Movies as an aid to teach principles of Cybersecurity and Cybercrime in Higher Education

Antonios Andreatos
Dept. of Aeronautical Sciences
Div. of Computer Engineering & Information Science
Hellenic Air Force Academy
Dekeleia Air Force Base
Dekeleia, Attica, 13671
antonios.andreatos@hafa.haf.gr, aandreatos@gmail.com
Greece

Received: August 18, 2020. Revised: September 14, 2020. Accepted: September 17, 2020.
Published: September 24, 2020.

Abstract- A pilot effort to raise students' awareness on the human factors of cybersecurity and cybercrime is presented. One day, instead of lectures, a commercial film was projected. The students were able to identify most of the cyberattacks related to the technical background given in the course, while they missed some of the frauds committed by the actors, related to the psycho-social and legal dimensions, which were not covered in the syllabus. The students had the opportunity to acquire some insight about the latter while enjoying the movie. The whole experiment was evaluated positively. Thus, it became clear to the students that cybersecurity has also a psycho-social dimension which should not be underestimated

Keywords- Network Security course, Cybersecurity, Cybercrime, Psycho-social dimension, Movie, Higher Education

I. Introduction

A. *The need for cybersecurity education*

INCREASING demand for security experts has motivated many universities to embed security courses in Engineering and Computer Science curricula. Following this trend, a Network Security course has been introduced in the 4th year of the undergraduate program of the Telecommunications and Electronics Engineering students of the Hellenic Air Force Academy (HAFA), about thirteen years ago. This specialization is equivalent to a Bachelor degree in Electrical Engineering, therefore, the Network Security course has technological orientation [1].

The material is covered in lectures, class demonstrations, assignments and lab exercises. Junior and senior students also participate in annual national and international cyber defense exercises. Specialists and professionals are often called to deliver lectures and presentations.

Participation in cyberdefense exercises set a wide background of domains including mobile computing, criminology/forensics, communications intelligence, imagery intelligence, human-computer interaction, information retrieval, information theory, management/ business, military science, ethics, psychology, etc.

Humans play the most crucial role in cybersecurity and often make the weakest link in the security chain [2]. There is a growing recognition that technical cyber security measures do not exist in a vacuum and need to operate in cohort with people [3]. Students not only need to acquire technical knowledge about cyberdefense, they should also be the carriers of a cyberdefense culture within their future organization. There is another reason why our students should acquire this knowledge: because they will become military officers. According to Sun Tzu, an ancient Chinese military strategist, author of the famous book “The Art of War”, a classic military treatise written circa 5th century BC:

> “If you know the enemy and know yourself, you need not fear the result of a hundred battles. If you know yourself but not the enemy, for every victory gained you will also suffer a defeat. If you know neither the enemy nor yourself, you will succumb in every battle.”
>
> Sun Tzu, The Art of War

B. *Organizational cybersecurity and human factors*

Organizational cybersecurity is a complex combination of technological factors and human factors; technology alone cannot guarantee cybersecurity. According to the ENISA Guidelines, models that stress ways to enable appropriate cybersecurity behavior are more effective than those using threat awareness or punishment [3].

Organizations should strive for active participation rather than compliance. Rapidly emerging threats require employees who are engaged and willing to step up. Measures to improve security behavior should be an ongoing, iterative process. The human factor in cybersecurity is never 'solved'. There is no other solution than human skills and knowledge; it is necessary to provide the personnel with proper and adequate information on the organization's security policy, the role of the employees, the resulting obligations and the consequences of omissions, in a regular and repetitive way. In order for an organization to be cyber-safe today, it must shift from technocentric view to an anthropocentric view by adopting knowledge from behavioral theories [3].

According to Safa et al., "the lack of information security awareness, ignorance, negligence, apathy, mischief, and resistance is the root of users' mistakes" causing undesirable security behavior by employees [4]. In other words, the lack of 'security culture' leads to failures.

To understand the potential risks of socio-technical systems and effectively protect their organization from cyberattacks, cybersecurity students need to consider how people perceive, feel, remember, think and solve problems, both defenders and attackers. This involves topics from the domain of cognitive psychology.

To understand the behavior of cybercriminals, cybersecurity students need to consider how people feel, react, remember, think and perceive social discrimination, inequalities and conflicts i.e., topics from the domain of social and behavioral psychology. These topics are often not covered in cybersecurity classes. An introductory course on behavioral psychology is offered by the HAFA, but it is relating to the workplace and not to the cyberspace [5].

However the psycho-social perspective is useful to engineering students, first, because it will guide them to design computer and information systems securely for a variety of user types, and second, because it will help them protect themselves and their organization. It is very important for cybersecurity students to learn that the user might prove to be the weak link for breaking a technically secure system, i.e., to examine the social implications and ethical issues concerning the use of computer systems in their organization.

Several modern cybersecurity attacks combine various methods including social engineering attacks. For instance, phishing emails and phone scams use many psychological principles causing a sense of scarcity or urgency, in order to persuade users to open a malicious link [6],[7].

In order to increase student participation and interest, the instructor has used gamification [8] and competition-based learning in this particular course in the past [1]. Moreover, the instructor has been using video clips in his classes because he believes in the power of the specific medium [9].

C. Movies in education

> "To an extent, every technological innovation presents an opportunity to rethink and re-imagine a curriculum. Even chalkboards were once a novelty... Textbooks, television, computers, and the Internet have all changed the landscape for social studies teachers and thinkers."
>
> (Hammond & Lee, 2010) [10]

Each new technology opens new possibilities for teachers to achieve the goals of the curriculum. Films are part of students' everyday life. Currently, movies are highly available in a variety of formats and can be easily played using common equipment such as computers. Films may provide notable pedagogical options and may prove rich resources of intrinsically motivating materials for learners.

Films have been used extensively in language courses [11], but rarely in engineering and science. Digital videos (but not movies) have been used as tools for learning mathematics [new 12= Niess & Walker, 2010]; films and movie clips have been used as tools for teaching selected concepts in physics [new 13= Efthimiou & Llewellyn, 2004]; [new 14= Solis & Orale, 2017]. To the best of the author's knowledge, there has been no prior attempt to employ films for teaching cybersecurity. Taylor et al. have developed a cybersecurity training tool which uses (among others) video documentary real-life case studies [7].

In this paper we describe the use of a movie as a pleasant and attractive means to introduce students to the social and psychological topics of cybersecurity [5],[7],[15].

D. Significance of the experiment

This study is timely as more and more movies are produced each year and the popularity of movies among the students is rising. It is a pioneer work because so far movies have not been used in the educational process of a cybersecurity or network security course (to the best of the author's knowledge). This study is also pioneer in the sense that it uses a movie to assess students' understanding of several cybersecurity attacks in practice.

II. Research plan

The research experiment was implemented during the academic year 2017-2018, in the Network Security course of the 8th (spring) semester.

A. Selecting the movie

The instructor used the following criteria in his selection of a hacking movie:

1) Relation to the course; presentation of several types of cyberattacks.

2) Presentation from the attacker's viewpoint.

3) Avoidance of hacking “in the broadest sense of the term” [16], that is, other genres mixed with hacking [16], [17]; focus on cyber-hacking. Under this prism, several famous movies such as ‘The Italian Job’, ‘Die Hard’, ‘Live Free or Die Hard’ and ‘The Matrix’ had to be excluded.

4) Limited runtime to fit in three academic hours, leaving time for the students to complete a questionnaire and for teacher to lead a discussion.

5) Attractive scenario to keep students interested.

The scenario of the movie starts as follows. Alex Danyliuk with his family immigrate from Eastern Europe to Canada seeking a better life. When his family encounters financial troubles, Alex leaves college and turns to a life of crime, with the help of Sye, a street-wise hustler who introduces him to the world of the black market. Alex meets Kira, a young female hacker, through the web. The three of them form a gang and earn a lot of money. At the same time Alex makes several contacts on the dark web. After some success, he attracts the attention of ‘Z’, a mysterious masked figure, who’s the head of a secret organization known as Anonymous, a number one target by the FBI. After a meeting, Z hires them to organize an international operation causing financial market chaos, which would profit them substantially. Alex agrees to this, seeing it as an opportunity to revenge the bank that laid off his mother [18], [19]. This movie is rated 6.2 on IMDB [17]. The film is also known as “Hacker” [19]. The runtime is 105 minutes.

The actors of the selected film are the same age as the students. In addition, the film is presented from the point of view of the main actor, which allows students to identify with the protagonist. In this way the students understand the motives that pushed the hacker into delinquent behavior and realize that the misuse of cybersecurity skills can lead to legal infractions. Figure 1 shows a screenshot with the protagonist of the film.

B. Selecting the date

The movie was displayed on April 13, 2018, the week right after the Orthodox Easter. This date was selected for two reasons: first, the syllabus coverage was satisfactory at that time, so we could afford a lecture for the movie; second, it was a transitional period from the Easter vacation back to work. Five out of the nine students coming from distant places had a longer period of absence (due to extra time for traveling). In such cases the instructor may choose not to continue lecturing but solve exercises, answer questions, etc. It was the perfect chance; therefore, four students watched the movie.

III. Methodology

A. Research instruments

Due to the small number of students, mainly qualitative research was used. The research tools used were semi-structured as well as open interviews [21], [22], [23]. The semi-structured interviews took place immediately after the screening (April 13, 2018). Students were asked to identify cyberattacks and cybercrimes committed by the hackers, as well as some other questions described below. Due to time constraints, students had to write their answers in a questionnaire. After that, they exchanged views in a constructive discussion facilitated by the instructor. Open interviews took place on May 7, 2018, after the final exams, in order to avoid biased answers [24].

B. The research questions

The main research questions were:

1) Are the students able to identify in practice the various types of attacks taught in theory [25],[26] and understand the corresponding motivation? The instrument used to test this research question was the questionnaire.

2) Are students able to detect common frauds in practice? The instrument used to assess this question was the questionnaire.

3) The projection of the psycho-social aspects; do the students possess the background necessary? The instruments used to assess this research question were both the questionnaire and the interview.

4) The students’ opinion on the use of movies in the specific course. The instrument used to assess this research question was the interview.

Most of the research questions appeared on the questionnaire. Some of the questions were related to the technical nature of cybersecurity whereas others were related to the part not covered in the syllabus, i.e., the psychosocial aspect.

B..1 Technical research questions

The students should recognize as many attacks as possible.

Q1) Which cyberattacks did you identify in the movie? (Open question – no list was given.)

Q2) Do you think that you have learned useful things about cyber security through the film?

B..2 Psycho-social research questions

Q3) The students were asked to characterize the main protagonist and classify him in one or more categories listed in the bibliography (Table 1 [25]; closed question).

Q4) Which frauds were committed by the protagonist? (Open question).

Q5) The students were asked to identify any relation between the movie and the Psychology course they attended during their 3rd year of studies.

B..3 Other questions

Q6) In addition, students were asked to rate the film compared to the films they had watched so far (numerical answer from 1 to 10).

Table 1: Some people who may cause security problems and their motivation [25]

Adversary	Goal
Student	To have fun snooping on people's email
Cracker	To test out someone's security system; steal data
Sales rep	To claim to represent all of Europe, not just Andorra
Corporation	To discover a competitor's strategic marketing plan
Ex-employee	To get revenge for being fired
Accountant	To embezzle money from a company
Stockbroker	To deny a promise made to a customer by email
Identity thief	To steal credit card numbers for sale
Government	To learn an enemy's military or industrial secrets
Terrorist	To steal biological warfare secrets

B..4 Interviews

The interview was semi-structured. There were some open questions concerning the two courses offered by the same instructor in that semester, namely Computer Networks II and Network Security. The first set of questions concerned the lectures and the lab exercises; in the second round of questions the students had the opportunity to freely make suggestions for the improvement of the courses. Finally, the third round of the interview was about the movie; the students were asked if they were watching movies regularly, if they had been displayed movies in other courses before and how did they like watching the movie as part of the course. The answers will be presented in the following section.

C. Student demographics

The class consisted of nine students, eight males and one female, aged 22 years. All students had lived together in the HAFA for four consecutive academic years and had followed the same educational and training program, hence the class was highly homogeneous.

D. Validity

The students filled in the questionnaire right after watching the movie, in order to easily recall it. Each student was sitting in their own desk and discussion was not allowed. The questionnaire was anonymous and the answers did not count towards the course grade. The instructor supervised the whole process and collected the questionnaires.

In order to avoid biased answers, the students who watched the movie were interviewed after the end of the course, several days later, on May 5, 2018.

IV. Research results

This research is mostly qualitative, because the sample is small; hence, it is rather superfluous to undertake a full-scale statistical analysis.

A. Results of the questionnaire

A..1 Technical research questions results

Q1) Let's start with open question Q1 of the questionnaire where the students were asked to identify the cyberattacks committed by the protagonists. Most students were able to spot the most obvious attacks such as social engineering and spear phishing; one of them did not respond. The average student identified 50% of the attacks (Table 2). The probable cause is the distance from theoretical definition to actual action. The film presented the attacks in a realistic matter. This is not the case in adventure movies where the hacker can break into any system in minutes and that is why such movies were rejected during the selection process (see section II).

Table 2: Success rate in identifying cyberattacks

Attacks	Success rate
Social engineering	75 %
Spear phishing	50 %
Malware	50 %
Other (DoS)	25 %

Q2) Open question Q1 of the questionnaire was: "Do you believe that you have learned useful things about cybersecurity through the movie?" The answer was 'some' (i.e., average) and we attribute this to the fact that the movie was a commercial one and it also included common frauds not relating to cybersecurity.

A..2 Psycho-social research questions results

Q3) Classify the main protagonist. The results of the questionnaire revealed that the students on average identified correctly (100%) seven out of ten cases (Table 3).

Q4) From open question no. 4 of the questionnaire, where the students were asked to identify the frauds committed by the protagonists, the answers varied a lot and only one of the students managed to identify almost all of the cybercrimes displayed (such as identity theft and credit card cloning).

Q5) The psychology course taken by our students during the 3rd year is about psychology in the workplace and it does not cover the psycho-social aspects of cybersecurity; hence, by displaying this movie, we have introduced this perspective to the students.

From the last two points we may conclude that students' awareness on the non-technical dimension of cybersecurity is inadequate; the movie revealed this fact

Fig. 1: The main protagonist in action

Table 3: Classification of the hacker's actions

Goal	**Checked by** (no. students)	**Success rate**
To have fun snooping on people's email		100%
To test out someone's security system; steal data	2	50%
To claim to represent all of Europe, not just Andorra		100%
To discover a competitor's strategic marketing plan		100%
To get revenge for being fired	3	75%
To embezzle money from a company	4	100%
To deny a promise made to a customer by email		100%
To steal credit card numbers for sale	4	100%
To learn an enemy's military or industrial secrets		100%
To steal biological warfare secrets	1*	75%
	(*) Wrong answer	

Table 4: Success rate in identifying cybercrimes

Cybercrimes	**Success rate**
Identity theft	50%
Credit card stealing & cloning	100%
Stock market fraud	25%
Fake news production	25%

and also gave them an opportunity to think constructively towards this direction.

A..3 Rating the movie

Q6) The average rank given by the students was 6.875 which is somewhat higher to the average IMDB rate (6.2 [20]) but still close enough, which implies that the students are familiar with the contemporary movie industry.

B. Results of the interview

As far as the interview is concerned, the instructor received critical as well as constructive feedback on the matters relating to the courses. Regarding the movie, the results revealed that:

- The students watch movies on a regular basis, which means that it was a good idea for the instructor to use this channel in order to communicate some additional aspects of cybersecurity, due to their familiarity with the medium.
- The students were shown documentaries and video clips in the past, in the War Ethics course, but they liked better watching an entire movie [11].
- One of the students admitted that they enjoyed the movie while the others confirmed that.
- One of the students had watched the same movie in the past; however they still found it interesting because this time they watched it from another perspective.
- Finally, all students agreed that it was a good idea to watch a movie in the framework of the Network Security course.

C. Limitations of this research

The results of this pilot experiment concern the HAFA students attending the specific Network Security course which has a technical orientation. These students acquired a specific background during their studies; hence the results cannot be generalized to other institutions [27]. However, the value of this research is that it revealed a gap in the curriculum that needs to be filled, as well as provided useful guidance to the instructor to give the necessary depth and orientation to the lesson, to improve student awareness. In addition, it introduced an innovative way of teaching the principles of cybersecurity and cybercrime in higher education, which could inspire other teachers.

V. Discussion

Research on human behavior (often termed 'behavioral science') encompasses a wide range of disciplines such as psychology, sociology, anthropology, human biology, behavioral economics, etc. The insight that humans are an integral part of the cybersecurity chain is not new. However, only in the last twenty years has there been an important social science research body that examines cybersecurity as a socio-technical problem and develops guidelines on how to effectively manage it. The socio-technical perspective includes the actions and decisions of security professionals, policy makers, systems designers, developers, as well as end users [3]. As the Network Security course syllabus is technically oriented, the film seemed a good solution to raise students' awareness of human behavior issues.

The movie narrates a whole story spanning several years of the protagonist's life in a realistic manner and teaches several issues such as social factors leading to offensive behavior, psychological factors such as the need to feel distinct, the need to socialize, to trust people, to love, etc. Moreover, the film presents several actual attacks; in real life, hackers use combinations of attacks in order to target a specific victim. This is a very important lesson because students in the classroom – or even in the lab – are only taught one attack at a time.

The movie presents the reality from the hackers' perspective and facilitates the students to better understand how the attackers think. In the classroom we examine cybersecurity from the viewpoint of the defender. However, a successful cyberdefender ought to know how cyberattackers think and act; according to Sun Tzu, a successful warrior must know their enemy. In other words, the students are taught to reframe a situation and alter roles. This is a very important ability, since it has been said that:

> "Defenders think in lists. Attackers think in graphs. As long as this is true, attackers win."
>
> John Lambert, GM, Microsoft Threat Intelligence Center

VI. Conclusion

Cyberspace is just another battlefield like land, sea, air and space. Hence, rules of engagement such as that of Sun Tzu's quoted in the Introduction, still hold. In Cyberspace where the opponents don't see one another, psycho-social factors might reveal useful knowledge of the enemy, especially when combined with other sciences such as psychology and artificial intelligence.

In this paper a pioneer effort of displaying a commercial movie in order to enhance student education on cybersecurity is described. The students assessed positively the experiment and also had the opportunity to get informed about some of the non-technical aspects of cyber-crime, such as the psycho-social and legal factors. It became clear that a youngster with extra information science skills may become a cybercriminal under special circumstances and that cybersecurity has also a psycho-social dimension. This dimension is beyond the technical background of the course, but it is evident that it should not be underestimated, for several reasons; first because can lead to delinquent behavior; second, because a wrong click by an untrained user may put into security risk a whole organization; third, because a user under pressure may easily make a mistake, etc.

The questionnaire filled by the students right after the movie proved to be an alternative way to test students' understanding of both technical knowledge (attacks) and socio-cultural aspects of cybersecurity.

Research results revealed that psycho-social and socio-cultural dimensions are missing from the curricula offered to HAFA Telecommunications and Electronics Engineering students. To address this problem, the following three measures are proposed:

- Add a special lecture to the Psychology course of the 3rd year.
- Add a special lecture about Cybersecurity Ethics to the War Ethics course of the 2nd year.
- Use proper video clips in the Cybersecurity course in addition to the technical content.

The instructor intended to repeat the experiment in the spring 2020 semester; however, the plans were canceled because of the Covid-19 imposed lockdown. A new educational research experiment is scheduled with another film in the future. Furthermore, an improved version of the questionnaire, enriched in the psycho-social dimension, will be used. An even more advanced idea is to employ video clips as well as films demonstrating cyberattacks in the assessment procedure.

References

[1] Andreatos, A., "Designing educational scenarios to teach network security", in Proc. of IEEE Educon 2017, Athens, Greece.

[2] Adams, A. and Sasse, M. A., "Users are not the enemy: Why users compromise computer security mechanisms and how to take remedial measures", Communications of the ACM, Vol. 42, No. 12, 1999, pp. 40-46.

[3] ENISA - European Union Agency For Network and Information Security, “Behavioural Sciences Research in the Field of Cybersecurity”. ISBN: 978-92-9204-267-7, DOI: 10.2824/324042, 2018.

[4] Safa, N. S., Von Solms, R. and Furnell, S., “Information security policy compliance model in organizations”, Computers and Security, 56, 2016. pp. 70-82.

[5] McAlaney, J., Thackray, H. and Taylor, J., “The social psychology of cybersecurity”, The Psychologist, vol. 29, no. 9, 2016, pp. 686-689.

[6] Cialdini, R. B., “Influence: Science and Practice (5th Edition)”, Englewood Cliffs, NJ: Prentice Hall, 2008.

[7] Taylor, J., McAlaney, J., James, S., Dale, J., Hodge, S., Thackray, H. and Richardson, C., “Teaching psychological principles to cybersecurity students”, In Proc. of IEEE Educon 2017, Athens, Greece, 2017.

[8] Hamman, S.T., Hopkinson, K. M., Markham, R. L., Chaplik, A. M. and Metzler, G.E., “Teaching game theory to improve adversarial thinking in cybersecurity students”, IEEE Transactions on Education, 99, 2017, pp. 1-7.

[9] Snelson, C., “Web-Based Video for e-Learning: Tapping into the YouTube phenomenon”. In H. H. Yang & S. C. Yuen (Eds.), Collective Intelligence and E-Learning 2.0: Implications of Web-Based Communities and Networking, pp. 147-166. New York: IGI Global, 2009.

[10] Hammond, T. C., and Lee, J. K., “Editorial: Digital video and social studies”, Contemporary Issues in Technology and Teacher Education, vol.10, no.1, 2010 pp. 124-132.

[11] Abdo, I. B., and Al-Awabdeh, A.-H., “Animated Videos Prove to be Beneficial in Teaching English Grammar as EFL: A Neurological Study of How Students Learn and Retain English Grammar”, Creative Education, vol. 8, 2017, pp. 1415-1423.

[12] M. L. Niess and J. M. Walker, Digital Videos as Tools for Learning Mathematics. Contemporary Issues in Technology and Teacher Education, vol. 10, no. 1, 2010, pp. 100-105.

[13] C. Efthimiou and R. Llewellyn, “Physics in Films” - A New Approach to Teaching Science, 2004.

[14] Solis, M. and Orale, R. (2017). “Use of Movie Scenes as Simulations to Enhance Students’ Performance on Selected Physics Concepts”. Journal of Academic Research, 2, pp. 1-6.

[15] Rogers, M. K., “The psyche of cybercriminals: A psycho-social perspective”. In G. Ghosh and E. Turrini (Eds.) Cybercrimes: A Multidisciplinary Analysis, 2010.

[16] Leyden, J., “Top 10 best hacking films of all time”. Available: https://portswigger.net/daily-swig/top-10-best-hacking-films-of-all-time, Apr. 2020.

[17] Barrasso, N., “7 Best Movies about Cybersecurity and Hacking”. Available: https://www.cybereason.com/blog/movies-about-cyber-security-hacking-crime, Apr. 2018.

[18] Hacker, the story, 2016. Available: https://www.imdb.com/ title/tt3173594/plotsummary?ref_=tt_stry_pl.

[19] Cybersecurityventures. Available: https://cybersecurity-ventures.com/movies-about-cybersecurity-and-hacking.

[20] Hacker, the movie, 2016. Available: http://www.imdb.com/title/tt3173594.

[21] Oppenheim, A. N., “Questionnaire Design, Interviewing and Attitude Measurement” (chapters 7 & 8), London & NY: Continuum, 1992.

[22] Bricki, N. and Green, J., “A Guide to Using Qualitative Research Methodology”, 2002, p. 2. Available: http://fieldresearch.msf.org/msf/bitstream/10144/84230/1/Qualitative+research+methodology.pdf.

[23] Newman, W. L., “Social Research Methods: Qualitative and Quantitative Approaches (5th ed.)”, Boston: A&B, pp. 268-288, 2003.

[24] Creswell, J. W., “Research design: qualitative, quantitative, and mixed methods approaches”, Thousand Oaks, CA: Sage, 2003.

[25] Tanenbaum, A. S. and Wetherall, D. J., “Computer Networks (5th ed.)”, Prentice Hall, 2011.

[26] L. Pavlík, “Modeling the Impact of Selected Cyber Threats on the Organization’s Parameters in the Framework of Cyber Risk Insurance”, WSEAS Transactions on Business and Economics, vol. 15, 2018, pp. 522-528.

[27] Price, J. H. and Murnan J., “Research Limitations and the Necessity of Reporting Them”, American Journal of Health Education, vol. 35, 2004, pp. 66-67.