Source: Screencapped.net

An Educator's' Guide to Internet Privacy using Mr. Robot

By Allison Nellis

LIS 611

Spring 2016

Table of Contents

Research Question/Introduction:

Over the course of the ten episodes that make up the first season of Mr. Robot’s focuses on several technology and privacy issues that are prevalent in today's society. This study guide will discuss the privacy issues on the individual and corporate level that occur throughout the series. This guide will also inform teachers and students of the specific laws that are associated with some of the privacy issues and breeches featured in the show, such as HIPAA laws for medical privacy, Remote Access Trojans (RAT) and how security systems are exploited that result in these issues. This guide will also provide teachers with talking points and questions that will help facilitate a meaningful post viewing discussion in the classroom.

Summary of Mr. Robot:

Mr. Robot follows Elliot Alderson, an engineer at a major cyber security company called Allsafe, as he is recruited by an underground hacker group known as F-Society as they plan to take down Elliot’s employer’s biggest client, tech conglomerate E-Corp. Over the course of Mr. Robot’s first season, sees Elliot not only use his skills as a hacker to carry out F-Society’s plan but to also lurk into the private lives of his loved ones. *Mr. Robot* premiered during the summer of 2015 with season one consisting of ten episodes. The show’s creator Sam Esmail intends for the show to cover the most up to date issues involving the tech world, which includes the Sony/Ashley Madison Hacks and Encryption services.

Objective:

By studying Mr. Robot in the context of this class, students will familiarize themselves with several issues that are relevant today. Through the reading of the foundational material provided later in this guide, students will develop a knowledge of some of the issues brought up in the show. Through this guide, educators will have a starting point in which they can incorporate Mr. Robot into their syllabus as a valuable learning tool. By the end of exercises included in this guide, students will be able to determine if television shows/movies can accurately portray current cybersecurity issues.

Foundational Readings:

Here educators will find resources in which they can begin to introduce Mr. Robot to their students. The readings and videos found here relating directly to the show should be supplementary to the students viewing Season 1. There are also resources relating to some of the basic legislation that the show and this study guide touches on.

Esmail, S. (March, 2016) *Coding on Camera: MR. ROBOT and Authenticity on TV | SXSW Convergence 2016.* Retrieved from: https://youtu.be/m3qgdEXN06E
As part of the 2016 SXSW festival, this panel included *Mr. Robot's* created Sam Esmail and lead actors Rami Malek and Christian Slater discussing the depiction of technology and hacker culture in mainstream media. The panelist also discusses the influences behind the show and the technological issues that become recurring themes in later seasons.

Grimes, R. (2002, September). Danger: Remote Access Trojans. Retrieved April 03, 2016, from https://technet.microsoft.com/en-us/library/dd632947.aspx
Grimes' article on Remote Access Trojans (RAT) will give students a foundational knowledge of this online security issue. Grimes details the different types of RAT's and how to remove them from a computer system. It is worth noting that this article was published in 2002, but is still a valuable resource for anyone wishing to gain insight on this issue.

Jones, R. (2015). *Mr. Robot: Every title and episode, explained*. Retrieved April 03, 2016, from: http://www.hopesandfears.com/hopes/culture/television/216489-mr-robot-episodes-titles-explained
Jones provides one of the most comprehensive breakdowns of each episode of Mr. Robot, and with the help of Information Security expert Peter Yeh explains some of the more technological aspects of the series in a easily digestible format. Along with a summary of each episode, there is a detailed explanation as to how the title of the episode relates to the plot and the characters.
http://us.practicallaw.com/6-502-0467

Practicallaw (2015, July.) *Data protection in United States: Overview. Retrieved April 03, 2016, from* http://us.practicallaw.com/6-502-0467
This brief summary of relevant legislation for data protection in the United States can be used as a starter resource for any student wishing to learn about information policy. This site covers everything from the specifics of the laws to the rights of the individual. There is also a resource page at the end of the article is students wish to learn more about a particular law.

Introduction of Specific Issues Covered in the Study Guide:

Although several issues are brought up during the first season of Mr. Robot, this study guide will only cover three. The three issues to be covered are as follows: Corporate cyber security (relating to large corporations such as Google that hold a variety of information about their customers), personal cyber security/privacy risks (such as the leaking of medical information, financial information, and social media/email services), and remote access trojans (otherwise known as RAT).

Summary of Issues within Mr. Robot with Examples and Case Law:

Corporate Cyber Security

Episodes that cover this issue: Every episode in Season 1

The main focus of season 1 of Mr. Robot is F-Society's mission to bring down E-Corp and clear all of the financial debts held by it's users. E-Corp is a technology giant that controls a majority of the world's finances and technology production (with the creation of phones, computers, and tablets). Throughout the season there are several major security breaches against E-Corp including the leak of incriminating emails and attempts to destroy their records kept in an iron mountain-esque facility.

Literature:

1. Edwards, A. V. (2015). *Digital is destroying everything: What the tech giants won't tell you about how robots, big data, and algorithms are radically remaking your future*.

   In Andrew Edwards' book, he argues that the conversion to a digital society has negatively impacted us as a society. Edwards discusses how the digital world has all but destroyed certain industries, such as the music business. He also discusses how the switch to a digital society has been used to the advantage of large corporations to collect data on their users in order to better serve their customers, but also put them at risk in the event of a cyber attack. Edwards also discusses how the digital world has shifted the way we elect our leaders, how we view higher education, and how going digital gives others the authoritative rule over our lives.

2. Piggin, R. (2016-02). *Cyber security trends: What should keep CEOs awake at night. International journal of critical infrastructure protection.* doi:10.1016/j.ijcip.2016.02.001

   In this article, Piggin charts out the trends in cyber attacks against large corporations in recent years. Piggin argues that hackers are not just going after governmental infrastructure, he gives the example of a cyber attack in late 2015 taking out the electricity in half of the homes in the Ukraine, but also big corporations who hold large sets of data relating to their customers. Piggin also reviews the security systems that some of these big corporations have in place and if they are suited to protect the sensitive data that they have collected.

3. Powers, S. (2015). Google, Information, and Power. In *The Real Cyber War: The Political Economy of Internet Freedom* (pp. 74–98). University of Illinois Press. Retrieved from http://www.jstor.org/stable/10.5406/j.ctt130jtjf.8

   In this article Shawn Powers discusses how technology giant Google is actively trying to protect the privacy and safety of its users. Powers discusses Google's political power in the debate over freedom of speech on the internet. Google is on the front line when it comes to cyber warfare, and Powers discusses the courses of action Google takes to protect themselves and their users.

Laws that have been violated:
As with all of the hacking incidents that come up in *Mr. Robot*, 18 U.S. Code § 1029 is being violated by Elliot and F-Society. 18 U.S. Code § 1029 covers fraudulent access to device connections, which include computer systems and personal devices. This U.S. Codes detail that the accused needs to knowingly commit these fraudulent actions in order to be tried.

As of the publishing of this study guide, there is currently a bill being reviewed by the Senate that would protect E-Corp's customers during a security breach. During the 114th Congress, a the Consumer Privacy Act was proposed that is aimed at protecting the consumer against any information obtained during a security breach. This would include any personal or financial information that is leaked that could be further used by hackers to steal identities. This bill would also forbid corporations from concealing such security breaches from their customers.

Since E-Corp is also acting as a financial institution, there are another set of laws that would apply to this situation, 18 U.S. Code § 1030, which is now part of the Computer Fraud and Abuse Act, which protects the computers of the Federal Government and Financial Institutions, both seen as protected entities in the eyes of the law.

Case Law/Recent Examples:
JP Morgan Chase Data Breach
Background:
In July of 2014, a group of hackers exploited a flaw on a JPMorgan Chase in order to tap into the data of the bank's 76 million customers. The security breach was not reported to the public until September 2014. Hackers collected data including social security numbers, addresses, emails, and phone numbers. Along with hacking into Chase, the hackers broke into multiple banks and collected over 80 million records in total.

Outcome: In November 2015, four men were indicted in relation to the hacking. Gery Shalon, Joshua Samuel Aaron, Zic Orenstein, and an unidentified fourth man were charged with unauthorized access to computers, wire fraud, and identity theft.

Sony Entertainment Email Scandal
Background:
In November of 2014, a hacker group calling themselves the Guardians of Peace began leaking sensitive information relating to Sony Entertainment. The information included sensitive HR related documents, personal emails, incriminating emails between employees, and entire films that were yet to be released. The hacker group claimed to have over 100 terabytes of data in their possession that was obtained through malware, speculation says the malware was installed through a phishing email.

Result: As of 2016 no one was officially charged for the hack, but there is much speculation that the hack came from North Korea. In response to this situation, President Obama issues a proposal to congress to amend the Racketeer Influenced and Corrupt Organizations Act (RICO) to include cyber crimes and to protect those affected by them.

Fig 1. From episode “1.07 V1ew-S0urce.Flv” in which Elliot visualizes all of the personal information he’s collected from his colleagues.

Personal Cyber Security/Privacy
Episodes that cover this issue: Every episode in Season 1
During the entire series Elliot uses his skills as a hacker to plug into the private lives of his loved ones. He uses this information to his advantage to manipulate certain situations to his advantage, using his friend’s medical records, private correspondences, social media accounts,

and banking records to gain the upper hand. One of the most explicit examples of this comes during episode 7 "eps1.6_v1ew-s0urce.flv". During a session with his therapist Krista, Elliot reveals all of the personal information he's collected on here. This includes monitoring her credit card activity (telling her he knows she buys her coffee every morning on her credit card and justifying it because the card gives her points), saying how she has a prescription for antidepressants but never fills it, and watching her via her webcam. Elliot is also known to snoop on his best friend Angela by checking her emails, text messages, and social media messages in order to gain insight into her personal life.

Literature:

1. Richards, N. (2015). *Intellectual privacy : Rethinking Civil Liberties in the Digital Age.*Oxford, UK: Oxford University Press.

   In this book, Neil Richards discusses the changing attitudes regarding privacy in recent years. With the rising of social media, the general public appears to become more comfortable with divulging personal information with a wider audience. But when does this become a problem? Richards discusses when we should consider certain situations a violation or privacy. The role of surveillance in our everyday lives, and especially on the internet, is a recurring theme throughout Richards' book. Richards also touches on issues regarding freedom of speech becoming interwoven with freedom of privacy.

2. Snyder, C. (2015). Handling Human Hacking: Creating a Comprehensive Defensive Strategy Against Modern Social Engineering.

   In this article Charles Snyder discusses the threat of a single person manipulating a person or organization/company in order to gain access. Snyder argues that hackers take on personalities in order to gain the trust of someone in a company's security team. By targeting a company on a one on one basis creates a larger security threat than a full scale DDoS attack. Hackers can utilize social media as part of their arsenal when choosing a victim and collecting data in order to create a fake persona. Snyder outlines a plan of defense that companies can adopt in order to protect themselves from what he calls "social engineers."

What laws have been violated:
Certainly in the cases where health related information is being collected and in cases used to Elliot's advantage is a violation of Health Insurance Portability and Accountability Act (HIPAA). HIPPA protects the right to confidentiality between an individual and their healthcare provided in terms of their medical history. Elliot hacked into Krista's health insurance records in order to determine that what prescriptions she has and whether or not she's filled them. Which would be information that only Krista and her doctor would be entitled to.

Another law that Elliot violated when snooping on his loved ones and colleagues is the Electronic Communications Privacy Act (ECPA). By intercepting the electronic communications of his friends he could be held accountable for Title II of the ECPA which protects messages on stored devices, for example text messages stored on a cellphone and email messages. The Consumer Privacy Protection Act of 2015, which has yet to pass through congress, can also be applied to these situations since this piece of legislation protects individuals who are the victims of identity theft and who have had information stolen under organizational/corporate security breaches. Elliot has breaks laws relating to fraudulent activity on personal devices which is discussed in further detail in the next section on Remote Access Trojans.

Case law/recent examples:
United States vs. Councilman
Background: Bradford C. Councilman of Interloc, INC managed a rare book list serv and provided email addresses to users under his own domain interloc.com. In 1998 Councilman instructed Interloc employees to intercept and store messages between users and Amazon.com. These messages were used to exploit the business being conducted in these messages and to gain personal information on Interloc's users. Councilman was accused of violating Wiretap Act, 18 U.S.C. § 2511, which prohibits the interception of wire, oral, or electronic communications. Councilman argued that emails were electronic storage, and at the time were not protected under the law.

Verdict: The case was dismissed in 2007 when the employees who testified that they were instructed to keep the emails were found to be unreliable.

Department of Justice vs. Joshua Hippler
Background: Between December 2012 and January 2013, Joshua Hippler collected medical records from an undisclosed health facility in which he was employed in order to use the records for personal gain. What separated this case apart from other HIPAA violation cases was the intention of the records once they were in Hippler's hands, he was found to be attempting to use said records for personal and even criminal usage.

Verdict: Hippler was sentenced to 18 months in a federal prison and ordered to pay $12,500 in restitution.

New Jersey vs. Dharun Ravi
Background: In September of 2010, Rutgers University freshman Tyler Clementi was spied on by his roommate Dharun Ravi on two different occasions engaged in intimate situations with a fellow male student. Ravi had spied on his roommate via his webcam, in which he had turned on remotely because he was worried about theft. After Ravi had seen the first incident, he broadcasted on his twitter page what he had witnessed and outed his roommate on the social media site. The second incident on September 21st involved Ravi planning to broadcast Clementi engaged in a sexual attack in the boy's bedroom, but decided not to when Clementi discovered the camera and unplugged it. Clementi filed reports with the resident assistant of his

dorm citing that he wished to be moved to a single room due to this invasion of privacy. On September 22nd, Clementi committed suicide. On September 28th, Ravi and an accomplice were charged with four counts of invasion of privacy.

Verdict: On March 16th, 2012 Ravi was found guilty of invasion of privacy, bias intimidation, and hindering apprehension. During a later sentencing hearing Ravi was sentenced to 30 days in jail, three years probation, a $10,00 fine, counseling on cyberbullying, and 300 hours of community service.

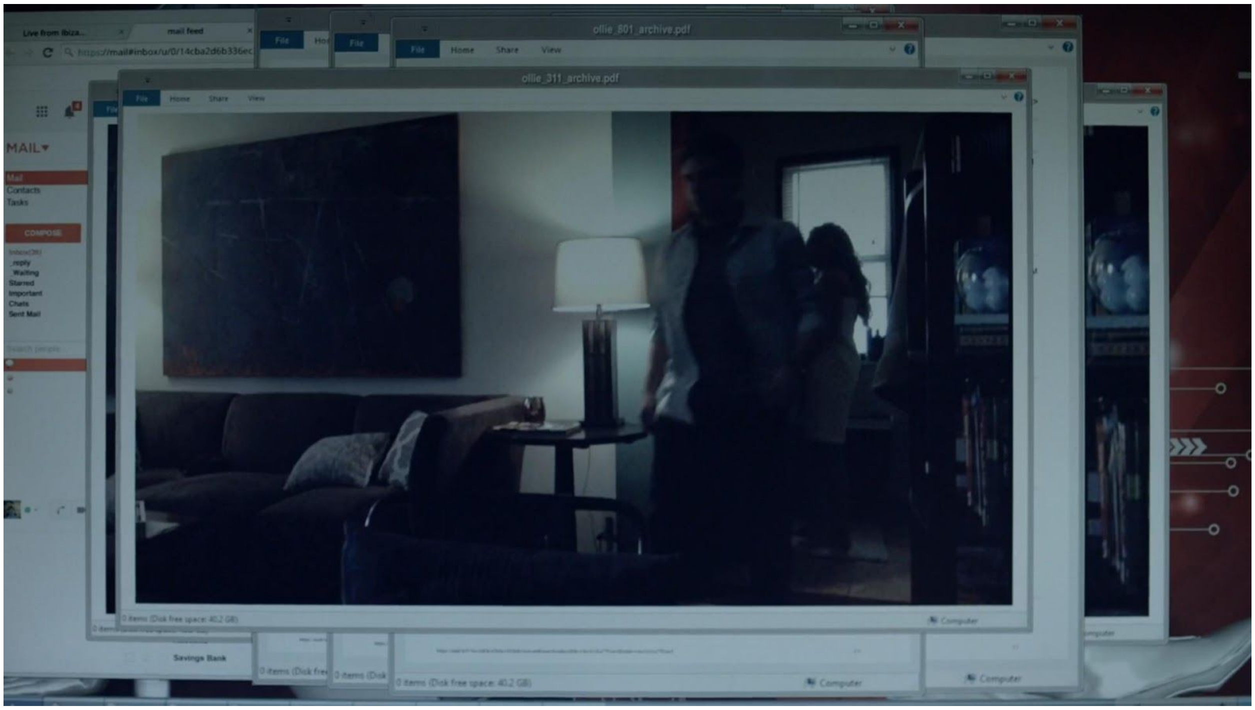

Fig 2. From episode“eps1.3_da3m0ns.mp4” Ollie’s Computer Activity Being Tracked by Hackers.

Remote Access Trojans/Hacking and Surveillance
Episodes that cover this issue: “eps1.2_d3bug.mkv” and “eps1.3_da3m0ns.mp4”
During the first half of the series Ollie, Angela’s boyfriend and also an Allsafe employee, accidentally installs a remote access trojan on his personal pc after accepting demo cd from a hacker named Cisco who is a liaison to the Chinese hacker group the Dark Army. Cisco is disguised as a street performer handing out music demo cds on the street. Ollie assuming that the cd handed to him would consist of only amateur rap music, unknowlingly installs a remote access trojan onto his personal computer. The hacker group uses information found on Ollie’s computer to blackmail him into installing a virus onto Allsafe’s system. The hacker group threatens to use personal emails, photos, and dating website info to destroy his relationship with his girlfriend.

Literature:

1. V. K. Gudipati, A. Vetwal, V. Kumar, A. Adeniyi and A. Abuzneid, "Detection of Trojan Horses by the analysis of system behavior and data packets," Systems, Applications and Technology Conference (LISAT), 2015 IEEE Long Island, Farmingdale, NY, 2015, pp. 1-4. doi: 10.1109/LISAT.2015.7160176

   In this article, the severity of the threat of trojans on the casual computer is discussed. Trojans have the ability to conceal themselves so well into a home computer that the user does not know that they're settings have been changed or that a trojan has been installed. The article goes into detail on the science behind how trojans are able to do this and transmit your personal data to hackers without your knowledge.

2. N. Hoque, Monowar H. Bhuyan, R.C. Baishya, D.K. Bhattacharyya, J.K. Kalita. *Network Attacks: Taxonomy, Tools and Systems.* Journal of Network and Computer Applications, Volume 40, April 2014, Pages 307-324, ISSN 1084-8045, http://dx.doi.org/10.1016/j.jnca.2013.08.001. (http://www.sciencedirect.com/science/article/pii/S1084804513001756)

   Network Attacks: Taxonomy, Tools and Systems is an essential article not only for students but also for anyone who is working in the cybersecurity field. This article provides readers with a baseline knowledge of the different tools utilized by hackers for cyber warfare. The authors also provide readers with a plan of defense in case their systems are ever the target of a large scale attack.

3. Warner, M. The Shadow War. (2014). The Shadow War. In *The Rise and Fall of Intelligence: An International Security History* (pp. 280–332). Georgetown University Press. Retrieved from http://www.jstor.org/stable/j.ctt6wpkvt.15

   In this chapter of Michael Warner's book *The Rise and Fall of Intelligence: An International Security History*, Warner argues that the greatest threat to the country post 9/11 comes from cyber warfare. Warner details the rise of what the calls "the shadow war" from the weeks following 9/11 to recent years. Warner puts cyber hacking in an international scope to describe the security situations that have faced other countries, such as England and Israel, in the past decade. Warner covers the different types of cyber issues from surveillance of citizens to direct attacks on governmental institutions.

What laws have been violated:
The use of Remote Access Trojans are not directly addressed in legislation but the action of installing RAT's on the personal devices of unknowing individuals can be covered under Federal Law 18 U.S. Code § 1029. This section under chapter 47 of Title 18 covers fraud and activity of connected devices. The code indicates that anyone intentionally takes control over a device in order to commit fraud is in violation of this law. As in our previous case of personal privacy

violation, the Electronic Communications Privacy Act can also be applied here since Ollie's personal information was compromised and is being threatened to be made public.

Case law/Recent examples:
Robbins vs. Lower Merion School District
Background: During the 2009-2010 school year the Lower Merion High School and Harrington High School, located in the Ardmore suburb of Philadelphia, distributed Macbook laptops to each of their combined 2,300 student body.The laptops provided by the schools were meant to be used at home and in class. On each of the laptops the tracking software LANrev was installed, along with the TheftTrack program. The school's officials had chosen to activate the TheftTrack program in order to gain access to the student's webcams and take screenshots of the student's computer activity. It is worth noting that the settings on the computer prohibited the students from using the laptop's camera settings, as in using photobooth or using the webcam for chatting. The lawsuit involved high school sophomore Blake J. Robbins, who in October of 2009 had 210 webcam shots and 218 screenshots taken of him and his online activity without his consent by school officials. These images included instant messages and photos of the student undressed. Robbins had become aware of these violations when a school staff member reprimanded the student's home behavior. The lawsuit cited that the school district was in direct violation of Electronics Communications Privacy Act. In February of 2010 U.S District Court Judge for Pennsylvania Jan DuBois ordered the school district to cease the surveillance of students through the school issues laptops.

Verdict: In April 2010, the court ruled in favor of the student and awarded Robbins a settlement of $610,000.

Discussion Questions and Exercises:

General Post Viewing Questions/Discussion Starters:

1. What cyber offense is being committed here?
2. Is it against the law?
3. What are some of the ethical implications of these crimes?

Group Activity:

1. What kind of security threat is this? (Corporate or Personal)
2. What information is being access?
3. Who is being exploited?
4. How has this information been obtained?

After answering the questions above, each group should take 20 minutes to create a plan of action to correct what has happened and to protect the individual or corporation from it ever happening again

Bibliography:

Bauman, Z., & Lyon, D. (2013). *Liquid surveillance: A conversation*. Cambridge, UK: Polity.

Department of Justice (2015, March 05).*Former Hospital Employee Sentenced for HIPAA Violations*. Retrieved April 04, 2016, from https://www.justice.gov/usao-edtx/pr/former-hospital-employee-sentenced-hipaa-violations

Doonan, M. HIPAA: Federalism and Implementation. (2013). HIPAA: Federalism and Implementation. In *American Federalism in Practice: The Formulation and Implementation of Contemporary Health Policy* (pp. 84–98). Brookings Institution Press. Retrieved from http://www.jstor.org/stable/10.7864/j.ctt4cg7p2.10

Edwards, A. V. (2015). *Digital is destroying everything: What the tech giants won't tell you about how robots, big data, and algorithms are radically remaking your future*.

Hathaway, O. A., Crootof, R., Levitz, P., Nix, H., Nowlan, A., Perdue, W., & Spiegel, J.. (2012). The Law of Cyber-Attack. *California Law Review*, *100*(4), 817–885. Retrieved from http://www.jstor.org/stable/23249823

Keizer, G. (February 18). *Pennsylvania Schools Spying on Students using Laptop Webcams, Claims Lawsuit*. Retrieved April 04, 2016, from http://www.computerworld.com/article/2521075/windows-pcs/pennsylvania-schools-spying-on-students-using-laptop-webcams--claims-lawsuit.html

Koenigs, M., Smith, C., & Ng, C. (2012, May 21). *Rutgers Trial: Dharun Ravi Sentenced to 30 Days in Jail*. Retrieved April 04, 2016, from http://abcnews.go.com/US/rutgers-trial-dharun-ravi-sentenced-30-days-jail/story?id=16394014

Kravets, D. (2010, April 06). *School District Allegedly Snapped Thousands of Student Webcam Spy Pics*. Retrieved April 04, 2016, from http://www.wired.com/2010/04/webcamscanda

N. Hoque, Monowar H. Bhuyan, R.C. Baishya, D.K. Bhattacharyya, J.K. Kalita, Network attacks: Taxonomy, tools and systems, Journal of Network and Computer Applications, Volume 40, April 2014, Pages 307-324, ISSN 1084-8045, http://dx.doi.org/10.1016/j.jnca.2013.08.001. (http://www.sciencedirect.com/science/article/pii/S1084804513001756)
Keywords: Network attacks; Tools; Systems; Protocol; DoS

Piggin, R. (2016-02). Cyber security trends: What should keep CEOs awake at night. International journal of critical infrastructure protection doi:10.1016/j.ijcip.2016.02.001

Powers, S. (2015). Google, Information, and Power. In *The Real Cyber War: The Political Economy of Internet Freedom* (pp. 74–98). University of Illinois Press. Retrieved from http://www.jstor.org/stable/10.5406/j.ctt130jtjf.8

Richards, N. (2015). *Intellectual privacy : Rethinking civil liberties in the digital age.*Oxford, UK: Oxford University Press.
Snyder, C. (2015). Handling Human Hacking: Creating a Comprehensive Defensive Strategy Against Modern Social Engineering.

Seal, M. (2015, February). *Sony's Hacking Saga over The Interview; Seth Rogen and Evan Goldberg Speak Out*. Retrieved April 04, 2016, from http://www.vanityfair.com/hollywood/2015/02/sony-hacking-seth-rogen-evan-goldberg

V. K. Gudipati, A. Vetwal, V. Kumar, A. Adeniyi and A. Abuzneid, "Detection of Trojan Horses by the analysis of system behavior and data packets," *Systems, Applications and Technology Conference (LISAT), 2015 IEEE Long Island*, Farmingdale, NY, 2015, pp. 1-4. doi: 10.1109/LISAT.2015.7160176

Warner, M. The Shadow War. (2014). The Shadow War. In *The Rise and Fall of Intelligence: An International Security History* (pp. 280–332). Georgetown University Press. Retrieved from http://www.jstor.org/stable/j.ctt6wpkvt.15

Zetter, K. (2015, November 15). *Four Indicted in Massive JP Morgan Chase Hack*. Retrieved April 04, 2016, from http://www.wired.com/2015/11/four-indicted-in-massive-jp-morgan-chase-hack/