=2636

SANS: Accreditation & Authorization. (n.d.). Retrieved June 8, 2015, from https://www.sans.edu/about/authorization

The Big Data Breaches of 2014. (2014). Retrieved June 3, 2015, from http://www.forbes.com/sites/moneybuilder/2015/01/13/the-big-data-breaches-of-2014/

The UCSB iCTF Competition. (n.d.). Retrieved June 16, 2015, from http://ictf.cs.ucsb.edu/

U.S. Charges Five Chinese Military Hackers for Cyber Espionage Against U.S. Corporations and a Labor Organization for Commercial Advantage. (2014, May 19). Retrieved June 1, 2015, from http://www.justice.gov/opa/pr/us-charges-five-chinese-military-hackers-cyber-espionage-against-us-corporations-and-labor

Vijaya, Jaikumar. "Target Breach Happened Because of a Basic Network Segmentation Error." Computerworld. February 6, 2014. Accessed June 7, 2015. http://www.computerworld.com/article/2487425/cybercrime-hacking/target-breach-happened-because-of-a-basic-network-segmentation-error.html.

Virtanen, Michael. "22.8 Million Personal Records of New Yorkers Exposed." Rochester Democrat and Chronicle. July 16, 2014. Accessed June 3, 2015. http://www.democratandchronicle.com/story/news/2014/07/15/data-security-breaches-new-york/12706213/.

Zetter, K. (2014, November 3). An Unprecedented Look at Stuxnet, the World's First Digital Weapon. Retrieved June 1, 2015, from http://www.wired.com/2014/11/countdown-to-zero-day-stuxnet/