Journal of Cybersecurity Education, Research and Practice

Volume 2018 | Number 2 Article 3

12-31-2018

Using Case Studies To Teach Cybersecurity Courses

Yu Cai
Michigan Technological University, cai@mtu.edu

Using Case Studies To Teach Cybersecurity Courses

Abstract
This paper introduces a holistic and case-analysis teaching model by integrating case studies into cybersecurity courses. The proposed model starts by analyzing real-world cyber breaches. Students look into the details of these attacks and learn how these attacks took place from the beginning to the end. During the process of case analysis, a list of security topics reflecting different aspects of these breaches is introduced. Through guided in-class discussion and hands-on lab assignments, student learning in lecture will be reinforced. Overall, the entire cybersecurity course is driven by case studies. The proposed model is great for teaching cybersecurity. First, the new model can easily draw students' interests with real-world cases. Second, the new model can help to teach human and business factors in cybersecurity. Third, the new model can improve student learning outcomes, particularly helping students gain a holistic view of security.

Keywords
Computer network security, computer science, education, education, security

Cover Page Footnote
The author thanks all the students at the School of Technology of Michigan Technological University that took part and responded in this study. This research work was supported in part by National Security Agency (NSA) under grant number H98230-17-1-0227 and H98230-17-1-0414.

INTRODUCTION

People with cybersecurity skills are in great demand as the threat environment increasingly becomes more complex and challenging. According to workforce reports by Cisco and Peninsula Press in 2015, there are more than 200k unfilled cybersecurity jobs in the U.S. alone, and the global figure of unfilled cybersecurity openings is 1 million. The global demand for cybersecurity professionals will rise to 6 million by 2019, with a projected shortfall of 1.5 million (Peninsula Press, 2015; Cisco Report, 2015). The need to have well-trained and well-prepared cybersecurity workforce is a pressing issue.

However, there are mismatches between industry needs and cybersecurity education. For example, even though security is treated as one of the top concerns by industry, a recent study by CloudPassage in 2016 finds only three of the top fifty U.S. computer science programs require at least one security course for graduation (CloudPassage, 2016). The study shows that "there is an incredible IT security skills gap... a major root cause is a lack of education and training at accredited schools". Another ISACA reports in 2017 finds that less than 25% of cybersecurity job candidates are qualified (ISACA report, 2016). There is a growing acceptance among the cybersecurity community that a holistic approach that incorporates technical, human and business factors is needed to better train students to meet industry needs and fill existing IT security skills gaps (LeTellier, V. , 2016).

The core idea of this paper is to explore a new Holistic & Case-Analysis (HCA) model for cybersecurity education. The new HCA model aims to restructure cybersecurity courses by integrating and analyzing high-profile cybersecurity breaches such as the Target breach in 2013 (US Senate Report, 2014), the Anthem breach in 2015 (Wiki on Anthem, 2015), the Equifax breach in 2017 (Berghel, H., 2017), a few DDoS attacks (Prince, M., 2013; Margolis et al., 2017), and other cases. Students will look into the details of these attacks, learn how these attacks took place from the beginning to the end, understand what security topics are relevant, and study how these attacks could be prevented or stopped. Students will also be able to replicate some of the breaches in a simulated virtual lab environment using similar tools and methods described in the case studies. Through guided in-class discussion, selected readings, and hands-on lab assignments centered around the case studies, students will explore various cybersecurity offensive and defensive techniques, and understand best practices and lessons learned in the real world. During the process of case analysis, students will learn how different subsystems interact with each other and obtain a whole picture of integrated cybersecurity systems. In addition, socio-technical topics including human and business factors are introduced during case analysis.

In the new HCA model, we go beyond the traditional case-study approach. For example, traditionally case studies are used to introduce or illustrate a single security topic to students. This traditional case study method is effective but not enough to help students link multiple and often seemingly unrelated security topics together. In the new HCA model, the entire cybersecurity course, from course topic selection to course schedule arrangement, from lecture content to lab activities, are all driven by cybersecurity case studies.

The authors conceived the idea of HCA during the normal process of teaching cybersecurity and related classes. The HCA model was tested in a cybersecurity course at Michigan Technology University during the summer/fall semester of 2015 and 2016. The small-scale pilot study shows that the new course is extremely well received by students. Most students (80%) expressed great interests and enthusiasm on cybersecurity during and after taking the course by using this HCA model. More than 30% students indicated that they plan to consider cybersecurity as career options in the future.

The authors would like to point out that the HCA model is young and may need refinement. Therefore, the main purpose of this paper is to introduce preliminary results and share findings with the cybersecurity education community.

PROJECT RATIONALE

A holistic or top-down teaching approach focuses on providing students a big picture or a macro view of a system, then breaking down the system into many compositional sub-systems. A bottom-up teaching approach begins with the component parts of a system and gradually builds up to the whole by piecing together many sub-systems. Both top-down and bottom-up can be effective teaching methods, but operate in the opposite direction.

Teaching with case studies is another common pedagogy widely used in many disciplines (Christensen, 1981; Stanford Newsletter on Teaching, 1994). Study cases are usually realistic, complex, and context-rich stories used to show the application of a theory or concept in real situations. Teaching with cases can help students actively engage in classroom participation and achieve positive learning outcomes.

There are three main advantages of the proposed HCA models.

First, the HCA model can increase students' interests in cybersecurity, thus attracting more students to the cybersecurity field. - "Interest is the best teacher!"

Increasing student engagement and interest is crucial to achieving positive educational outcomes. Students usually have a great curiosity to know what happened in real-world cyber breaches, especially when those cases of security incidents have a direct or even indirect impact on themselves or the technologies they use. Analyzing these high-profile breaches are an eye-opening experience for most students. The instructor can easily motivate students to explore and research details of these cyber breaches and then analyze underlying security topics. The past few years have witnessed a significant enrollment growth for computing majors across the nation. However, attracting computing students to the cybersecurity field remains a challenging issue. It is our hope that the increased interests and personal impact of cybersecurity will motivate more students to choose cybersecurity as academic and professional career options.

Second, the HCA model is great for teaching human and business factors in cybersecurity by analyzing complicated real-world socio-technical systems which are often across multiple cultures. - "Only amateurs attack machines; professionals target people."

During case analysis, it is a natural step to draw student's attention to human, social, ethical, organizational, and economic factors, and the complex interaction between these factors. In traditional cybersecurity courses, it can be difficult to find a good place to fit human, social and business factors especially from a global perspective. Analyzing the social engineering and human aspect is a key element in providing students experience with the human factor that is often missing from more purely technical cybersecurity courses.

Third, the HCA model may improve student learning outcomes by helping student link individual security topics and understand how they are used in real-world systems. - "You can't see the forest for the trees."

Traditional cybersecurity courses are usually bottom-up where security topics are taught one by one in an isolated context, with little or no final integration. The main drawback is that students will have a hard time linking these topics together to see the whole larger picture of cybersecurity in enterprise networks. In the new model, we start by dissecting the real-life cyber breaches and real-world enterprise networks. During case analysis, students are guided to follow the footprint of hackers, including topics such as the technical and social tools and methodologies used, amount of time spent and persistence when breaking into and staying in a system, and the collaboration and organization required to perform cyberattacks. Students will not only get hands-on and practical experience, but also start to see how different security mechanisms interact with each other, and how they are integrated into enterprise networks, and how the weakest links in a system are exploited by hackers, thus obtaining a comprehensive and holistic view of cybersecurity.

In summary, we believe that the proposed model has several unique advantages and can better prepare students for industry needs. Figure 1 compares the proposed HCA model with the bottom-up model in cybersecurity education.

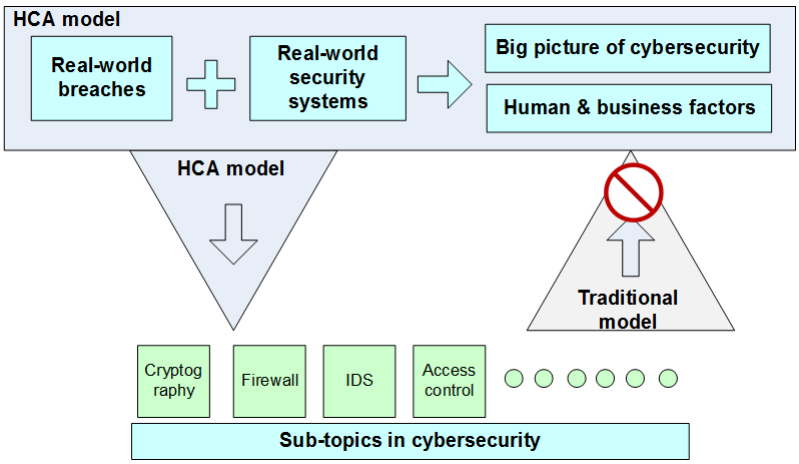

Figure 1. The Holistic and Case-analysis (HCA) model vs. the bottom-up model

Additional reasons to adopt the HCA model

Below we discuss some additional reasons to adopt the HCA model in cybersecurity education.

First, there are many high-profile cyber breaches that illustrate many lessons people could learn. To a certain extent, the cybersecurity industry is driven by cyber breaches and cyber threats, so should cybersecurity education.

Second, the HCA model can better prepare students for industry jobs where there are more brownfield projects than greenfield projects. Brownfield projects mean to start a project based on prior work or to rebuild a product from an existing one. Greenfield projects mean to start a project without the need to consider any prior work. The HCA approach usually starts with an existing system and tries to break it down or fix some existing problems, which is similar to most industry jobs. The traditional bottom-up approach usually starts to build a system from the scratch which is only ideal in an academic environment or simulated hypothetical environment.

Third, the HCA model can help instructor select cybersecurity topics to meet industry needs. Cybersecurity courses (or programs) typically cover a wide range of topics and evolve at a very fast pace. It is always challenging for instructors to decide which topics to cover. By utilizing the new model, some timely cybersecurity topics such as email phishing, web security, ransomware, privileged escalation, vulnerability scanning, and privileged account management will be introduced into the new course.

RELATED WORK

Case Study

According to Lawrence, a useful case study is "the vehicle by which a chunk of reality is brought into the classroom to be worked over by the class and the instructor. A good case keeps the class discussion grounded upon some of the stubborn facts that must be faced in real life situations" (Christensen, 1981). Case studies have been used widely in higher education fields (Kreber, 2001).

Case study is a commonly used teaching method in computer science education. For example, (Baumgartner, 2013) studied using case studies to design and deliver technology-centered computing education courses. (Cai and Arney, 2017) introduced case studies in cybersecurity education. (Mitchell et al., 2012) used case studies to develop a curriculum for communicating parallel and distributed computing concepts.

Cybersecurity Education

There is a growing pool of efforts on cybersecurity education including teaching pedagogies, curriculum materials, lab platforms, and faculty training.

Several effective teaching pedagogies are developed to improve student learning outcomes on cybersecurity. For example, hacker curriculum and offensive security curriculum are presented in (Bratus, 2007; Trabelsi and Ibrahim, 2013). Cybersecurity hacking competitions / Hackathons are introduced in iCTF (Doupé et al., 2011), CCDC (NCCDC, 2016) and (Denning et al., 2013).

Other approaches include game-based learning (Jin et al., 2018), project-based learning (Estes et al., 2016), problem-based learning (Wilson, 2017), and inquiry-based learning (Kerven et al., 2017). In (Jin et al., 2018), the authors described their experience of GenCyber summer camp activities in the format of game-based learning and hands-on labs to stimulate the K-12 stu-dents' interest in the cybersecurity field and raise their awareness of cybersecurity and safe online behavior. In (Wilson, 2017), the authors presented the OWASP project to teach cyberse-curity defense through web-based hacking to undergraduate students.

For curriculum materials, the NSF sponsored SEED (Du, 2011) and ITSEED (Bai and Wang, 2014) project present a set of well-documented security labs. Also, cloud-based virtual lab plat-forms such as EDURange (Weiss et al., 2015) and DETERlab (Peterson and Reiher, 2010) have been developed for security education.

The U.S. government has recognized the importance of cybersecurity with two efforts. The first effort is the National Initiative for Cybersecurity Education (NICE) effort led by National Insti-tute of Standards and Technology (NIST), and the other one is the National Centers of Academ-ic Excellence (CAE) led by National Security Agency (NSA) and Department of Homeland Se-curity (DHS).

Information Assurance and Security has been added as a core topic in the ACM/IEEE Computer Science Curriculum and IT curriculum. There are also continuing efforts to promote cybersecu-rity education to K-12 teachers and students (Gorka et al., 2017).

DETAILED COURSE DESCRIPTION

Selection of course topics

Table 1 compares course topics in a traditional cybersecurity course and in the new cybersecurity course with the HCA model. The topics are extracted from the classic textbook "Corporate Computer Security (4rd Edition)" by Randall J. Boyle and Raymond R. Panko. This textbook provides excellent coverage on a variety of security topics, and is used here as an example and for illustration purposes.

In Table 1, topics with an underline are newly added content in the new course, and topics with italic font are case studies. Subtopics identified by the HCA model represent some of the timely and urgent needs of the industry. These subtopics will be continuously updated based on real-world cyber breaches and security incidents. The instructors can choose new subtopics based on their own course customization needs.

Sample network architecture in an enterprise environment

In the HCA model, we will introduce a basic network architecture in an enterprise environment (Figure 2). This figure will be used with case studies to help students understand what real-world network systems look like, how different subsystems interact with each other, and how these subsystems are integrated together.

Table 1. Comparison of Cybersecurity Course Topics.
(Note: Underline is for new topics; italic is for case studies)

Topics in a traditional course	**Topics in the new course**
1. Introduction 2. Planning & Policy 3. Cryptography 4. Network security 5. Access control 6. Firewall 7. Host Hardening 8. Application security 9. Data protection 10. Incident response	1. Introduction & *Case study on Target breach* 2. Cryptography 3. Email Phishing & Social Engineering 4. Web security (including SQL injection, XSS attack, and Malicious code) 5. Network security & *Case study on DDoS attacks* 6. Access control (including privilege account management) 7. Firewall (including next-generation firewall) & Intrusion Detection Systems (including user behavior analytics) 8. Malware (including ransomware) 9. Incident Response & *Case study on Anthem breach* 10. Risk Analysis

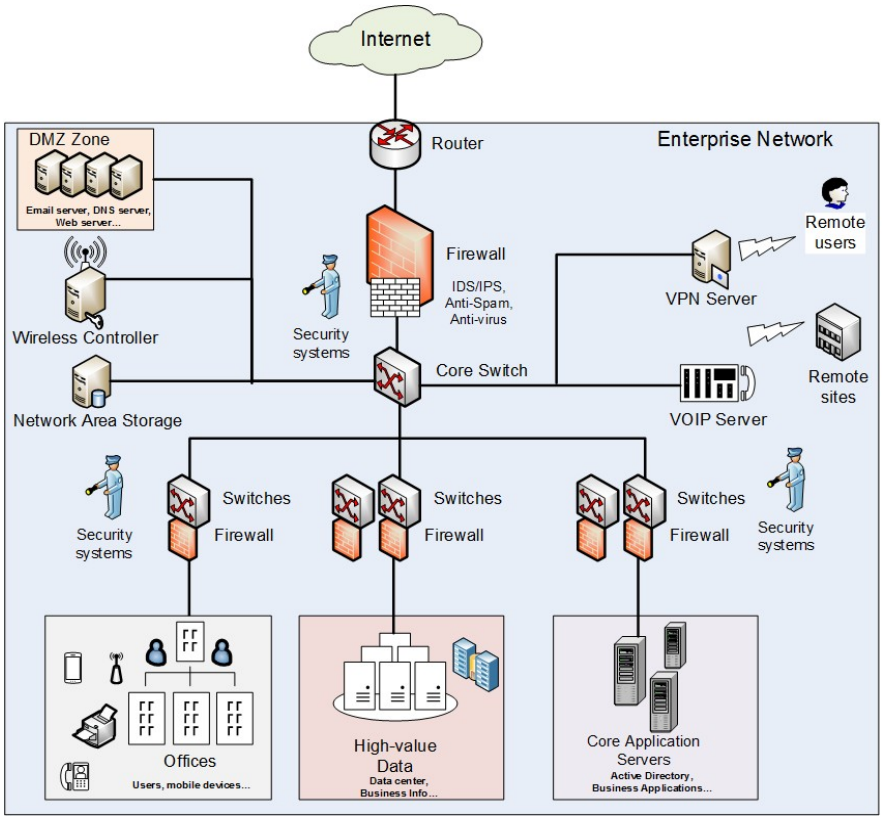

Figure 2. Sample network architecture in an enterprise environment

Figure 2 includes some common network components which are described briefly below:
Internet: The organization is usually connected to the Internet via dedicated lines, broadband or 3G/4G, etc.
Router: Usually a Layer-3 network router connecting LAN and WAN networks.
Firewall etc.: Usually includes Firewall, Anti-phishing, Anti-spam, Antivirus, Intrusion Detection Systems (IDS), Intrusion Prevention Systems (IPS), and content filtering. Sometimes they are called *Unified Threat Management Appliance (UTM).*
Core switch: Usually a Layer-3 network switch connecting systems such as Network Area Storage, Wireless Controller, VOIP phone server, VPN server, and Demilitarized Zone (DMZ).
DMZ Zone: Usually includes computer servers such as ERP, Web Server, Mail Server, Database Server, and Application Servers.

Sample case study: Target data breach

In this section, we will use the Target data breach to illustrate the HCA model.

The Target data breach started around late 2013 and became publicly known around Dec. 2013. Hackers gained access to more than 40 million credit and debit card information through malware on Target's Point-Of-Sale (POS) systems. The Target Company to date has not publicly release details of the breach, and probably never will, but enough information exists online and within the cybersecurity community to piece together what likely happened during the breach. This information can help people prevent similar attacks in the future. Figure 3 is a diagram illustrating the Target data breach with a timeline. Information was collected from a number of sources (US Senate Report, 2014; Kassner, 2015; KrebsonSecurity, 2015; Cyphort, 2014;).

There are several reasons why we decide to use the Target data breach as one of the representative cases. First, the Target breach represents a typical class of cyber threats called Advanced Persistent Threat (APT). APT is a set of stealthy and continuous cyber hacking processes with the intention of stealing high-value data and information from targeted organizations. Second, the Target breach happened in 2013, short enough so that lessons learned are not out of date, also long enough so that there are sufficient details available to piece things together. Third, the Target breach is a high-profile case, which can easily draw students' attention and interests.

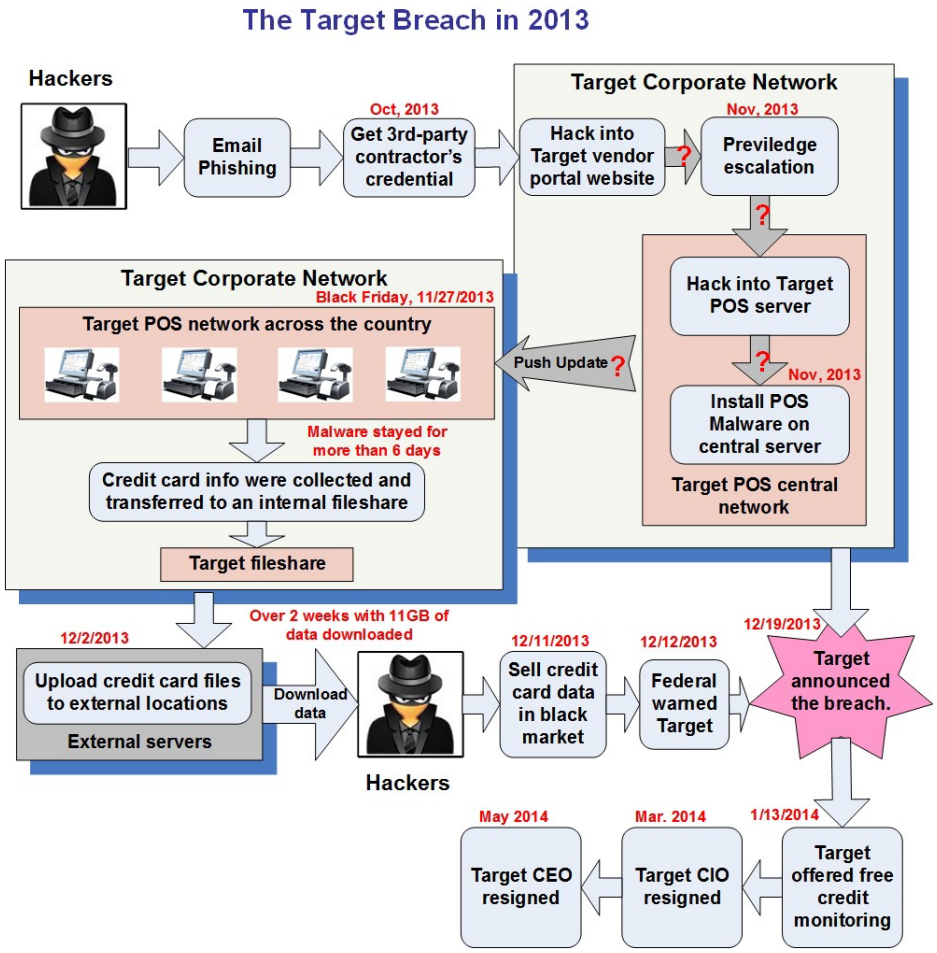

Figure 3. The Target data breach in 2013

There are two ways of using the Target case. First, we describe using an in-class discussion on the Target case during the semester where students answer questions and have round-table type discussions on the Target breach. Table 2 is a list of sample discussion questions on the Target case. Second, we use the Target breach as a real-world example when teaching individual security topics that are often abstract and can be difficult to conceptualize. Table 3 shows the corresponding security topics at the different stage of the Target case.

During case discussion, special attention is given to help students understand how different security mechanisms and systems are integrated into corporate networks, what the common weakest links are, and how those weakest links could be exploited by hackers. By walking through multiple case studies like the Target breach and the Anthem breach, students will obtain a holistic view of cybersecurity, and start to link many conceptual and abstract security topics together by understanding how they are applied to a real-world situation.

Another important point in case discussion is to guide students to pay special attention to human / social factors in today's complicated and global, yet somewhat fragile socio-technical cyber systems. Students will learn to consider multiple views on human, social, organizational, economic and technical factors and the complex interaction among these factors in real-world cases.

Table 2. Sample questions & answers for the in-class discussion on the Target breach

Discussion questions	**Key points in answers**
1) Use your own word to explain what happened in the Target data breach.	1) Open answer
2) The HVAC contractor's credentials were compromised by email phishing. Please propose at least two security mechanisms to guard against email phishing.	2) Email spam filter; phishing education
3) If you are the hacker, please propose a scheme for phishing email attack. Be as real as possible.	3) Open answer
4) The stolen credentials alone are not enough to access the company's POS devices. The hackers then acquired elevated rights that allowed them to navigate company's network and to deploy malware. This process is called Privilege Escalation. Name as many ways as you know to do privilege escalation.	4) SQL injection attack; buffer overflow attack; XSS attack; 0-day attack; weak or default password
5) For privilege escalation, the hackers need to do vulnerability scanning on the Target network. Please propose as many ways as you know to do vulnerability scanning?	5) Nmap; Nessus; penetration test
6) Many POS machines on the market nowadays are vulnerable to viruses and malware. Please propose a few measures to enhance POS security.	6) Internal firewall on POS network; malware detection
7) Target admitted that they ignored many alerts from their network security devices because of alert overload. If you are the Target CTO, what would you do to alleviate the problem of alert overload?	7) Upgrade security soft-ware; better training

8) The security experts criticize Target for failing to isolate sensitive sections of their networks from those more easily accessible to outsiders. If you are the Target CTO, please propose a feasible solution to segment and categorize your networks and resources.	8) Internal firewall and IDS; privileged account monitoring; network segmentation
9) IT Weaknesses Paved the Way for Target Hackers. Please identify as many weaknesses as possible in the Target IT security.	9) Open answer
10) If you are the Target CIO, what would you do to improve IT security?	10) Open answer

Table 3. Analysis of the Target data breach

Anatomy of the Target breach	**Corresponding cybersecurity topics**
Step 1. Hackers launched phishing attacks on Target 3rd-party contractor	Email phishing; Social engineering; Phishing education
Step 2. Hackers gained access to Target portal website with compromised credentials	Two-factor authentication; Access control; Firewall
Step 3. Privilege escalation within Target network	Vulnerability scanning; Common vulnerabilities: buffer overflow, SQL injection, XSS; Software patch management; Network segmentation
Step 4. Hackers gained control of Target POS server and installed Malware on POS machines	Privilege account management; User behavior analytics; Host hardening; Alert overloading
Step 5. Hackers collected credit card information with malware and stored data on an internal file share	Malware, virus, and worm
Step 6. Hackers downloaded stolen data from Target network	Firewall; Intrusion detection system
Step 7. Hackers sold credit card data on the black market	Security regulations; Risk analysis
Step 8. Target publicly announced the breach	Incident response; Penetration test

A list of case studies on cybersecurity

The authors have collected a set of cybersecurity breaches and plan to collect more in the future. Cases in Table 4 are comprehensive cases and should be covered with great detail and in-depth analysis. This is the scope of case analysis. Cases in Table 5 are short cases with fewer details (usually 10-15 minutes). The plan is to collect as many high-profile cyber breaches as possible and turn them into usable cases for a cybersecurity course. By having both lists available, instructors can customize courses and find an appropriate balance of covering many topics (scale) and spending the time to do a deep-dive analysis (scope) on fewer topics.

Table 4. Comprehensive cyber breaches

Case Studies	Referencing Materials and Links
1. The Target data breach in 2013	1. Michael Kassner. Anatomy of the target data breach, 2015. Available at http://www.zdnet.com/article/anatomy-of-the-target-data-breach-missed-opportunities-and-lessons-learned/. 2. KrebsonSecurity. Verizon security report on target, 2015. Available at https://krebsonsecurity.com/2015/09/inside-target-corp-days-after-2013-breach/.
2. The Anthem data breach in 2015	1. Inside Anthem: Dissecting the Breach. Available at https://www.youtube.com/watch?v=yB06EoE2lcw 2. California Department of Insurance. Regulatory Settlement Agreement on Anthem. Available at http://www.insurance.ca.gov/0400-news/0100-press-releases/2016/upload/Fully-Executed-RSA-2.PDF
3. DDoS attacks	1. Matthew Prince. Lessons from Surviving a 300Gbps Denial of Service Attack. Blackhat conference 2013. 2. Mirai IOT bonet in 2016. Available at https://www.incapsula.com/blog/malware-analysis-mirai-ddos-botnet.html

One of the potential downsides to case-based pedagogies is that students tend to focus too much on the idiosyncrasies of the particular case making it difficult for conclusions and lessons learned from any single case to be generalized in other case scenarios. Therefore it is suggested to compare and contrast multiple cases and scenarios in a course to help students extract and formulate new cross-case and generalizable concepts that can be applied to future situations and scenarios. For example: one of the discussion questions ask students to compare the Target breach and the Anthem breach and identify similarities and differences.

A study package with the following materials was developed for each case in the Table 4:

a) A video tutorial introducing the case (typically 30-40 minutes): students need to watch the video and get a basic idea of what happened in the breach before attending the classroom discussion

b) A list of discussion questions (typically ten): students need to finish the discussion questions after watching the video and before attending the classroom discussion. See Table 2 for example.

c) A PowerPoint presentation with technical details and lessons learned from the case (typically 30-50 pages): used by the instructor to guide the classroom discussion. Each case study will take one or two lectures, mixed with student discussion and instructor comment/lecture.

d) Selected readings from publicly available sources to provide students with an expanded awareness of topics. These selected readings can be either required assignment (graded), or optional (ungraded).

Table 5. Cyber breaches for individual topics

Case Studies	**Corresponding Topics**	**Referencing Links**
4. Mark Zuckerberg's social media accounts were hacked in 2016.	Password management, human factors	https://theringer.com/mark-zuckerberg-was-hacked-because-hes-bad-at-passwords-3c38514398b6
5. Panama paper breach in 2016.	Web server security, software patch management	http://www.forbes.com/sites/jasonbloomberg/2016/04/21/cybersecurity-lessons-learned-from-panama-papers-breach/
6. OpenSSL Heartbleed attack in 2014.	Zero-day attack, https security, buffer overflow	https://en.wikipedia.org/wiki/Heartbleed
7. An Internet-of-Things DDoS attack on Dyn DNS in 2016.	DDoS attack, security on Internet-of-Things	https://krebsonsecurity.com/2017/12/mirai-iot-botnet-co-authors-plead-guilty/
8. Ransomware on San Francisco public transportation in 2016.	Malware, Ransomware	http://arstechnica.com/security/2016/11/san-francisco-muni-hit-by-black-friday-ransomware-attack/
9. The JPMorgan data breach in 2014.	Email phishing, end-host hardening	https://en.wikipedia.org/wiki/2014_JPMorgan_Chase_data_breach

10. The SWIFT and Bangladesh bank hack in 2016.	Backdoor attack, malware	https://en.wikipedia.org/wiki/2015%E2%80%9316_SWIFT_banking_hack
11. Equifax data breach in 2017.	Web security; zero-day attack	https://en.wikipedia.org/wiki/Equifax
12. WannaCry ransomware in 2017.	Ransomware; zero-day vulnerability	https://en.wikipedia.org/wiki/WannaCry_ransomware_attack

Case studies in Table 5 typically take 10-20 minutes. The instructors can decide how to use them based on course content. Our plan is to collect as many high-profile cyber breaches as possible and turn them into usable cases for a cybersecurity course.

Lab assignments

Hands-on lab assignments are an important part of the HCA approach. The new cybersecurity course has 10 hands-on labs, designed to help student practice classroom theory and examples in a simulated virtual environment. Each lab session is designed to be successfully completed in a 2-hour block. We recommend using a cloud-based lab platform to provide virtual machines with multiple operating systems and other technical resources for students and instructors to have both a consistent and shared platform. Additionally, these virtual machines can be "quarantined" as to not allow any security research tools to affect other systems. There are many works in this field such as DETERlab, so we will not focus on the lab platform and setup.

These labs are designed based on the HCA principle with an emphasis on providing a simulated lab environment to allow students to mimic real-world breaches. Students will try to follow the footprint of hackers in high-profile cyber breaches. Students will explore common offensive and defensive cybersecurity techniques. Here is a list of lab topics.

Lab 1: Set up virtual machines for lab use
Objectives: get familiar with cloud-based virtual lab platform; be exposed to Windows and popular Linux distributions including Redhat(Fedora, CentOS), Kali, Ubuntu, and Debian.

Lab 2: Email phishing and social engineering
Objectives: explore different ways of sending phishing emails, such as PHP sendmail; play with email filters and try to bypass them; set up a phishing scheme.

Case study: students will be required to set up a phishing site and send out phishing emails to mimic the Target data breach.

Lab 3: Common web vulnerabilities
Objectives: explorer common web weaknesses; SQL injection attack; Javascript-based XSS attack; Javascript-based malicious code attack
Case study: students will be able to hack a WordPress site that mimics the Panama paper breach.

Lab 4: Network scanning and sniffing
Objectives: learn the initial step of hacking - reconnaissance; introduce methods of network scanning and sniffing such as NMAP, Xprobe2, p0f, Wireshark.

Lab 5: Vulnerability Scanning,
Objectives: learn methods of penetration test and vulnerability scanning in the simulated network; learn tools like Nessus, Nikto, and OpenVAS
Case study: students will be able to hack an Apache Struts 2 web server that mimics the Equifax data breach.

Lab 6: Password cracking
Objectives: learn password cracking with John the Ripper; learn Cain & Abel on Windows.

Lab 7: Spoofing and Man-in-the-Middle Attacks
Objectives: introduce ARP spoofing and man-in-the-middle attacks with Ettercap; introduce IP spoofing and MAC address spoofing;

Lab 8: Common backdoor attacks
Objectives: introduce "Swiss Army Knife" Crypcat; backdoor with Crypcat; ICMP-Backdoor; Metasploit to explore common backdoors.
Case study: students will hack into a self-contained, sandbox VM environment using backdoor malware.

Lab 9: Intrusion detection system (IDS)
Objectives: introduce a common open source IDS - Snort; setup and configure Snort.

Lab 10: Ethical hacking with Kali Linux
Objectives: learn the hacker's arsenal - Kali Linux which has hundreds of cybersecurity tools; use Kali Linux for penetration test; use Metasploit.
Case study: students will be able to simulate the EternalBlue vulnerability and the WannaCry ransomware with Metasploit.

COURSE ASSESSMENT RESULTS

The HCA model was developed and tested in a cybersecurity course at Michigan Technological University during the fall semester of 2015 and 2016, with a class of 20 students and 26 students respectively. The same cybersecurity course was taught in Fall 2014 with 16 students by using the traditional method. The group of 2014 was used as a comparison group for content knowledge assessment.

The summative course assessment was conducted on three components of the investigation: (1) changes in content knowledge, if any, associated with the instructional interventions; (2) student motivation and self-efficacy; (3) assessment of teacher instruction and pedagogical environment.

Assessment of content knowledge.

A pre-post design was used to assess student learning on content knowledge. Students were assessed using traditional tools such as labs, quizzes, and exams. The content knowledge assessment was conducted at both course-level and module-level. The assessment results provide ongoing feedback on student learning, as well as the success of the project in realizing its goals.

Students were asked to finish a pre-course survey at the beginning of the class to evaluate their technical background for the class of 2014, 2015 and 2016. The pre-course survey consisted of a set of student self-evaluation questions on cybersecurity knowledge and a set of technical questions to test student's understanding of prerequisite knowledge. There were no significant differences in student background when they entered the course for the classes of 2014, 2015 and 2016.

For post-course assessment, lab reports, mid-term exam and final exam were used to evaluate student's accomplishment of content knowledge. There are eight subject areas to assess: 1. cryptography; 2. phishing & web security; 3. access control; 4. IDS & DDoS; 5. firewall; 6. various offensive security methods; 7. various defensive security methods; 8. risk analysis & incident response. The subject of phishing & web security and risk analysis & incident response were not assessed in 2014. The assessment metric is the percentage of students who score 75% or higher. The result is shown in Table 6.

Table 6. Assessment of student content knowledge.
The metric is the percentage of students who score 75% or higher.

Topic	2014	2015	2016
1. Cryptography	82	81	88
2. Phishing & web security	N/A	87	96
3. Access control	71	87	77
4. IDS & DDoS	76	81	77
5. Firewall	65	61	70
6. Offensive security methods	81	87	96
7. Defensive security methods	77	81	96
8. Risk analysis & incident response	N/A	68	65

The grand average of assessment data on topic 1-8 shows slight improvement, as illustrated in Figure 4. Topic 6 and 7 cover comprehensive offensive and defensive security knowledge. Students show improvement in topic 6 and 7 as illustrated in Figure 4. While initial results appear promising, it is too early to attribute these improvement to the new teaching model. However, considering that the new HCA model covers more topics and study cases than the traditional model, the assessment results show that the new model at very least didn't sacrifice student performance for additional content and case studies.

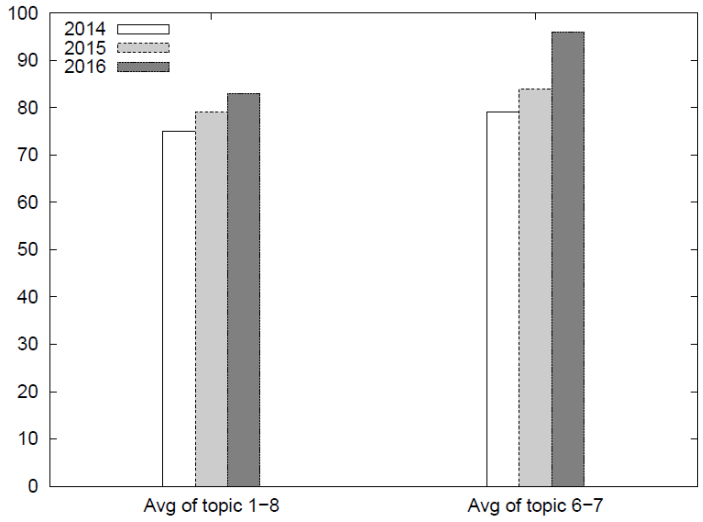

Figure 4. Avg of topic 1-8 and avg of topic 6-7 of student content knowledge.

Assessment of student motivation and self-efficacy.

Student feedbacks at the end of the course was very positive as students reported being motivated and actively engaged in classroom and lab activities. Student motivation and self-efficacy were improved as they were more confident in their abilities to tackle complicated cybersecurity breaches, as illustrated in Table 7.

Figure 5 shows the grand average of assessment data in Table 7 categorized into "Student motivation and interest" and "Student self-efficacy on analytical skills". It is observed that there were improvements in 2015 and 2016 (using case studies) in both categories compared with the 2014 baseline results (no case studies).

Table 7. Assessment of student motivation and self-efficacy on analytical skills. Using a Likert scale from 1 (Strongly Disagree) to 5 (Strongly agree).

Question	**2014**	**2015**	**2016**
Student motivation and interest			
This course was intellectually stimulating	4.3	4.6	4.5
This course has stimulated my interest in cybersecurity	4.2	4.5	4.4
I am more interested in the subject now than I was before I took this class	3.6	3.9	4.0
This course stimulated my enthusiasm for further learning in cybersecurity	4.0	4.5	4.5
Student self-efficacy on analytical skills			
This course helped me sharpen my analytical skills on cybersecurity problems	3.9	4.3	4.2
This course helped me develop problem-solving skills on cybersecurity problems	4.0	4.3	4.2
This course helped me identify the weakest link in an enterprise environment	N/A	4.0	4.2
This course helped me understand how the weakest link is exploited by hackers	N/A	4.4	4.3
This course helped me feel more confident about tackling cybersecurity problems	3.8	3.9	4.0

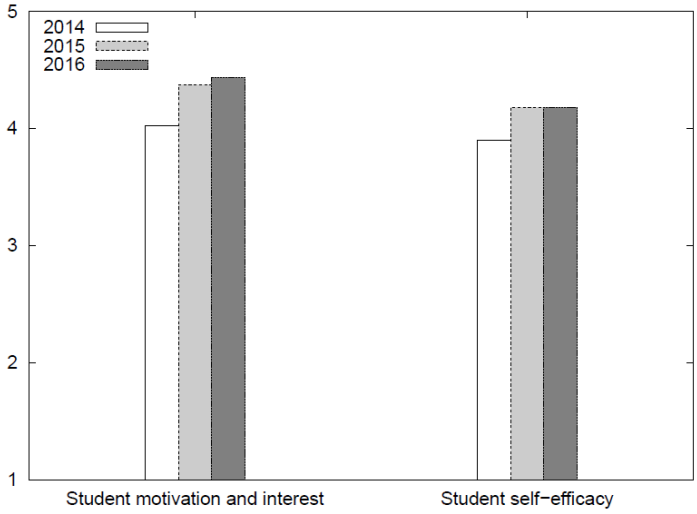

Figure 5. Grand average of student motivation/interest and self-efficacy.

Assessment of teacher instruction and pedagogical environment.

At the end of the course, students were asked to finish a survey for course evaluation covering several dimensions of the teaching and learning process. Students answer these questions on a Likert scale from 1 (Strongly Disagree) to 5 (Strongly agree). The classroom response rate was over 70% participation compared to the university average of 60-66%. Table 8 shows the assessment results for 2015 and 2016. Figure 6 shows the averages of these assessment results based on different categories. The assessment results show that students gave very positive feedback on case studies and the course.

Table 8. Course assessment.
Using a Likert scale from 1 (Strongly Disagree) to 5 (Strongly agree).

Question	**2015**	**2016**
Case study questions		
The case studies help my learning in this course	4.3	4.2
The case studies are thought-provoking	4.1	4.0
The case studies stimulate my interests in cybersecurity	4.4	4.3
The case studies help me understand what happened in the real world	4.7	4.6
The case studies helped me link security topics together	4.4	4.3
The case studies help me gain a holistic view of cybersecurity	4.2	4.1
The case studies helped me understand socio-technical factors	4.0	4.1

The case studies is one of my favorite parts of this course	4.1	4.0
Good teaching style		
The instructor was enthusiastic about the subject matter of the course	4.9	4.8
The instructor communicated the course material clearly	4.6	4.3
The instructor engaged students by encouraging participation during class	4.9	4.5
The instructor made the connection between the course material and the relevant industry	5.0	4.9
The instructor used technology appropriately	4.8	4.6
Course objectives		
I understood the goals and objectives of this course	4.8	4.4
The goals and objectives of this course were relevant to me	4.8	4.5
Appropriate workload		
My effort in this course was adequate to meet course objectives	4.8	4.4
I came prepared for each class session	4.7	4.1
The instructor engaged students by encouraging course preparation and reflection	4.7	4.5
General questions		
What do you think of the teaching pace for this course? (3 is at the right pace)	2.9	2.9
How difficult is this course? (3 is at the right difficulty level)	2.9	2.6
Overall		
Taking everything into account, I consider this course to be an excellent course.	4.8	4.7

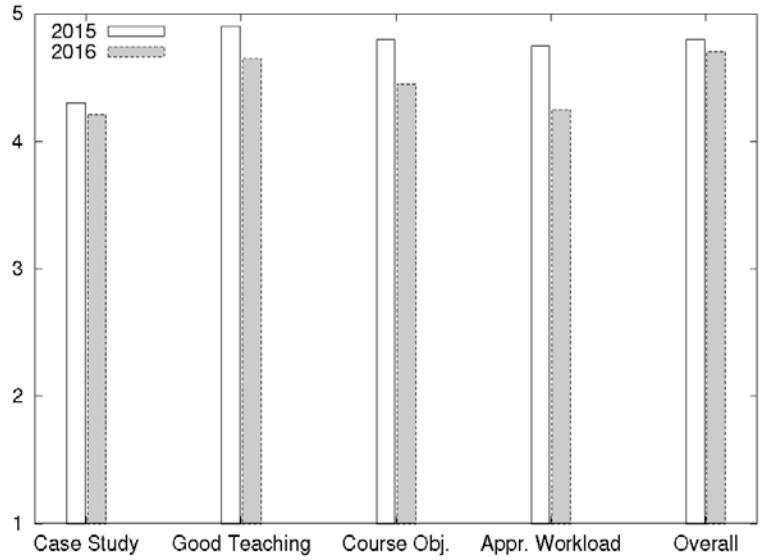

Figure 6. Averages of course assessment in 2015 and 2016, on a scale from 1 to 5, for assessment on Case Study, Good Teaching Style, Course Objectives, Appropriate Workload, and Overall evaluation.

CONCLUSION

This paper presents an HCA teaching model by dissecting high-profile cybersecurity breaches to teach cybersecurity courses. The successful outcomes of the proposed project has the potential to improve cybersecurity education. The case study materials developed in this project can be adapted and used in many other cybersecurity courses. The new HCA model will help to bridge the existing gaps between university education and industry need for real-world and practical understanding on cybersecuirty.

With the encouraging initial results, there are still many questions left open as stated in this paper. Therefore, furture analysis and assessments are needed to demonstate successful innovation in cybersecurity education through the proposed HCA model.

REFERENCES

Baumgartner, I. (2013), Using case studies to design and deliver technology-centered computing education courses: An innovative approach from an undergraduate information systems program in singapore, in 'Proceedings of the 18th ACM Conference on Innovation and Technology in Computer Science Education', ITiCSE '13

Bai, Y. and Wang, X. (2014). ITSEED: hands-on labs for it security education. In Proceedings of the 45th ACM technical symposium on Computer science education.

Berghel, H. (2017). Equifax and the latest round of identity theft roulette. Computer, 50(12):72–76.

Blackhat USA (2013). Lessons from surviving a 300gbps denial of service attack. Available at https://www.youtube.com/watch?v=w04ZAXftQ_Y.

Bratus, S. (2007). What hackers learn that the rest of us don't: Notes on hacker curriculum. IEEE Security & Privacy, 5:72–75.

Cai, Y. & Arney, T. (2017), Cybersecurity should be taught top-down and case-driven, in 'Proceedings of ACM SIGITE'.

Cyphort (2014). Dissecting the target breach. Available at https://www.youtube.com/watch?v=hiKoBxn3smY.

Christensen, C. R. (1981), Teaching By the Case Method, Harvard Business School, Boston, Massachusetts.

Cisco Report. (2015). Mitigating the cybersecurity skills shortage. Available at http://-www.cisco.com/c/dam/en/us/products/collateral/security/cybersecurity-talent.pdf.

CloudPassage (2016). Cloudpassage study finds u.s. universities failing in cybersecurity education. Available at https://www.cloudpassage.com/company/press-releases/cloudpassage-study-finds-u-s-universities-failing-cybersecurity-education/.

Denning, T., Lerner, A., Shostack, A., and Kohno, T. (2013). Control-alt-hack: The design and evaluation of a card game for computer security awareness and education. In Proceedings of the 2013 ACM SIGSAC Conference on Computer & Communications Security, pages 915–928.

Doupé, A., Egele, M., Caillat, B., Stringhini, G., Yakin, G., Zand, A., Cavedon, L., and Vigna, G. (2011). Hit 'em where it hurts: A live security exercise on cyber situational awareness. In Proceedings of the 27th Annual Computer Security Applications Conference, pages 51–61.

Du, W. (2011). SEED: Hands-on lab exercises for computer security education. IEEE Security & Privacy, 9:70–73.

Estes, T., Finocchiaro, J., Blair, J., Robison, J., Dalme, J., Emana, M., Jenkins, L. & Sobiesk, E. (2016), A capstone design project for teaching cybersecurity to non-technical users, in 'Proceedings of the 17th Annual Conference on Information Technology Education', SIGITE '16, ACM, New York, NY, USA, pp. 142–147.

Gorka, S., McNett, A., Miller, J. R. & Webb, B. M. (2017), Improving the pipeline: After-school program for preparing information assurance and cyber defense professionals, in 'Proceedings of the 18th Annual Conference on Information Technology Education', SIGITE '17, ACM, New York, NY, USA, pp. 167–167.

Jin, G., Tu, M., Kim, T.-H., Heffron, J. & White, J. (2018), Game based cybersecurity training for high school students, in 'Proceedings of the 49th ACM Technical Symposium on Computer Science Education', SIGCSE '18, ACM, New York, NY, USA, pp. 68–73.

Kerven, D., Nagel, K., Smith, S., Abraham, S. & Young, L. (2017), Scenario-based inquiry for engagement in general education computing, in 'Proceedings of the 2017 ACM SIGCSE Technical Symposium on Computer Science Education', SIGCSE '17, ACM, New York, NY, USA, pp. 303–308.

Kassner, M. (2015). Anatomy of the target data breach. Available at http://www.zdnet.com/article/anatomy-of-the-target-data-breach-missed-opportunities-and-lessons-learned/.

KrebsonSecurity (2015). Verizon security report on target. Available at https://krebsonsecurity.com/2015/09/inside-target-corp-days-after-2013-breach/.

Kreber, C. (2001), 'Learning experientially through case studies? a conceptual analysis', Teaching in Higher Education 6(2), 217–228.

LeTellier, V. (2016). The Argument for Holistic Cybersecurity. Available at https://-www.securitymagazine.com/blogs/14-security-blog/post/87239-the-argument-for-holistic-cybersecurity.

Margolis, J., Oh, T. T., Jadhav, S., Jeong, J. P., Kim, Y. H., and Kim, J. N. (2017). Analysis and impact of iot malware. In Proceedings of the 18th Annual Conference on Information Technology Education, SIGITE '17, pages 187–187, New York, NY, USA. ACM

Mitchell, J. E., Qiu, J., Canonio, M., Jha, S., Hayden, L., O'Leary, B. A., Figueiredo, R. & Fox, G. (2012), Futuregrid education: Using case studies to develop a curriculum for communicating parallel and distributed computing concepts, in 'Proceedings of the 1st Conference of the Extreme Science and Engineering Discovery Environment: Bridging from the eXtreme to the Campus and Beyond', XSEDE '12, ACM, New York, NY, USA, pp. 61:1–61:5.

NCCDC (2016). Collegiate Cyber Defense Competition. Available at http://nationalccdc.org.

Hult News. (2015), 'Experience is the best teacher : A case in point'. Available at http://-www.hult.edu/news/experience-is-the-best-teacher/.

ISACA report. (2016). State of cybersecurity. Available at https://www.isaca.org/cyber/-Documents/state-of-cybersecurity_res_eng_0316.pdf.

Peterson, P. A. H. and Reiher, P. L. (2010). Security exercises for the online classroom with deter. In Proceedings of the 3rd International Conference on Cyber Security Experimentation and Test, pages 1–8.

Peninsula Press. (2015). Demand to fill cybersecurity jobs booming. Available at http://-nsulapress.com/2015/03/31/cybersecurity-jobs-growth/.

Prince, M. (2013). Lessons from surviving a 300gbps denial of service attack. Blackhat USA.

Soy, S. K. (1997), 'The case study as a research method'. Available at https://-www.ischool.utexas.edu/~ssoy/usesusers/l391d1b.htm.

Stanford University Newsletter on Teaching (1994), 'Teaching with case studies'. Available at https://web.stanford.edu/dept/CTL/Newsletter/case_studies.pdf.

Trabelsi, Z. and Ibrahim, W. (2013). Teaching ethical hacking in information security curriculum: A case study. In Proceedings of the 2013 IEEE Global Engineering Education Conference (EDUCON).

US Senate Report (2014). A kill chain analysis of the 2013 target data breach.

Wilson, B. (2017), 'Teaching security defense through web-based hacking at the undergraduate level', J. Comput. Sci. Coll. 33(2), 121–128.

Wiki on Anthem (2015). Anthem medical data breach. Available at https://en.wikipedia.org/wiki/-Anthem_medical_data_breach.

Weiss, R. S., Boesen, S., Sullivan, J. F., Locasto, M. E., Mache, J., and Nilsen, E. (2015). Teaching cybersecurity analysis skills in the cloud. In Proceedings of the 46th ACM Technical Symposium on Computer Science Education, pages 332–337.