Academic year 2016-2017

Erasmus Mundus Joint Master Degree
in Economics of Globalisation
and European Integration

The economics of organized crime in Europe

Master dissertation

Student	Martin Roškot, MBA
Home institution	Vysoká škola ekonomická v Praze
Supervisor	Nicola Daniele Coniglio, PhD
Submission date	30th September 2017

Declaration of Authorship

I, Martin Roškot hereby declare that the thesis “The economics of organized crime in Europe” was written by myself, and that all presented results are my own, unless stated otherwise. The literature sources listed in the Reference section

Prague, September 30th, 2017

Signature

Acknowledgements

I would like to express my gratitude to the supervisor of the dissertation Professor Nicola Daniele Coniglio, PhD for his guidance, support and valuable recommendations.

Table of Contents

Introduction

This thesis was conducted to investigate the cyber area of organized crime - cyber-crime, as it represents a potential growing threat to public and private organisations. The ongoing development of the internet and creation of new opportunities for doing business internationally through e-commerce makes more businesses operating in the cyber space vulnerable to cyber-attacks. Countries are expanding their communication networks which leads to better information exchange, faster transactions or increased marketing and publicity.[1] Information technologies and internet affect all economic sectors.[2] These advantages come with a massive cost of potential threat to security, as the interconnectivity increases the vulnerability of information security breaches. This puts our activities such as government, business, military or even our private lives in stake. Cyber-crime cost European Union EUR 265 billion a year.[3] Businesses lost millions of EURs in preventing further attacks, regaining lost businesses and stolen assets or repairing company`s damaged reputation.

Cyber-crime, defined as a crime performed with an element of technology are either illegal or illicit computer mediated activities which can be performed on the global electronic network.[4] It has changed over past few years with attackers employing increased knowledge in cyber-fraud, cyber-terrorism, cyber-pornography, hacking and money laundering. Hackers have generated an emotion composed of admiration and fear over the past twenty years by using their computers to commit cyber-attacks.[5]

This becomes a big threat to publicly traded companies due to its effects on reputation and loss of stakeholder`s confidence[6] and therefore the outflow of their investment capital. When a company is perceived to be a target of a cyber-attack it can lose its current businesses and such a loss of contracts may almost instantly affect its market value. The impact of announcements of information security breaches on the stock market return has been examined for instance in studies of Campbell[7], Cavusoglu[8], Hovav and D'Arcy[9] or Kannan.[10] Results of these researches suggest that the announcements have mostly a significant negative impact. The literature related to the economics of cyber-crime is however very limited.

This thesis investigates the impact of ransomware cyber-attacks "WannaCry" and "Petya" on stock prices of publicly traded companies in the EU. This dissertation also analyses a set of

[1] Alkaabi, A.O.S., 2010 „Combating Computer Crime: An International Perspective", Queensland of Technology University.

[2] Campbell, K., Gordon, L., Loeb, M., Zhou, L., 2003. The economic cost of publicly announced information security breaches: Empirical evidence from the stock market. Journal of Computer security 11, 431-448.

[3] Europol. 2017. European Cyber-crime Centre - EC3 | About Europol | Europol. [ONLINE]

[4] Douglas W. Thomas and Brian D. Loader as cited by Yar M., Cyber Crime and Society, London: SAGE Publications, 2005, p. 9.

[5] Parton T., 2011 „Cyber Crime: Protecting Against the Growing Economic Crime", PWC Crime Survey, p. 5.

[6] Brockett, P.L., Golden L.L., Wolman W. Enterprise cyber risk management, in Risk management for the future – Theory and cases, Jan Emblemsvag. 2012.

[7] Campbell, K., Gordon, L., Loeb, M., Zhou, L., 2003. The economic cost of publicly announced information security breaches: Empirical evidence from the stock market. Journal of Computer security 11, 431-448.

[8] Cavusoglu, H., Mishra, B., Raghunathan, S., 2004. The effect of Internet security breach announcements on market value: capital market reactions for breached firms and Internet security developers. International Journal of Electronic Commerce 9, 69-104.

[9] Hovav, A., D'Arcy, J., 2004. The impact of virus attak on the market value of firms. Information System Security 13 (3), 32-40.

[10] Kannan, A., Rees, J., Sridhar, S., 2007. Market reaction to information security breach announcements: an empirical analysis. International Journal of Electronic Commerce 12, 69-91.

case studies related to largest recent cyber-crime events which happened in the first half of 2017. The goal of this thesis is to address these questions:

1. Is the cyber-crime a threat to companies?
2. How does cyber-crime announcements and publications affect stock prices?

Literature review

Norton Security Symantec Corporation defines cyber-crime as a crime that involves computer or cyber aspect.[11] Cyber-terrorism term has been adopted by the United States Armed Forces, explaining it as *premeditated, politically motivated attacks by sub national groups or clandestine agents or individuals against information and computer systems, computer programs, and data that result in violence against non-combatant targets.* Cyberwarfare is described as attacks that are planned and led against nations or their agents, ICT systems, computer programs and data, causing loss for the enemy. Although cyber-crime, cyber-terrorism and cyberwarfare may seem to be very similar, they differ in the attacker`s motivation.[12] As long as there has been an Internet, criminals have sought to exploit it, however exploitation of cyber systems started long before the internet was found.

Cyber-crime

Brief history

Cyber-crime has evolved gradually since the beginning of 20th century, starting with Morse code spoofing by magician Nevil Maskelyne in 1903. Enigma machine code was then breached later in 1932. In the 1943 first electronical programmable computer Colossus was invented and used to hack the Nazi punched card system by René Carmille, comptroller general of the Vichy French Army in 1943.[13] First cyber-crime case in 1970 involved an information breach into New York's Dime Savings Bank and embezzling of over $2 million.[14] In 1979 network infrastructure of ARPA, an agency of U.S. Department of Defense was misused for commercial purposes by marketing executive of Digital Equipment Corporation (DEC).[15] Cyber-crime activities increased rapidly since 1990`s. An internet activist non-profit organization Electronic Frontier Foundation (EFF) has been found in the same year and within 7 years the percentage of households in the US owning computers increased from 15% to 35%.[16]

Since then ideal conditions for cyber-crime had formed. The amount of cyber-attacks and their sophistication has influenced national interests and required governments to modify their security strategies and 108 countries had implemented offensive cyber warfare capabilities by 2007.[17] The role of cyber-crime is increasing, especially in strategic planning, international

[11] Norton. 2017. Cyber-crime - The Definition of Cyber-crime | Norton. [ONLINE]
[12] Janczewski Lech J. and Andrew M. Colarik, ed., 2008 Cyber Warfare and Cyber Terrorism, Hershey (PA): Information Science Reference.
[13] Davis Amanda. 2015. A History of Hacking. [ONLINE]
[14] Wavefront. 2016. A BRIEF HISTORY OF CYBERCRIME. [ONLINE]
[15] Goodman, Danny, 2004. Spam wars : our last best chance to defeat spammers, scammers, and hackers. 1st ed. New York: SelectBooks, Inc.
[16] "Issues in labor Statistics" (PDF). 1999 U.S. Department of Labor.
[17] Markoff John. 2017. A Code for Chaos - The New York Times. [ONLINE]

relations and politics. Cyber-crime corresponds with characteristics of organized crime as cyber-criminals engage whenever there is an opportunity to exploit. Furthermore, it supports operations of regular organized crime, such as trafficking of drugs, people, arms or piracy into money-laundering etc.

The Global Cyber war

According to security experts, the battleground has been shifting towards the private sector due to the fact that many services involving sensitive data are provided by private companies.[18] Hackers` activities are monitored in China and Iran, involving espionage and intellectual property theft. Russia and Eastern Europe suffers from identity and valuable assets thefts. In the United States hacktivist group, Anonymous, has been targeting both private and public organizations, but they engaged also abroad. The cyber war takes place all over the world. The Malware Stuxnet has demonstrated how large impact a cyber security incident can have in 2010, followed by malwares Skywiper in 2012 and Red October in 2013.

Stuxnet, is believed, was designed by Israel in the ongoing tension between Iran and Israel, supported by the U.S. in order to sabotage Iranian nuclear facilities. The virus was revealed in 2010, hitting Siemens industrial computer systems in nuclear, power and oil industry. The consequences were however even more damaging as it affected activities of industrial control computers in China, India and Indonesia.[19] According to *The Economist*, Stuxnet was built by well-funded computer experts with excellent knowledge, as the complexity and sophistication of the virus suggest. It has started under Bush administration in 2006 as operation Olympic Games and was accelerated under president Obama.[20] According to the same source Bush believed that attacking Iranian nuclear facility in Natanz was the only way to prevent Israeli conventional strike. Iran had returned the strike and hit U.S. banks, oil producer in Saudi Arabia and in 2011 attacked the Dutch certificate authority DigiNotar.[21]
In 2013 both North and South Korean organizations became targets in internet breakdown attack. Lately attackers who are supported by Chinese government became large threat as they are ubiquitous and make the impression of omnipotence.[22] It is worth exploring the theoretical background of cyber-crime in order to understand the economic consequences.

Cyber-terrorism

It is essential to analyse roots of cyber-terrorism to understand its causes and consequences. Some authors define cyber-terrorism as the effort made by terrorist organizations to disrupt IT systems in order to create panic, alarm or to disrupt physical facilities. Another approach defines cyber-terrorism as a sub-type of cyber-crime, while cyber-crime is not always leading in terror.[23] These are some of characteristics that cyber-terrorism has in common:

- a group of people have been frightened

[18] Violino Bob. 2017. Unseen, all-out cyber war on the U.S. has begun | InfoWorld. [ONLINE]
[19] Markoff John. 2017. A Code for Chaos - The New York Times. [ONLINE]
[20] Sanger E. David. 2017. Obama Ordered Wave of Cyberattacks Against Iran - The New York Times. [ONLINE]
[21] Keizer Gregg. 2017. Hackers spied on 300,000 Iranians using fake Google certificate | Computerworld. [ONLINE]
[22] The Economist. 2013. A giant cage. [ONLINE]
[23] Gadish, O., 2017. Cyber Terror: How It Happens And What We Can Do. 1st ed. Amazon: OGM.

- informational technologies were used to cause mayhem, destruction or harm to personal objectives[24]
- a terrorist organization utilize the internet to establish communication network in order to recruit new member.[25]

Certain opinions even deny such statements and according to Harper, it is inappropriate to label it as terrorism because creation of fear, serious physical harm or death is unlikely using electronic tools.[26] Unfortunately, it has been proven that cyber-attacking tools can and do such damages. According to NATO`s definition cyber-terrorism is *a cyber-attack using or exploiting computer or communications networks to cause sufficient destruction or disruption to generate fear or to intimidate a society into an ideological goal.*[27]

The explanation of the cyberterrorists` intentions are differentiated by three factors. The most common incentive is creating **fear** in their victims, while attacking their critical infrastructures. Creation of fear of losing control in groups or societies.[28] The **spectacular factor** assumes the attack to be and actual attack, causing reputation damage and direct losses. Amazon i.e. was hit by a denial of service attack in 1999, resulting in direct losses due to suspended trading. Third factor suggests that attackers will hit the weak spots. They are exploiting the **vulnerability** with a malicious code in order to gain remote access offering full control. Cyberterrorists develop sophisticated plans, gather set of software and perform full analysis of the victim`s system during the preparation of the attack.[29] Cyberterrorists act independently as non-state actors. According to prof. Robert A. Pape almost all terrorists have specific a strategic goal in common, to force modern democracies to withdraw military units from the country that the terrorist perceives as his home.[30] First record of cyber-terrorist attack is from 1997 when the Black Tigers, a wing of militant Sri Lankan separatist organisation, used jamming device to flood e-mail boxes of Sri Lankan embassies all over the world with over 800 e-mails per day.[31] During Kosovo war in 1998 a cyber-attack was conducted against NATO computers involving defacement of the US government websites.[32] A Chinese activist group responsible for this attack justified the attack as revenge for the accidental bombing of the Chinese embassy in Belgrade by NATO forces.

Profile of the attackers

Motivation for attackers to commit a cyber-crime is mixed. It is an opportunity offering high returns at almost no risk of being caught and relatively low cost. Their incentive is even emphasised by the absence of physical contact with the victim`s computer and the fact that

[24] Kent Anderson, Prague Post. 2017. Virtual hostage | Prague Post. [ONLINE]

[25] Worth F. Robert. 2017. 'Terror on the Internet,' by Gabriel Weimann - The New York Times Book Review - The New York Times. [ONLINE]

[26] Harper Jim. 2017. “There’s no such thing as cyber terrorism” — RT News. [ONLINE]

[27] NATO, (2008). Cyber defence concept MC0571. Brussels, Belgium.

[28] Korstanje M 2017 English Speaking Countries and the culture of Fear: understanding technology and terrorism”. Threat Mitigation and Detection of Cyber Warfare and Terrorism. Chapter 5 (pp. 93-111) IGI Global, Hershey, Pennsylvania, US.

[29] Prichard, J.J. & MacDonald, L.E. 2004. Cyber Terrorism: A Study of the Extent of Coverage in Computer Security Textbooks. *Journal of Information Technology Education, 3*, 279-289

[30] Pape Robert, 2005 Dying to Win: The Strategic Logic of Suicide Terrorism, New York: Random House.

[31] Denning E. Dorothy. 2000. Cyberterrorism threat. [ONLINE]

[32] Chris Nuttall, BBC. 1999. Kosovo info warfare spreads. [ONLINE]

they can stay hidden. Nowadays, hackers engage in many ways. It is worth exploring the theoretical background of cyber-crime in order to understand its economic consequences. According to Andress (2011) it is possible to distinct between different types of hackers.[33]

Categories of cyber-attackers:

1. Organized attackers: **Cyber terrorists** are those intending to make a political statement or to inflict psychological and physical damage on their targets. Their goal is to achieve political gain by threatening opponents or the public. Although it may seem that cyber terrorists` funds are limited, they are able to raise millions of dollars which they then spend for the attacks. Further they may spend the funds for commercial consulting and expertise.[34] Primary motivation of **hacktivists** is to raise awareness and to encourage changes through fear, but political statements can also be included as well as damages.[35] **Nation-state attackers** engage in sabotage and data gathering on behalf of governments. Unlike other types of organized hackers these have access to advanced training, sufficient funds. They can often count on backup of scientific capabilities of the state. They are well organized and that allows them to perform more sophisticated attacks aimed at specific goals.[36] Professional criminals may form organized groups of **criminal actors**,[37] which are usually acting within complex criminal environments in cyberspace. These groups are segmented into layers and they are well service oriented.[38] They focus on control, power and wealth.[39]
2. Hackers: This group consists of benign explorers, malicious intruders or computer trespassers. Their primary incentive for hacking is the challenge and achievement from obtaining access.[40] So called **black hats** are hackers who perform malicious exploitation of a target system. They perform illegal activities in order to achieve either financial or political gain on behalf of criminal organization or governments. This type illegal activities include espionage (i.e. obtaining of sensitive data through unauthorized access for personal, political or criminal purposes), extortion, theft (i.e.

[33] Andress, J., & Winterfeld, S., 2011. Cyber Warfare: Techniques, Tactics and Tools for Security Practitioners. Waltham, MA: Elsevier.

[34] Howard, J. D. 1997. An Analysis of Security Incidents on the Internet 1989–1995. Doctoral Thesis, Carnegie-Mellon University, Pittsburgh, PA.

[35] Cohen, F., Phillips, C., Painton Swiler, L., Gaylor, T., Leary, P., Rupley, F., & Isler, R. 1998. A Cause and Effect Model of Attacks on Information Systems: Some Analysis Based on That Model, and The Application of That Model for Cyber Warfare in CID. *Computers & Security,* 17(3): 211-221. http://dx.doi.org/10.1016/S0167-4048(98)80312-X

[36] Cohen, F., Phillips, C., Painton Swiler, L., Gaylor, T., Leary, P., Rupley, F., & Isler, R. 1998. A Cause and Effect Model of Attacks on Information Systems: Some Analysis Based on That Model, and The Application of That Model for Cyber Warfare in CID. *Computers & Security,* 17(3): 211-221. http://dx.doi.org/10.1016/S0167-4048(98)80312-X

[37] Cohen, F., Phillips, C., Painton Swiler, L., Gaylor, T., Leary, P., Rupley, F., & Isler, R. 1998. A Cause and Effect Model of Attacks on Information Systems: Some Analysis Based on That Model, and The Application of That Model for Cyber Warfare in CID. *Computers & Security,* 17(3): 211-221. http://dx.doi.org/10.1016/S0167-4048(98)80312-X

[38] Grau, D., & Kennedy, C. 2014. TIM Lecture Series – The Business Of Cybersecurity. *Technology Innovation Management Review,* 4(4): 53–57. http://timreview.ca/article/785

[39] Gragido, W., Molina, D., Pierce, J., & Selby, N. 2012. Blackhatonomics: An Inside Look at the Economics of Cyber-crime. Waltham, MA: Elsevier.

[40] Howard, J. D. 1997. An Analysis of Security Incidents on the Internet 1989–1995. Doctoral Thesis, Carnegie-Mellon University, Pittsburgh, PA.

theft of valuable data, intellectual property) or vandalism.[41] **White hats** on the other hand conclude system breaches in order to reveal weaknesses usually on behalf of the owners of the system or it is a part of their contract.[42]

3. Amateurs: They use information, instructions and tools available on the internet to exploit computer systems. Their incentive can be the challenge itself, skill development or attracting an attention of hacker groups, hoping to pass the entry criteria.[43] Regardless the nature of their intentions, those tools may cause big harm in their hands.

Actions taken by cyber-attackers are not always intentional and yet they present cybersecurity risk. Cebula & Young[44] describe different types of actions: Unintentional **inadvertent actions** mostly taken by insiders, **deliberate actions** which are meant to cause damages and **inaction**, i.e. underestimating security threats, absence of action to solve the situation due to insufficient knowledge, skills or guidance.

Considering the actions taken by hackers it is possible to distinct their motivation for deliberate actions into three categories:

- Political motivation involves espionage, making political statements, protests or retaliatory actions. It may also include destruction, disruption or taking control of strategic targets. More recently, cyber spying involves monitoring of public activities on social networks.
- Economic motivation particularly includes need for achieving personal gain or gain for an organization. Except typical theft of intellectual property, funds or credit card information, it also involves fraud, industrial espionage or blackmailing.
- Socio-cultural motivation stands behind philosophical, theological and political cyber-attacks. They can also be performed for humanitarian goals, as well as for fun, curiosity, need for publicity or self-esteem.[45]

Motivations behind cyber-attacks in May 2017 is shown on the graph:

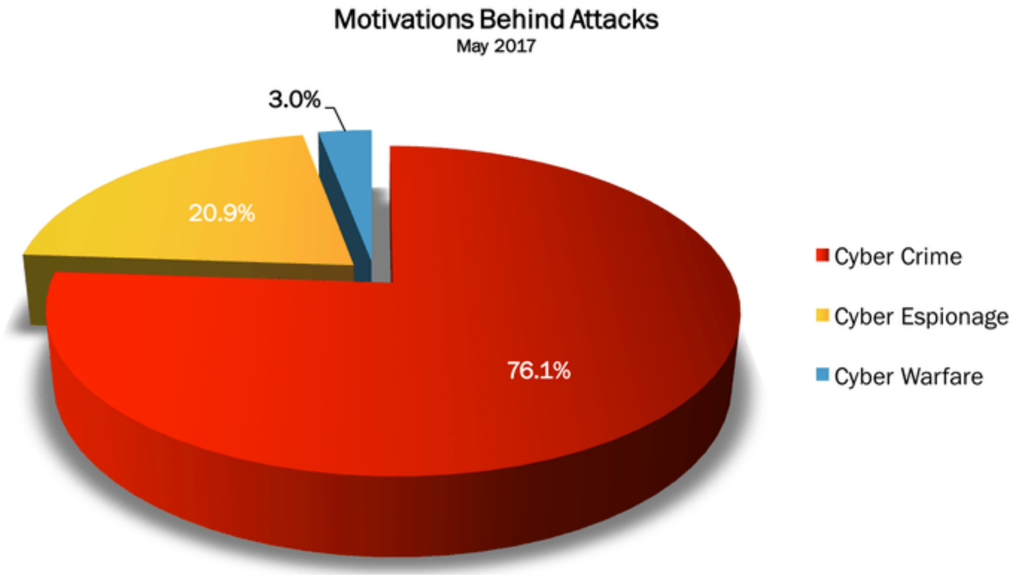
[41] Shakarian, P., Shakarian, J., & Ruef, A., 2013. Introduction to Cyber-Warfare: A Multidisciplinary Approach. Waltham, MA: Elsevier

[42] Cohen, F., Phillips, C., Painton Swiler, L., Gaylor, T., Leary, P., Rupley, F., & Isler, R. 1998. A Cause and Effect Model of Attacks on Information Systems: Some Analysis Based on That Model, and The Application of That Model for Cyber Warfare in CID. *Computers & Security,* 17(3): 211-221. http://dx.doi.org/10.1016/S0167-4048(98)80312-X

[43] Andress, J., & Winterfeld, S., 2011. Cyber Warfare: Techniques, Tactics and Tools for Security Practitioners. Waltham, MA: Elsevier.

[44] Cebula J. James, Young R. Lisa. 2010. A Taxonomy of Operational Cyber Security Risks. [ONLINE]

[45] Gandhi, R., Sharma, A., Mahoney, W., Sousan, W., Zhu, Q., & Laplante, P. 2011. Dimensions of Cyber-Attacks: Cultural, Social, Economic, and Political. *IEEE Technology and Society Magazine*, 30(1): 28-38.



Graph: Motivations behind cyber-attacks[46]

Categories of cyber-crime

Data related crimes:

- Data interception – monitoring the target`s outflowing and inflowing data streams, data gathering, may be performed as a preparation for an upcoming attack. Network communication monitoring involves method *sniffing,* observing regular data streams, reading the content.
- Data modification – involves third party penetrating in the informational flow and adjusting or editing the data before it is delivered. This attack has been used in its more sophisticated form to attack Bangladesh central bank and steal USD 100 million.[47]
- Data theft – includes unauthorized redistribution or illegally gained possession of corporate/personal data, passwords, bank card details, insurance information.

Network related crimes:

- Network interferences – attacking of functional computer network to edit and transmit malicious or fake information. Involves also damaging, suppressing or deleting of network communication.
- Network sabotage – deliberate and malicious act of disruption of the processes and functions or possible destruction or damage to equipment or information

Access related crimes

- Unauthorized access – viewing or possession of something without legal authority.
- Virus dissemination – virus spreading[48]

[46] Paolo Passeri, (2017), May 2017 Cyber Attacks Statistics [ONLINE].
[47] Tyler Durden. 2016. The Incredible Story Of How Hackers Stole $100 Million From The New York Fed Tyler Durden's picture. [ONLINE].
[48] CAPEC. 2017. CAPEC-117: Interception (Version 2.11) . [ONLINE].

Types of cyber-attacks

Cyber-attacks consist of phases, in similar way as a traditional crime. The attack requires preliminary observation in which the attacker analyses regular activities of the target, searches for basic information about him and devices he is using. Penetration phase involves forcing the victim to install the virus in a form of infected file, through e-mail, webpage or via USB device. If the attacker has access to a computer within the victim`s system, he can gain remote control almost instantly.

Once the attacker gains control over the system he assesses the internal capabilities and then he steals the information or/and disrupt the system, making the data unreadable. In addition, the attacker may remove any evidence of a cyber-attack i.e. use proxy servers, duplicated IP and MAC addresses and delete traces by erasing log files. Cyber-attacks can be performed with:

- **Malware** is a malicious program that can perform a variety of functions, including encrypting, stealing or erasing valuable data or taking control of core computing functions and monitoring users` activity.
    - Virus has an algorithm for self-replicating and it requires to be injected to a program and be executed to replicate itself. Virus can be placed even in the boot sector of the system and disable any access to the data for the owner.
    - Worm is a malicious program that replicates itself over standard network protocols unlike virus. It is a standalone type of malware. Mostly used for monitoring activities of a server and data collection and is being employed as a part of industrial espionage.[49]
    - Trojan pretends to be a legitimate function however the hidden algorithm infects the system and starts the malicious activity. Viruses and worms may be distributed via a Trojan horse software in order to install backdoor and remote control tool or keyboard logger software.[50]
    - Ransomware is a type of malicious software which has been designed to disable access to a computer until a ransom is paid. It is done by either locking the user`s screen or by locking the files. Modern ransomware types also encrypt the files and user is required to make an online payment to obtain a decrypt key.[51]

  Distribution of malware is conducted via email attachments, internet browser scripts, merged with pictures, pdf documents or executable software etc.

- **Distributed Denial of Service (DDoS)** attack involves group of compromised computers attacking a target, typically server or a website in order to disrupt its service activities. The attacker controls a network of bots and through the bots he sends large number of messages to the target and slows it down or he may completely disrupt it.[52]

[49] OECD (2009), Computer Viruses and Other Malicious Software: A Threat to the Internet Economy, Paris: OECD Publishing.

[50] Ibid.

[51] Ransomware - Definition - Trend Micro USA . 2017. Ransomware - Definition - Trend Micro USA . [ONLINE].

[52] Margaret Rouse. 2017. distributed denial of service (DDoS) attack. [ONLINE].

- **Unauthorized access** is gained by the attacker when he obtains administrator level access via social-engineering tools or he exploits the system to obtain certain password file which can be then cracked with brute force attack. This type of cyber-attack is aimed at a specific individual[53]
- **Advanced Persistent Threats (APTs)** is a set of computer hacking processes, targeting either private organizations or states for business or political motives. It involves unauthorized person to gain access to a network with the intention of data theft rather than causing damage to the network.[54]
- **Phishing** is an attempt to gather personal information such as login details, passwords, credit card details or communication history and content. The attacker carries out the attack by email spoofing or via instant messages. The victim is redirected to fake login webpage allowing the attacker to extract the login details and infect victim`s computer with further malware.[55]

Technical progress and ongoing innovation enables attackers to create more sophisticated attack methods. Therefore, malware attacks are considered to be the biggest internet threat. Recently there has been many cases with fraudulent anti-virus software or infected advertisement pages. Hackers can easily generate encrypted virus algorithms with help of Virus Construction Kits, which allows for virus creation eve those with little knowledge of software engineering and encryption. With help of above mentioned tools, hackers can:

- Disrupt electrical power systems of oil companies, transportation, water supply systems, banking and finance[56]
- Modify production of medications and drugs through unauthorized access[57]
- Change blood types of patients through unauthorized access to medical records[58]
- Share and report sensitive or secret information, such as military plans and movements of soldiers[59]
- Redirect political opinions and perceptions through exploiting and altering published information and facts[60]
- Perform identity theft[61]

Other potential risks:

- International business activity expansion
- Speed of computers is increasing and speeds up spreading of a virus.
- Hackers focus on zero-days (yet unknown) exploits development.

[53] NIST Computer Security Resource Center (CSRC). 2017. NIST Computer Security Resource Center (CSRC). [ONLINE].

[54] SearchSecurity. 2017. What is advanced persistent threat (APT)? - Definition from WhatIs.com. [ONLINE].

[55] Ramzan, Zulfikar (2010). "Phishing attacks and countermeasures". In Stamp, Mark & Stavroulakis, Peter. Handbook of Information and Communication Security. Springer.

[56] Embar-Seddon, A., 2002. Cyberterrorism. American Behavioral Scientist 45 (6), 1033–1043

[57] Wehde, E., 1998. US vulnerable to cyberterrorism. Computer Fraud & Security 1998 (1), 6–7.

[58] Gengler, B., 1999. Politicians speak out on cyberterrorism. Network Security 1999 (10), 6

[59] Desouza, K., Hensgen, T., 2003. Semiotic emergent framework to address the reality of cyberterrorism. Technological Forecasting and Social Change 70 (4),
385–396.

[60] Stanton, J.J., 2002. Terror in cyberspace. American Behavioral Scientist 45 (6), 1017–1032.

[61] Gordon, S., Ford, R., 2002. Cyberterrorism? Computer & Security 21 (7), 636–647

- Digitalization comes with information and transaction risks.

Although it may seem that cybersecurity keeps up with technical development, it is actually the work model of the attackers what stands behind the most of their success, not the technical tools. Cyber attackers have been offering the stolen information back to the victim. This is a change in behaviour - targeting the buyer within the circle of companies and individuals instead of hacking into large database and stealing information that could be sold to another criminal group and possibly used i.e. for credit cards production. Organized group of hackers also use services of brokers to distribute the card details faster through dark web. Those stolen cards were often used to buy prepaid card gifts which then could have been used to pay on regular e-shops, such as e-Bay. Nowadays the malicious software includes the element of time window, while the amount of demanded money increases until the data is deleted. Buyers have only limited time to regain stolen information.[62]

Intellectual property theft

In 2009, the intellectual property repositories of high-tech companies were targeted during operation Aurora. Hackers used hosts in China, Germany, Taipei, UK and US. The attackers focused on modification of intellectual property (IP) of high-tech, security and defense contractor companies.[63] Same methods used by cyber-attackers have been used by groups acting on behalf of governments for political espionage. However, it is almost impossible to link a cyber-attack to a specific group or a government due to lack of the evidence. In November 2014 information systems of the film studio Sony Pictures Entertainment Inc. were breached by hacker group called “Guardians of Peace”. Hacked data, including personal information of Sony Pictures employees, e-mails, information on executive salaries and copies of then-unreleased Sony films were leaked.[64] According to C-SPAN the hackers have stolen 47,000 Social Security numbers. The attackers claimed to have taken over 100 terabytes of data. Final step was to destroy infected data and IT infrastructure by running malware *Shamoon wiper.*[65] The leaked information led to several accusations. In 2015, The Verge informed that Motion Picture Association of America was lobbying to mandate US internet service providers to implement new system disallowing consumers to access pirate websites.[66] Later that year, WikiLeaks released more than 30,000 documents stolen via the cyber-attack.[67] According to senior general manager of Sony Pictures the hack caused $35 million in economic costs, including investigation and remediation costs.[68]

Events mentioned above show how losing customer data can be costly. Moreover, loss of intellectual property may threaten a company`s future. The biggest risk is that unlike for other cyber-crimes, the IP theft stays undiscovered for longer time. Which counts for higher costs, especially nowadays, when IP may represent over 80% of a firm`s value. Advancements in technology, globalization and growth are the reasons why IP theft through cyber-crime became much faster.

[62] Sher-Jan Mahmood. 2015. THE NEW ECONOMICS OF CYBER-CRIME. [ONLINE].
[63] Dark Reading. 2017. 'Aurora' Attacks Still Under Way, Investigators .... [ONLINE].
[64] Siboni Gabi, Siman David. 2014. Cyberspace Extortion: North Korea versus the United States. [ONLINE].
[65] Gallagher Sean. 2016. Shamoon wiper malware returns with a vengeance. [ONLINE].
[66] Brandom Russell. 2015. The MPAA has a new plan to stop copyright violations at the border. [ONLINE].
[67] Lang Brent. 2015. WikiLeaks Publishes Thousands of Hacked Sony Documents. [ONLINE].
[68] Hornyak Tim. 2015. Hack to cost Sony $35 million in IT repairs. [ONLINE].

Cyber-crime prevention and prosecution

Cyber-crime activities are broadly prosecuted nowadays. In the United States, the FBI has ranked cyber-crime prosecution as one of its top law enforcement activities. In Europe, Europol has no executive power unlike the FBI in the U.S. and provides support service for the law enforcement agencies of the EU Member States, which means that Europol officials cannot perform any executive actions without the approval of national authorities. However, Europol provides support through set of tools that can contribute to the executive measures carried out by relevant national authorities. Law enforcement response to cyber-crime in the EU has been improved by setting up the European Cyber-crime Centre (EC3) in 2013 to protect European citizens, businesses and governments. Regardless the difficulty of providing reliable estimates, EU perceives cyber-crime to be a wide and varied problem.

EC3 is a key part of Europol`s and the EU`s response, that consists of three-stage approach to the fight against online fraudulent activities: forensics, strategy and operations.[69]

1) Forensics expertise consists of two sections focusing on digital forensics and documents forensics. Each of them analyses operational support, research and development.

2) Strategy teams provide support by establishing new partnerships and by coordinating prevention and awareness measures. Furthermore, they are responsible for:

    - strategic analysis
    - the formulation of policy and legislative measures
    - the development of standardized training

3) The operations level of the EC3 focuses on:

    - Cyber-crimes committed by organised crime groups, especially those generating large profits, such as online frauds
    - Cyber-crimes seriously harming victims, such as child sexual exploitation
    - Cyber-crimes that impact critical infrastructure and information systems in the EU

Activities of the European Cyber-crime Centre are also supported by the Cyber Intelligence Team (CIT) that provides cyber-crime-related information collected from public, private and open sources. The CIT also identifies emerging threats and patterns.[70]

Another institution working alongside EC3 is the Joint Cyber-crime Action Taskforce (J-CAT). Objectives of the J-CAT are pro-active, intelligence-led and coordinated actions against cyber-crime. Its approach can be staged into:

- Identification of cases
- Preparation of prioritised cases
- Investigation and operational activities

[69] Europol. 2017. European Cyber-crime Centre - EC3 | About Europol | Europol. [ONLINE].
[70] Ibid.

- Prosecution of investigated cases[71]

J-CAT focuses on the most important international cyber-crime cases that have impact on Member states and their citizens. It also coordinates its operations with the FBI in order to dismantle international cyber-criminal groups. It had successfully taken down over 610 ".onion" websites running on Tor network, which were providing criminal services in November 2014 and two years later it has dismantled "Avalanche" network, arrested 5 criminals in 4 countries and seized 39 servers.[72]

The economics of hacking

Peter T. Leeson and Christopher J. Coyne managed to describe hacking markets. They assume that hackers can be either fame-driven or profit-driven.[73]

Fame-driven hacker market model consists of two components, fame and the quantity of hacking. Supply side of the model reflects producers of exploits who search for fame. The supply curve is conventionally positively shaped. The idea behind this is that the more famous the hackers become the more motivated they are to release new hacking tools and exploits. If their notoriety decreases their motivation also decreases. The position of the curve is given by the number of hackers in the community and the fixed and variable costs of the hackers. Their fixed costs are expenses that have to be paid for their hardware and software equipment, and variable costs denote mostly electricity. The demand side differs from conventional approach. The more exploits and hacking tools are released by the hackers, the more new information becomes available to further development and the hacking community is happier. Hence more fame is given to hackers. The reaction function of the hacking community reflects changes of fame given to different amounts of exploits supplied by hackers and is also positively sloped.[74] Two options are possible:

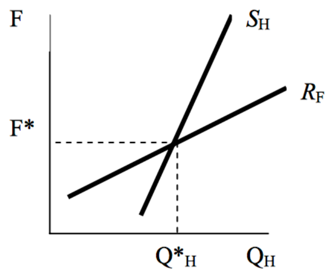


Figure 1.

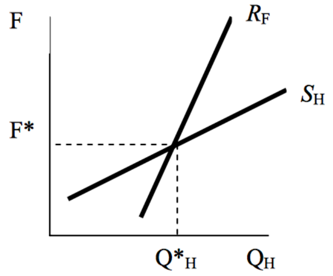


Figure 2.

Figure 1. represents better responsivity of hackers to fame variability and the supply curve is less elastic. In figure 2. it is the community of hackers which is more responsive to variability in fame.[75]

[71] Ibid.
[72] EC3. 2017. Europol Unclassified - Basic Protection Level. [ONLINE].
[73] Peter T. Leeson, Christopher J. Coyne. 2005. The Economics of Computer Hacking. [ONLINE].
[74] Ibid.
[75] Ibid.

Market for profit-motivated hackers is represented by conventional price and quantity space, where the behaviour of suppliers and demanders equilibrates by price. Supply curve is positively sloped unlike demand curve. The larger quantity of exploits or hacking activities is provided by hackers the more they are rewarded and oppositely. If hackers charge more, lower quantity of hacking is demanded and vice versa. The price elasticities are not expected to be extreme for supply nor for demand for exploits or hacking activities. The position of these curves is also traditional. The only irregularity is the *black hats* specific higher reward due to the risk they are undertaking. Hence it is assumed that equilibrium for market of *black hats* is above the one for *white hats.* According to Leeson the rates of return comparison between these two profit-driven markets involve analysis of flows of hackers between the legal and illegal sector and their competition. Leeson adds, that more profitable *white hats* market could be beneficial for society at two points – less illegal activities and increase in security awareness.[76]

The cost of cyber-crime

Estimating cost of cyber-crime is limited due to unavailability of data and methodologies. Information breaches are hard to evaluate as it is complicated to estimate the probability of cyber-attack. Companies aren't exactly willing to publish information on such breaches themselves. However, it is very like it will have certain negative effects. **Financial markets** may become sceptic and react negatively on any information about information breach. Investors may start to perceive victim company as too much risky and short their positions. It would lead to negative publicity and affected the company`s **reputation**, giving its competitors advantage. Furthermore, the investors as well as customers may be taking even legal action. Litigation and **liability concerns** are another reason for not publishing the report willingly.[77] Also, it is a gesture against the attackers.[78]

According to OECD, Stuxnet malware exploited up to four unknown vulnerabilities at once. It was built to stay undetected over multiple channels by redistributing into removable devices over LAN network. Once it has reached a maximum number of infections, system triggers self-destruction. In 2010, Symantec has recorded circa 100 000 hosts infected by Stuxnet virus.[79] Due to the sophistication of the virus experts valuated Stuxnet development worth USD 10 million.[80] Consumer strikes become also more frequent. According to results of the Norton Survey on Consumer Cyber-crime from 24 countries involving over thirteen thousand adults there has been 556 million cyber-crime victims in past year. Exploitation through social media becomes as well more frequent.[81] Survey held in 2012 by Symantec estimated cost of cyber-crime in USA at USD 21 billion, USD 16 billion in Europe and over 46 billion in China. The global average cost of consumer cyber-crime was USD 110 billion. In 2015, it was USD 3 trillion.

[76] Ibid.

[77] CRS Report for Congress. 2004. The Economic Impact of Cyber-Attacks. [ONLINE].

[78] Ibid.

[79] OECD (2012a), Internet Economy Outlook 2012, Paris: OECD Publishing.

[80] Hesseldahl Arik. 2010. 2010 Was the Year the Internet Got Scary. Get Used to It.. [ONLINE].

[81] Symantec. 2013. 2012 NORTON CYBER-CRIME REPORT. [ONLINE].

E-commerce is at risk as well as it is widely used for both B2B and B2C relationships.[82] The value of e-commerce in 2016 was USD 1.914 trillion, accounting for 8.7% of total retail spending worldwide and is expected to reach 4.058 trillion in 2020.[83] There is increasing ratio of targeted attacks, in the UK more than 70% of medium to large companies admitted to having been victim of ATP, with global average 116 per day.

Companies estimate cost of cyber-crime by considering their spending on risk reduction and potential loss elimination. They may have to invest into building new and safer operating procedures and into protective software and hardware. Further costs due to damages involve repair costs, recovery costs. Cyber-activists aim to strike and shut down online operations. Victim then may be forced to shut down its payment services[84] and lose sales and would be risking closing down the business. There has been annual increase in cyber-crime costs, unfortunately many cyber-attacks stay hidden, which makes it difficult to estimate the total losses. Market value of a company is at stake once the information about the attack is announced through television broadcast or social media. We could expect losing faith of the company`s investors if their assets, personal details or transaction information is insecure. According to McAfee, cyber-crime is the reason for slower pace of global innovation, affecting international trade, innovation or global economic growth.[85]

Cyber security and information breaches has been topic of a large number of researches (Anderson and Moore[86], Eisenstein[87], Shackelford[88], Winn and Govern[89], Geers[90], Kundur et al.[91], Brockett et al.[92], Odulaja and Wada[93]), but literature on the cyber-crime impact on EU companies is still rather small. Becoming a victim of cyber-crime may have direct impact on company`s health. Firms can face lower sales revenue, fall in profits, reputation damage, decrease in market value and dividends.[94][95] The way cyber-crime affects firms can be calculated by measuring the market value as it reflects the investors` confidence. Campbell et

[82] Khurana Ajeet. 2016. Ecommerce Security Is of Paramount Importance. [ONLINE].
[83] Emarketer. 2016. Worldwide Retail Ecommerce Sales Will Reach $1.915 Trillion This Year. [ONLINE].
[84] Hinks Jamie. 2013. Anonymous hackers plead guilty to Paypal shutdown. [ONLINE].
[85] McAfee. 2014. Economic impact of cybercrime II. [ONLINE].
[86] Anderson, R.,, Moore, T., 2008. Information Security Economics – and Beyond. In Deontic Logic in Computer Science - Lecture note in computer science 5076, 49.
[87] Eisenstein, E.M., 2008. Identity theft: An exploratory study with implications for marketers Journal of Business Research 61, 1160–1172.
[88] Shackelford S.J., 2008. From Nuclear War to Net War: Analogizing Cyber Attacks in International Law. International Law 27 (1), 191-251.
[89] Winn, J., Govern, K., 2009. Identity theft: risks and challenges to business of data compromise. Journal of Science Technology & Environmental Law 28 (1), 49-63.
[90] Geers, K., 2010. The Challenge of Cyber Attack Deterrence. Computer Law & Security Review 26 (3), 298-303.
[91] Kundur, D., Feng, X., Mashayekh, S., Liu, S., Zourntos, T., Butler-Purry, K.L., 2011. Towards modelling the impact of cyber attacks on a smart grid. International Journal of Security and Networks 6 (1), 2-13.
[92] Brockett, P.L., Golden L.L., Wolman W., 2012. Enterprise cyber risk management, in Risk management for the future – Theory and cases, Jan Emblemsvag.
[93] Odulaja, G.O, Wada, F., 2012. Assessing Cyber crime and its Impact on E-Banking In Nigeria Using Social Theories. African Journal of computing & ICTs 4 (2), 69-82.
[94] Power, R., 2002. CSI/FBI 2002 Computer Crime and Security Survey. Computer Security Issues and Trends 18 (2), 7-30.
[95] Gordon, L.A., Loeb, M.P., Lucyshyn W., 2003. Information security expenditures and real options: a wait-and-see approach. Computer Security Journal 19 (2), 1-7.

al.[96], Cavusoglu et al.[97], Hovav and D'Arcy[98] have estimated the cyber-crime impacts on the market stocks. They applied the event study methodology to assess the impact of an event on the value of a firm. Implicit and explicit costs to firms due to information security breaches are analysed by Iheagwara[99]. Power[100] presents his survey results and shows how these breaches may cause significant financial losses for firms. Results of Campbell[101] suggest that the type of information breach influences Cumulative Abnormal Returns (CAR). Announcement of a cyber-crime is believed to result into a negative CAR. Campbell et al.[102] suggest there is a highly significant negative reaction of investors on cyber-attacks when confidential data were breached. Cavusoglu et al.[103] focused on market value change in a time window of 2 days from announcement of a breach. His results suggest that firms lost average 2,1% of their market value. Another research suggesting significant market reactions to cyberattack reports in 10 days was held by Ishiguro et al.[104]. He also found that reactions in the US stock market are faster than in Japanese market. Statistically significant negative impact on stocks on the announcement day was measured by Acquisti et al.[105]

[96] Campbell, K., Gordon, L., Loeb, M., Zhou, L., 2003. The economic cost of publicly announced information security breaches: Empirical evidence from the stock market. Journal of Computer security 11, 431-448.

[97] Cavusoglu, H., Mishra, B., Raghunathan, S., 2004. The effect of Internet security breach announcements on market value: capital market reactions for breached firms and Internet security developers. International Journal of Electronic Commerce 9, 69-104.

[98] Hovav, A., D'Arcy, J., 2004. The impact of virus attak on the market value of firms. Information System Security 13 (3), 32-40.

[99] Iheagwara, C., Blyth, A., Singhal, M., 2004. Cost effective management frameworks for intrusion detection systems. Journal of Computer Security 12, 777-798.

[100] Power, R., 2002. CSI/FBI 2002 Computer Crime and Security Survey. Computer Security Issues and Trends 18 (2), 7-30.

[101] Campbell, K., Gordon, L., Loeb, M., Zhou, L., 2003. The economic cost of publicly announced information security breaches: Empirical evidence from the stock market. Journal of Computer security 11, 431-448.

[102] Ibid.

[103] Cavusoglu, H., Mishra, B., Raghunathan, S., 2004. The effect of Internet security breach announcements on market value: capital market reactions for breached firms and Internet security developers. International Journal of Electronic Commerce 9, 69-104.

[104] Ishiguro, M., Tanaka, H., Matsuura, I., Murase, I., 2007. The effect of information security incidents on corporate values in the Japanese stock market. In Workshop on the Economics of Securing Information Infrastructure, Arlington.

[105] Acquisti, A., Friedman, A., Telang, R., 2006. Is there a cost to privacy breaches? An event study. Workshop on the Economics of Information Security, Cambridge, UK.

Event cases

This chapter introduces events that are subjects of this analysis.

WannaCry attack

The “WannaCry” ransomware is a global cyber-attacking tool that has affected more than 200 000 organisations in 150 countries. In the United Kingdom, it has affected 47 National Health Services (NHS) trusts and caused mass cancelling of operations patients were turned away from Accident & Emergency (A&E). The vulnerability was published by According to Symantec, the virus has used a flaw in Microsoft`s Windows SMB Server Remote Code Execution Vulnerability.[106] It consists of two parts, where the worm module spreads the virus and the ransom module encrypts data on victim`s computer and demands payment – ransom. WannaCry worm demanded approximately $300 in Bitcoin within first three days and $700 within seven days.[107] The malicious file is usually included in e-mail as an attachment. Once it is downloaded and it locks the data, only two files are available to the user: instructions on how to proceed and the WannaCry program itself. Symantec also informs that the security flaw impacts all versions of the Windows operating systems running file protocol SMBv1 which can digitally sign communications and confirm the recipients` authenticity.[108] Furthermore, the virus attempts to install Tor domains, which provide a unique Bitcoin payment address and decryption keys if the victim paid the ransom. The propagation of the worm involves spreading over local network but it can also spread to any computer by generating potential target IP addresses randomly.[109]

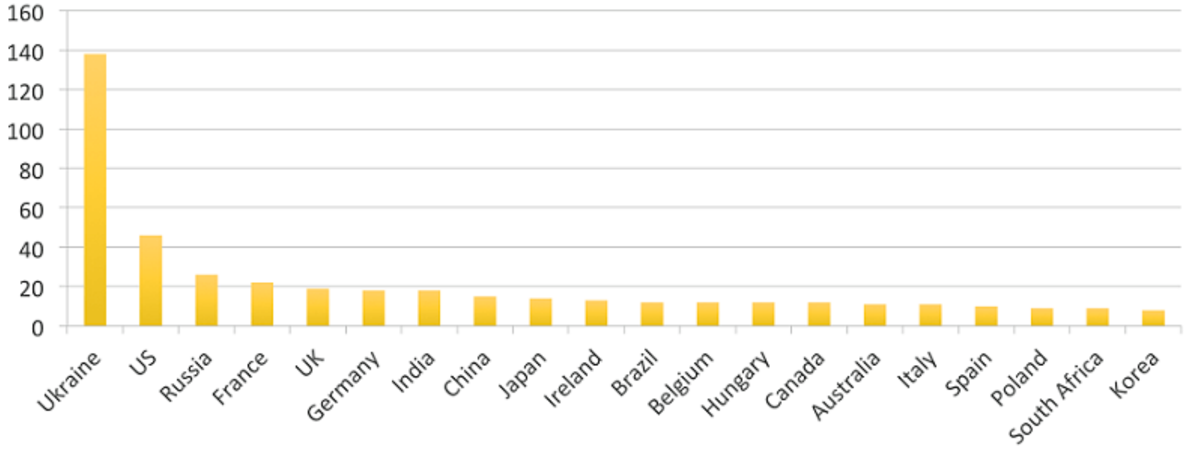
Microsoft Windows has released patches to these vulnerabilities on March 14. 2017, a month before they were published by hacker group called The Shadow Brokers after their unsuccessful attempt to sell the leaked materials.[110] According to the statement of The Shadow Brokers these vulnerabilities and exploits were initially used by the Equation Group threat actor, tied to NSA`s Tailored Access Operation Unit[111] against enterprises firewalls, anti-virus programs and Microsoft products.[112] This information is even supported by the Kaspersky lab report indicating connection between Equation Group and the makers of Stuxnet.[113] The worm module included piece of code that checked for availability of certain domain and the virus stopped spreading itself if the domain was reachable. This “kill switch” was used to stop WannaCry malware spreading, as the domain was purchased.[114] As of 14 June 2017, a total of 327 payments totalling $130,634.77 had been transferred according to online Bitcoin wallet checker.[115] The economic costs of WannaCry typically include business interruptions and

[106] Symantec Security Response. 2017. Ransom.Wannacry. [ONLINE].
[107] Ibid.
[108] Ibid.
[109] Ibid.
[110] Ibid.
[111] Goodin Dan. 2016. Confirmed: hacking tool leak came from “omnipotent” NSA-tied group. [ONLINE].
[112] Ibid.
[113] Kaspersky Lab. 2015. Equation Group: Questions and Answers. [ONLINE].
[114] The Guardian. 2017. Briton who stopped WannaCry attack arrested over separate malware claims. [ONLINE].
[115] "@actual_ransom tweets". Twitter. Retrieved 19 May2017.

repairs. Risk-modelling firm Cyence estimated economical cost of the attack to reach $6 billion global cost.[116] No hacker group claimed responsibility for the attack.

Petya attack

Within two months from the WannaCry attack, another global cyber-attack called "Petya" started spreading and affecting companies, public institutions as well as infrastructure. It also spreads through local networks that use Microsoft Windows operating systems and although it also demands a ransom $300 to be paid in Bitcoin, it differs in critical point – it fails to provide a way for victims to recover the encrypted data. It is unknown whether purposely or not.[117] According to MalwareTech security article this worm was not designed to extort and make money but to cause damage and destroy.[118] The infections started in Ukraine where more than 80 companies were hit. Estimates released on 27 July 2017 by Symantec show list of top 20 countries based on numbers of affected companies:

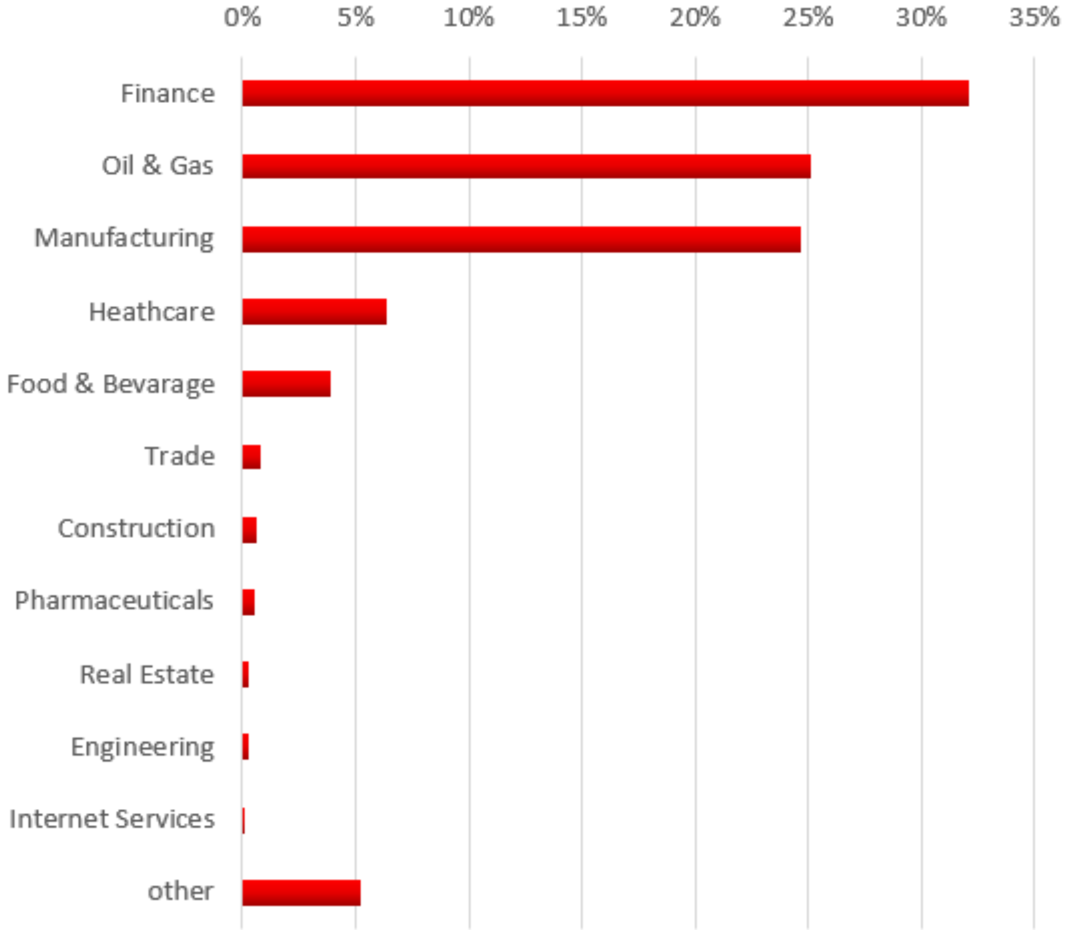


Picture: Top 20 countries affected by Petya attack[119]

However, Dmitry Peskov, press secretary of Russian president Vladimir Putin stated that the attack has caused no serious damage to Russia.[120] In contrast to this, British advertising company WPP belongs between those to say its IT systems had been struck down. Nurofen maker Reckitt Benckiser said the cyber-attack disrupted production and deliveries of goods to customers in several countries. It has estimated $100 million hit in its revenue. This resulted in 1% drop in growth forecast for Reckitt. Among other affected publicly traded companies belong Danish shipping company AP Moller Maersk which had been forced to redirect ships to alternative locations as the virus left its computer systems unable to dock and unload containers at some of its ports.[121] Some of the other affected companies are: German personal-care company Beiersdorf AG, Deutsche Post, one of the largest pharmaceutical companies

[116] Barlyn Suzanne. 2017. Global cyber attacks could trigger economic losses on par with catastrophic natural disasters. [ONLINE].
[117] Fortune. 2017. Petya Attack: Watch 'NotPetya' Malware Wreck a Computer | Fortune.com. [ONLINE].
[118] MalwareTech. 2017. Petya Ransomware Attack – What's Known. [ONLINE].
[119] Symantec, (2017), Top 20 countries affected by Petya attack [ONLINE].
[120] BBC News. 2017. Tax software blamed for cyber-attack spread - BBC News. [ONLINE].
[121] The Guardian. 2017. Massive cyber-attack could cost Nurofen and Durex maker £100m | Business | The Guardian. [ONLINE].

Merck & Co, Russian Oil company Rosneft or French construction material producer Saint Gobain.[122] All companies mentioned above are subject of this analysis.
According to McAfee security engineer the Petya attack targeted also energy companies, the power grid, bus stations, gas stations and banks.[123] Kaspersky Security Networks shows that at least 50% of affected companies are manufacturing and oil & gas enterprises:



Picture: Petya targets by industry[124]

According to Cyence, Petya attack caused up to $850 million in economic losses. Lloyd informed that average losses for a scenario involving a hacking of operating systems ranged from $9.7 bn to $28.7bn.[125]

[122] Ibid.
[123] BBC News. 2017. Global ransomware attack causes turmoil - BBC News. [ONLINE].
[124] Kaspersky Security Networks, (2017), Petya targets by industry [ONLINE].
[125] Suzanne Barlyn. 2017. Global cyber attacks could trigger economic losses on par with catastrophic natural disasters. [ONLINE].

Methodology

An event study methodology has been used to assess the impact of cyber-crime events on market value of companies affected during ransomware attacks in 2017. List of companies was selected given these restrictions and limitation:

1) Only companies with publicly traded status were included.
2) Companies originating in Europe were selected, including one company traded on US stock market and one company where major shareholder is the Russian government.
3) The data`s availability to public.

The data was obtained using Yahoo Finance historical data. MacKinlay explains the general methodology of an event study as *measuring the impact of a specific event on the value of a firm, using financial market data.*[126] According to Chen, the short-horizon event studies are more reliable than long-horizon event studies.[127] Assuming that financial markets react to news, Acquisti suggest that financial losses will be shown in the company`s stock price.[128] The idea behind this assumption is that stock market returns can capture both implicit and explicit costs of the fraudulent activity. The economic cost of cyberattack will be captured in the following days after the information was revealed. According to Fama, the event study methodology stands on assumption of semi-strong efficient market hypothesis, which implies that all public information is calculated into a stock`s current price.[129]

First step is to calculate abnormal returns (AR) which present forecast errors of a normal return generating mode. Abnormal returns are represented as the stock return of a firm obtained on a day of the event minus the expected stock return. Abnormal returns were estimated using single-index model developed by William Sharpe in 1963, involving OLS regression of the stock returns on day *t* on return on market index on day *t* for 120 days prior to the event. Model that is used to measure the normal return Ri,t is:

$$R_{i,t} = \alpha_i + \beta_i R_{m,t} + \varepsilon_{i,t}$$

Where Ri,t is the rate of return for stock *i* of the victim company on day *t*, Rm,t is the rate of return on market index on day *t*, calculated without the risk free rate (Rf). The risk component of share *i* is shown as coefficient α_i, and β_i is the beta coefficient of share *i.* The random error is expressed as $\varepsilon_{i,t}$. For my thesis, I select following European indexes: CAC 40 Paris, DAX Frankfurt, OMXC 20 Copenhagen, LSE London, MICEX Moscow, IBEX 35 Madrid. In order to evaluate performance of antivirus companies, NASDAQ index has also been included. The ARi,t is calculated over the estimated period as:

$$AR_{i,t} = R_{i,t} - (\alpha_i + \beta_i R_{m,t})$$

[126] MacKinlay, A. C. 1997 “Event Studies in Economics and Finance,” Journal of Economic Literature Vol. XXXV, Issue 1.

[127] Chen, M.Y., 2014 'I Just Did 400 Million Event Studies' – A Study of Market Model Robustness and Deterioration in Times of Crisis.

[128] Acquisti, A., Friedman, A., Telang, R., 2006. Is there a cost to privacy breaches? An event study. Workshop on the Economics of Information Security, Cambridge, UK.

[129] Fama, E.F., Fisher, L., Jensen, M., Roll, R., 1969. The adjustement of stock prices to new information. International Economic Review 10, 1-21.

The date of the announcement of the cyber-attack is defined as day zero, being set within the event window defined as range of -τ1 days before and +τ2 day after the event. Various event windows with different lengths were considered: (-20;20), (-10;10), (-5;5), (-3;3), (-1;1).

The calculation of the average abnormal returns for *n* firm stocks on day *t* is done as follows:

$$AAR_t = \frac{1}{N}\sum_{i=1}^{N} AR_{i,t}$$

Cumulative abnormal return (CAR) is then measured over the event window and calculated as:

$$CAR_i = \sum_{t=T_1+1}^{T_2} AR_{i,t}$$

Where the event window *i* is presented as (τ1, τ2).

The average CAR is then calculated for the event period as follows:

$$CAAR = \frac{1}{N}\sum_{i=1}^{N} CAR_i$$

Where *n* denotes the number of events.

Testing the statistical significance of average CAR will show whether there was increased volatility in return, caused by the cyber-attack. Cross sectional test has been applied, using the Brown and Warner[130]:

$$t_{CAAR} = \sqrt{N}\,\frac{CAAR}{S_{CAAR}}$$

Where S_{CAAR} is the standard deviation of the cumulative abnormal returns across the sample, calculated as:

$$S^2_{CAAR} = \frac{1}{N-1}\sum_{i=1}^{N}(CAR_i - CAAR)^2.$$

The t-test has a t-distribution of N-1 degrees of freedom.

[130] Brown, Stephen J., and Jerold B. Warner. "Measuring Security Price Performance", Journal of Financial Economics, 1980, 8(3), 205-258.

Results

Results are divided into three sections, where first two refer to two recent cyber-attacks: Ransomware attack "Wannacry" that happened on 12. 5. 2017 and more aggressive Ransomware attack "Petya" that occurred on 27. 6. 2017 which, unlike Wannacry, aimed to delete affected data. Third section shows performance of antivirus companies during Petya attack event. Following results show test values at the 90% confidence level or higher. Mean Cumulative Abnormal Returns are shown for event windows (-20;20), (-10;10), (-5;5), (-3;3) and (-1;1) for three companies involving Renault SA, Portugal Telecom and Telefonica.

Table: Test statistics for CAARs for the sample during Wannacry attack:

Event window	No of firms	Mean CAR	T-test	P-value	T-critical
(-20;20)	3	-0.005286779	-0.186057714	0.565219325	2.91998558
(-10;10)	3	0.017351469	2.622463566	0.05991289*	1.885618083
(-5;5)	3	0.042276027	0.996448228	0.212009619	2.91998558
(-3;3)	3	-0.005897352	-0.396965906	0.6351262	2.91998558
(-1;1)	3	-0.005413494	-0.445182742	0.650132923	2.91998558

*Statistically significant at 10% (one-tailed test)

**Statistically significant at 5% (one-tailed test)

***Statistically significant at 1% (one-tailed test)

This table shows that statistically significant results were measured for event window (-10;10) and the impact was positive so that it did not lead to negative returns for these companies, although the mean CAR was negative during the shorter event windows as well as in the longest event window. These results are partially consistent with previous literature, stating that often, but not always, cyber-attacks have a significant negative impact.

Following table focuses on Petya attack, which affected companies and institutions from all over the world. The sample includes AP Moller Maersk, Beiersdorf AG, Deutsche Post, Reckitt Benckiser, Rosneft, Saint Gobain and WPP.

Table: Test statistics for CAARs for the sample during Petya attack:

Event window	No of firms	Mean CAR	T-test	P-value	T-critical
(-20;20)	8	0.201577856	2.459042634	0.02176318**	1.894578605
(-10;10)	8	0.124208463	2.839810491	0.012525706**	1.894578605
(-5;5)	8	0.065094935	2.50134103	0.020455932**	1.894578605
(-3;3)	8	0.043474614	2.994467186	0.010049426**	1.894578605
(-1;1)	8	0.017436205	1.874678375	0.051483898*	1.414923928

*Statistically significant at 10% (one-tailed test)

**Statistically significant at 5% (one-tailed test)

***Statistically significant at 1% (one-tailed test)

This table shows potential differences between two kinds of attack and reflects reactions of the investors to the more aggressive character of the Petya attack. Statistical significance was measured for all event windows. Paradoxically, the aggressiveness of this attack does not lead to negative returns either. We can see that there was steeper increase in returns from the first day of the announcement, as it takes a while until the news reach investors, in addition it may be explained by the fact, that stakeholders also wait for firms` reaction to becoming a victim of a cyber-attack. Furthermore, it may reflect trust of investors and expected future growth of European markets. Ultimately, this attack did not involve mass redistribution of stolen personal information as cyber-attacks had in the past. Given a closer look on details of this analysis, it is worth showing that oil company Rosneft, with major stakeholder, the Russian government, showed statistically significant abnormal returns starting from two days after the attack:

Table: Parametric T-test for Abnormal returns of Rosneft company

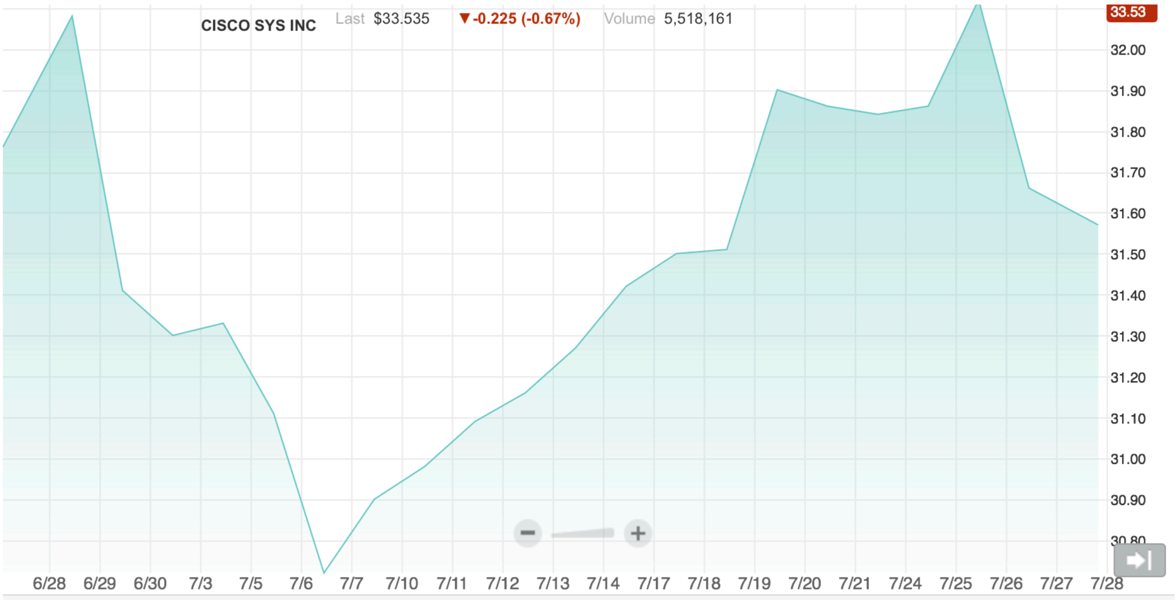
Event time t	Abnormal returns	T-test	Significance as AR/St.err > 1.96
0	0.008055879	0.804554626	no
1	0.010138474	1.012547001	no
2	0.026942149	2.690759207	yes
3	0.021876424	2.184836497	yes
4	0.037871017	3.782244205	yes
5	0.032792211	3.275015087	yes

This table represents strong performance of the oil company, although it underwent a powerful hacking attack. Despite the fact that it could lead to serious consequences, the company has *moved to a reserve production processing system and neither oil output nor refining have been stopped.*[131] Such announcements seem to be supporting the investors` confidence about the company`s future performance. WannaCry and Petya attacks affected computer networks on a broad scale and the results may be distorted by the limited size of the sample due to data availability. This may also explain why no significant negative results were found in my analysis.

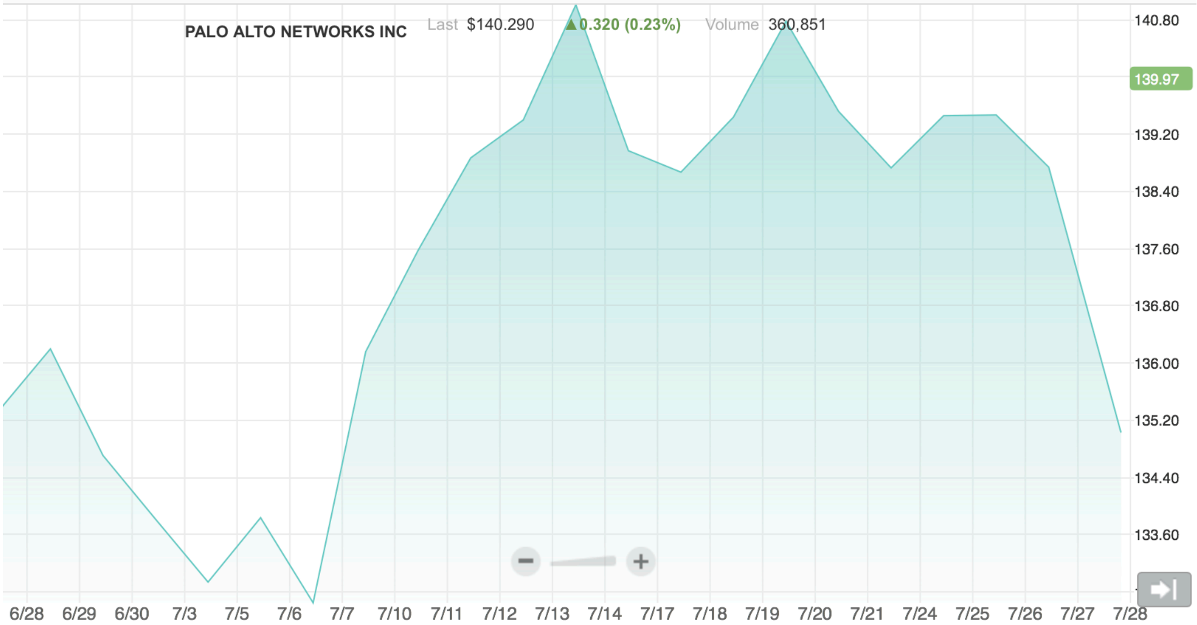
Finally, I present consequences of cyber-attacks on stock returns of antivirus companies. This sample includes six largest publicly traded antivirus companies, and has been created after recent merges which happened in the internet security market: Cisco, Fireeye, Palo Alto Networks, Science Application International Company, Sophos and Symantec.
Stock prices of antivirus companies are shown in following charts for period 06/27/2017 - 07/27/2017:

[131] U.S.. 2017. Russia's Rosneft says hit by cyber attack, oil production unaffected | Reuters. [ONLINE].

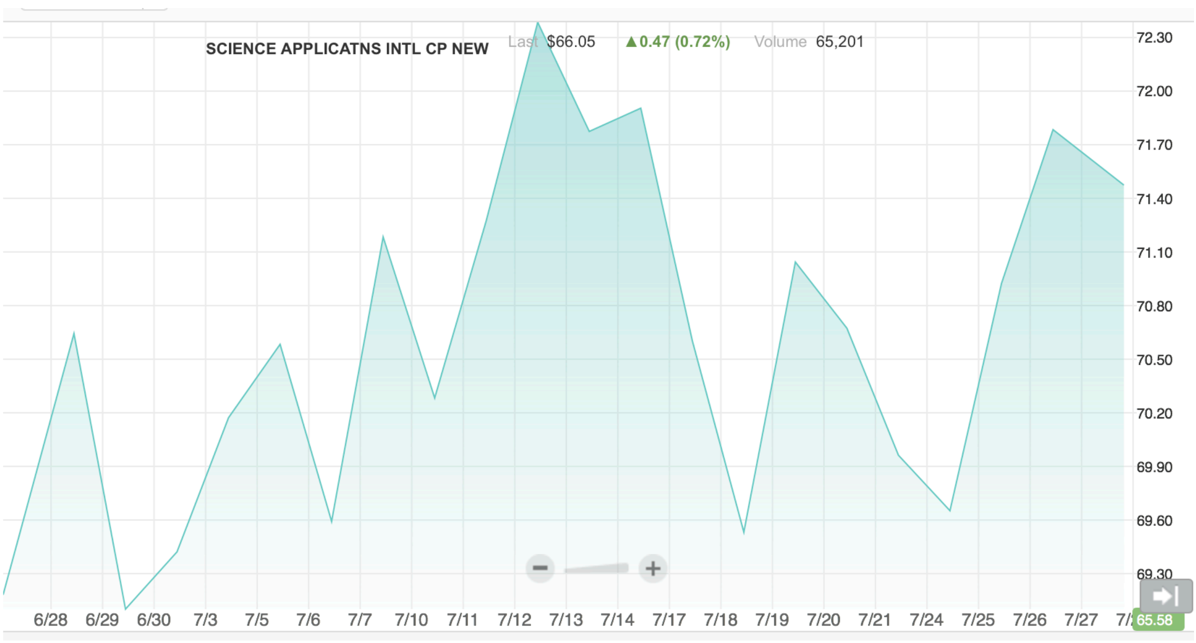
CISCO stock prices after the attack:



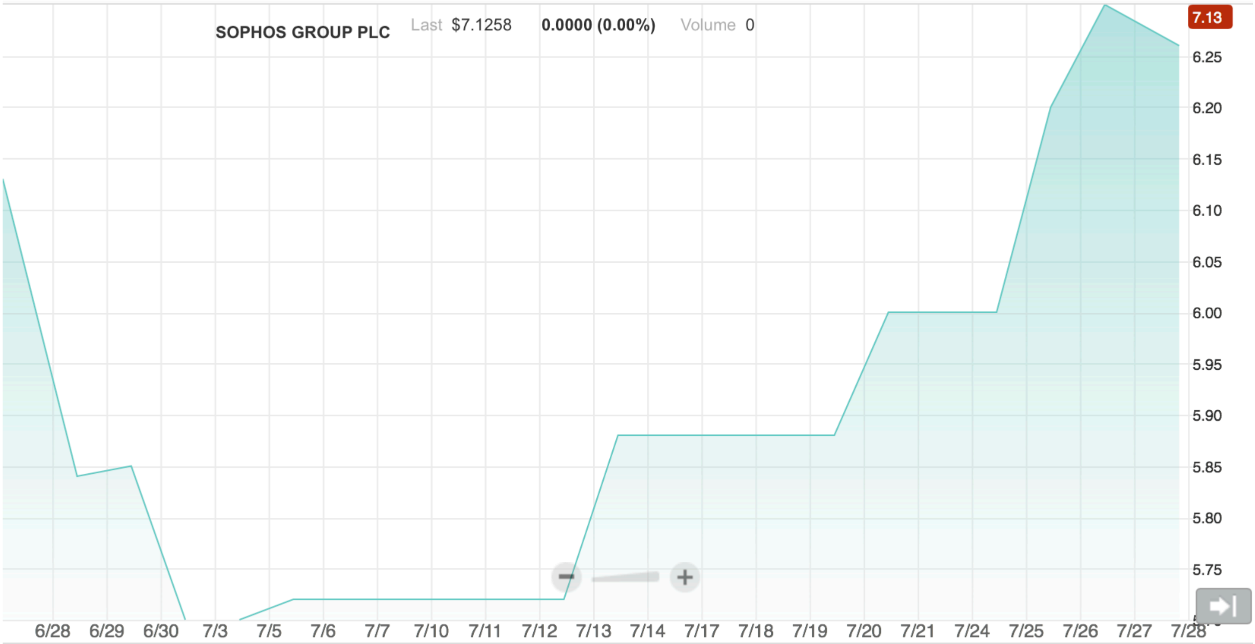
Palo Alto Networks stock prices after the attack:



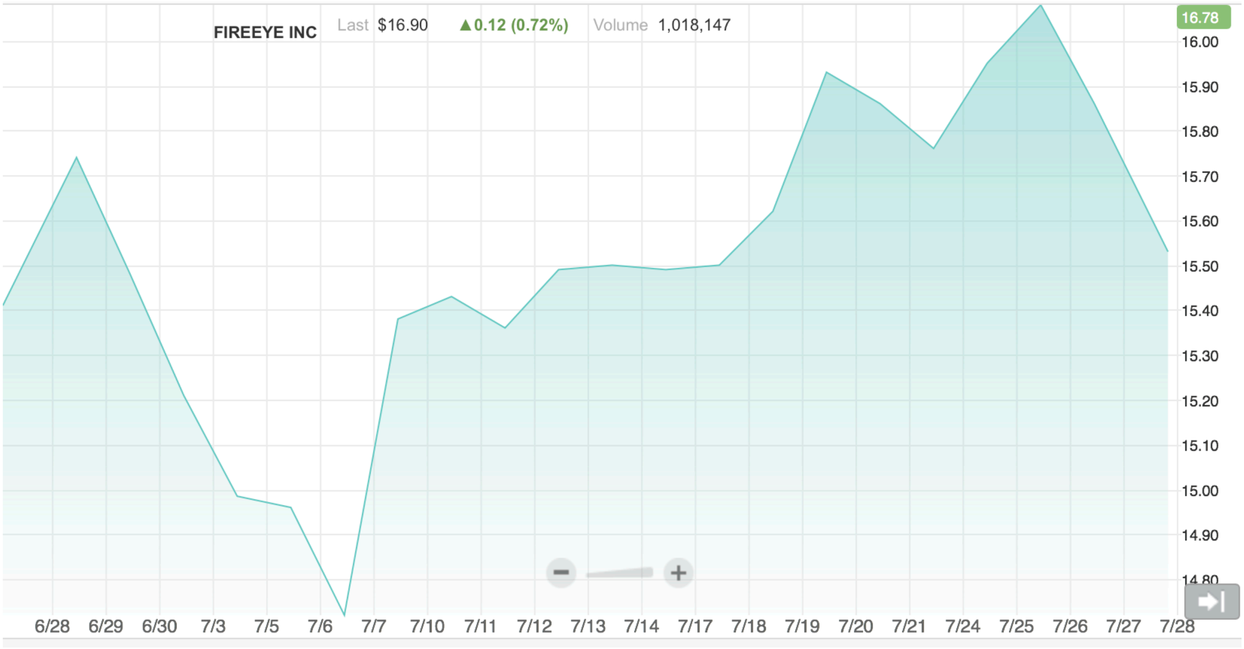
Science Application International Corporation stock prices after the attack:



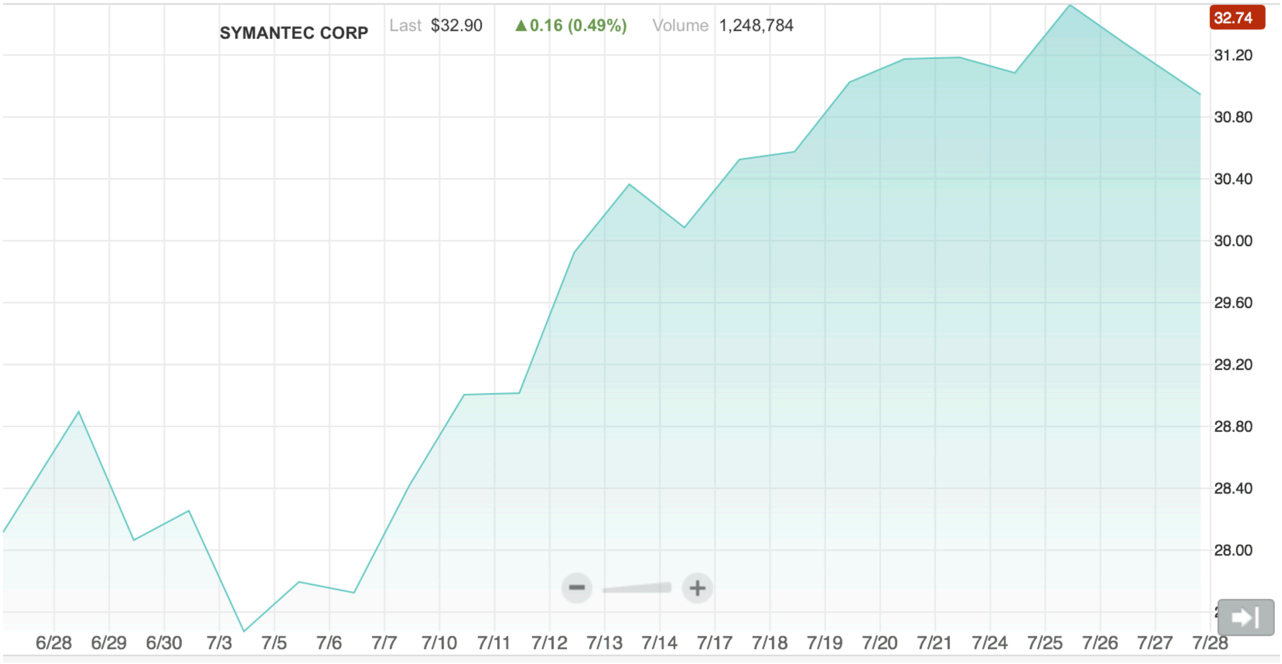
Sophos Group stock prices after the attack:



FireEye Inc. stock prices after the attack:



Symantec stock prices after the attack:



Source: NASDAQ interactive charts, period (06/27/2017 - 07/27/2017)

Table: Test statistics for CAARs for the sample of antivirus companies during Petya attack:

Event window	No of firms	Mean CAR	T-test	P-value	T-critical
(-20;20)	6	0.09322324	1.894773386	0.058321556*	1.475884049
(-10;10)	6	0.011234323	0.318483173	0.381495942	1.475884049
(-5;5)	6	-0.012900289	-1.410426493	0.891256276	1.475884049
(-3;3)	6	-0.008141476	-0.974711192	0.81276539	1.475884049
(-1;1)	6	-0.015548948	-3.507612907	0.991427835	1.475884049

*Statistically significant at 10% (one-tailed test)

**Statistically significant at 5% (one-tailed test)

***Statistically significant at 1% (one-tailed test)

This table show results at statistical significance at the 90% confidence level or above. Furthermore, it proves that the cyber-attack has affected antivirus companies` returns significantly only in the longest event window (-20;20), although that cumulative abnormal returns were negative for five days from the day of the announcement. Thus, news on information breaches may possibly lead antivirus companies to positive returns. Eventually, first days of negative abnormal returns may reflect uncertainty brought by wide cyber-attack. Following change in CARs` direction may imply probable increase in demand for services of these firms as repair or preventive actions taken by victims. Hence, according to Zack Equity Research a cyber-attack may prove to be actually good for companies, as investors buy shares, shooting up share prices.[132]

[132] Zacks Equity Research. 2017. Cybersecurity Stocks Shoot Up on Petya Ransomware Attack. [ONLINE].

Conclusions

Cyber-crime presents a significant problem for publicly traded companies, however the type of cyber-attack matters. This study estimates the impact that the announcements of cyber-security breaches have on market returns. This analysis focuses on consequences of two worldwide ransomware attacks, “Wannacry” and “Petya attack” which had hit publicly traded companies and other institutions in more than 150 countries on 12.5.2017 and 27.6. 2017 respectively.

Literature review provides description with general information on cyber-crime topic, including evaluation of different cyber-attacks, differentiating between cyber-terrorists, hacktivist or hacker engaging in corporate espionage for instance. This part also introduces many researches held on the topic of the evaluation of the economic cost of cyber-crime. There is a prevailing opinion, that public announcements of cyber-security breaches lead to negative cumulative abnormal returns over an event window, which captures both implicit and explicit costs of the cyber-attack. Therefore, an event study methodology has been used to evaluate the impact of ransomware attack.

The sample used for this analysis involves 11 affected firms and 6 antivirus companies. As my results suggest, the announcements of information breaches due to ransomware exploits have impact on stock market returns. Specifically, I found evidence of mostly positive investors` reactions to the announcements. Results are divided accordingly to the sample partition.

First section suggests that there was only little impact of “Wannacry” ransomware attack on market returns. Although stock market reactions differ by the sector, the market was positively affected in general. This ransomware attack did not affect any intraday operations of these firms and apparently, announcements of PR sections of affected companies led to strengthening of their investors` confidence.

Second section analyses the impact of more aggressive “Petya attack”, that aimed to destroy affected data. Surprisingly, found evidence proves, that such an information security breach leads to increased market returns. In particular, for the 95% confidence level, the sample shows a positive and statistically significant cumulating of abnormal returns starting since the third day from the announcement. These figures do not match results of previous literature related to the impacts of cyber-attacks. However, the reason for this, is the specific character of the ransomware exploits. This analysis proves, that neither cyber-extortion nor cyber-blackmailing will result into loss of investors` confidence.

Third section of this analysis focuses on the impact of the “Petya” ransomware attack on market returns of antivirus companies. Results of this section have expectable implications. Statistically significant results were found for 90% confidence level in the longest event window (-20;20). Although during first days after the attack the stock market reactions were negative, but not significant, Cumulative Abnormal Returns switched to positive values after few days later, as both government and companies spending on information security is expected to increase.

This thesis managed to evaluate the impact of ransomware related cyber-crime on the companies` financial health. Results have strikingly interesting implications, especially when suggesting that ransomware attacks lead companies to positive market returns. Cyber-crime though, still represents a threat to companies and other types of cyber-attacks deserve to be further investigated. Different IT exploits may have different consequences and could be potentially leading to damage on firms` reputation. Thus, it is necessary for companies to avoid becoming victim of cyber-crime. Information systems should be continuously monitored and background checks are needed to be done for all employees. In addition, companies should have a plan of action for responding to information breaches. The ransomware attacks that are subject of this analysis are aiming to hit outdated operating systems, hence preventive measures should be emphasized, as they are not as costly as the repairs.

Reference

Online sources:

1. "@actual_ransom tweets". Twitter. Retrieved 19 May2017.
2. Barlyn Suzanne. 2017. Global cyber attacks could trigger economic losses on par with catastrophic natural disasters. [ONLINE] Available at: http://www.independent.co.uk/news/business/news/global-cyber-attacks-economic-losses-natural-disasters-catastrophic-petya-wannacry-cyence-a7844586.html. [Accessed 19 September 2017].
3. BBC News. 2017. Global ransomware attack causes turmoil - BBC News. [ONLINE] Available at: http://www.bbc.com/news/technology-40416611. [Accessed 17 September 2017].
4. BBC News. 2017. Tax software blamed for cyber-attack spread - BBC News. [ONLINE] Available at: http://www.bbc.com/news/technology-40428967. [Accessed 17 September 2017].
5. Brandom Russell. 2015. The MPAA has a new plan to stop copyright violations at the border. [ONLINE] Available at: https://www.theverge.com/2015/1/2/7481409/the-mpaa-has-a-new-plan-to-stop-copyright-violations-at-the-border. [Accessed 19 September 2017].
6. CAPEC - CAPEC-117: Interception (Version 2.11) . 2017. CAPEC - CAPEC-117: Interception (Version 2.11) . [ONLINE] Available at: http://capec.mitre.org/data/definitions/117.html. [Accessed 20 September 2017].
7. Cebula J. James, Young R. Lisa. 2010. A Taxonomy of Operational Cyber Security Risks. [ONLINE] Available at: http://www.sei.cmu.edu/reports/10tn028.pdf. [Accessed 20 September 2017].
8. Chris Nuttall, BBC. 1999. Kosovo info warfare spreads. [ONLINE] Available at: http://news.bbc.co.uk/2/hi/science/nature/308788.stm. [Accessed 19 September 2017].
9. CRS Report for Congress. 2004. The Economic Impact of Cyber-Attacks. [ONLINE] Available at: https://fas.org/sgp/crs/misc/RL32331.pdf. [Accessed 20 September 2017].
10. Cyber-crime - The Definition of Cyber-crime | Norton. 2017. Cyber-crime - The Definition of Cyber-crime | Norton. [ONLINE] Available at: https://us.norton.com/cyber-crime-definition. [Accessed 28 July 2017]
11. Dark Reading. 2017. 'Aurora' Attacks Still Under Way, Investigators .... [ONLINE] Available at: https://www.darkreading.com/attacks-breaches/aurora-attacks-still-under-way-investigators-closing-in-on-malware-creators/d/d-id/1132922. [Accessed 20 September 2017].
12. Davis Amanda. 2015. A History of Hacking. [ONLINE] Available at: http://theinstitute.ieee.org/technology-focus/technology-history/a-history-of-hacking. [Accessed 20 September 2017].
13. Denning E. Dorothy. 2000. Cyberterrorism threat. [ONLINE] Available at: http://palmer.wellesley.edu/~ivolic/pdf/Classes/Handouts/NumberTheoryHandouts/Cyberterror-Denning.pdf. [Accessed 19 September 2017].
14. Durden Tyler. 2016. The Incredible Story Of How Hackers Stole $100 Million From The New York Fed Tyler Durden's picture. [ONLINE] Available at: http://www.zerohedge.com/news/2016-03-10/incredible-story-how-hackers-stole-100-million-new-york-fed. [Accessed 8 August 2017].
15. EC3. 2017. Europol Unclassified - Basic Protection Level. [ONLINE] Available at: https://ccis.no/wp-content/pdf/2017-ccis-symposium/. [Accessed 15 September 2017].
16. Emarketer. 2016. Worldwide Retail Ecommerce Sales Will Reach $1.915 Trillion This Year. [ONLINE] Available at: https://www.emarketer.com/Article/Worldwide-Retail-Ecommerce-Sales-Will-Reach-1915-Trillion-This-Year/1014369. [Accessed 7 August 2017].
17. Europol. 2017. European Cyber-crime Centre - EC3 | About Europol | Europol. [ONLINE] Available at: https://www.europol.europa.eu/about-europol/european-cyber-crime-centre-ec3. [Accessed 25 July 2017].
18. Fortune. 2017. Petya Attack: Watch 'NotPetya' Malware Wreck a Computer | Fortune.com. [ONLINE] Available at: http://fortune.com/2017/06/30/petya-ransomware-video/. [Accessed 17 September 2017]
19. Gallagher Sean. 2016. Shamoon wiper malware returns with a vengeance. [ONLINE] Available at: https://arstechnica.com/information-technology/2016/12/shamoon-wiper-malware-returns-with-a-vengeance/. [Accessed 20 September 2017].
20. Goodin Dan. 2016. Confirmed: hacking tool leak came from “omnipotent” NSA-tied group. [ONLINE] Available at: https://arstechnica.com/information-technology/2016/08/code-dumped-online-came-from-omnipotent-nsa-tied-hacking-group/. [Accessed 17 September 2017].

21. Harper Jim. 2017. “There’s no such thing as cyber terrorism” — RT News. [ONLINE] Available at: https://www.rt.com/news/no-cyber-terrorism-obama/. [Accessed 20 September 2017].
22. Hesseldahl Arik. 2010. 2010 Was the Year the Internet Got Scary. Get Used to It.. [ONLINE] Available at: http://allthingsd.com/20101230/2010-was-the-year-the-internet-got-scary-get-used-to-it/. [Accessed 7 August 2017].
23. Hinks Jamie. 2013. Anonymous hackers plead guilty to Paypal shutdown. [ONLINE] Available at: http://www.itproportal.com/2013/12/11/anonymous-hackers-plead-guilty-paypal-shutdown/. [Accessed 8 August 2017].
24. Hornyak Tim. 2015. Hack to cost Sony $35 million in IT repairs. [ONLINE] Available at: https://www.networkworld.com/article/2879814/data-center/sony-hack-cost-15-million-but-earnings-unaffected.html. [Accessed 19 September 2017].
25. Kaspersky Lab. 2015. Equation Group: Questions and Answers. [ONLINE] Available at: https://securelist.com/files/2015/02/Equation_group_questions_and_answers.pdf. [Accessed 17 September 2017].
26. Kaspersky Security Networks, (2017), Petya targets by industry [ONLINE]. Available at: https://ics-cert.kaspersky.com/wp-content/uploads/sites/6/2017/06/1706-expetr-4.png [Accessed 17 September 2017].
27. Keizer Gregg. 2017. Hackers spied on 300,000 Iranians using fake Google certificate | Computerworld. [ONLINE] Available at: https://www.computerworld.com/article/2510951/cybercrime-hacking/hackers-spied-on-300-000-iranians-using-fake-google-certificate.html. [Accessed 20 September 2017].
28. Kent Anderson, Prague Post. 2017. Virtual hostage | Prague Post. [ONLINE] Available at: https://www.praguepost.com/opinion/5996-virtual-hostage.html. [Accessed 20 September 2017].
29. Khurana Ajeet. 2016. Ecommerce Security Is of Paramount Importance. [ONLINE] Available at: https://www.thebalance.com/ecommerce-security-is-of-paramount-importance-1141621. [Accessed 7 August 2017].
30. Lang Brent. 2015. WikiLeaks Publishes Thousands of Hacked Sony Documents. [ONLINE] Available at: https://variety.com/2015/film/news/wikileaks-sony-hack-1201473964/. [Accessed 19 September 2017].
31. Leeson T. Peter, Coyne J. Christopher. 2005. The Economics of Computer Hacking. [ONLINE] Available at: http://www.peterleeson.com/hackers.pdf. [Accessed 19 September 2017].
32. MalwareTech. 2017. Petya Ransomware Attack – What’s Known. [ONLINE] Available at: https://www.malwaretech.com/2017/06/petya-ransomware-attack-whats-known.html. [Accessed 19 September 2017].
33. Markoff John. 2017. A Code for Chaos - The New York Times. [ONLINE] Available at: http://www.nytimes.com/2010/10/03/weekinreview/03markoff.html. [Accessed 20 September 2017].
34. McAfee. 2014. Economic impact of cybercrime II. [ONLINE] Available at: https://www.mcafee.com/de/resources/reports/rp-economic-impact-cybercrime2.pdf. [Accessed 20 September 2017].
35. NIST Computer Security Resource Center (CSRC). 2017. NIST Computer Security Resource Center (CSRC). [ONLINE] Available at: http://csrc.nist.gov/index.html. [Accessed 07 August 2017].
36. Passeri Paolo, (2017), May 2017 Cyber Attacks Statistics [ONLINE]. Available at: https://i1.wp.com/www.hackmageddon.com/wp-content/uploads/2017/07/May-2017-Motivations.png?resize=800%2C415 [Accessed 7 August 2017].
37. Ransomware - Definition - Trend Micro USA . 2017. Ransomware - Definition - Trend Micro USA . [ONLINE] Available at: https://www.trendmicro.com/vinfo/us/security/definition/ransomware. [Accessed 10 August 2017].
38. Rouse Margaret. 2017. distributed denial of service (DDoS) attack. [ONLINE] Available at: http://searchsecurity.techtarget.com/definition/distributed-denial-of-service-attack. [Accessed 7 August 2017].
39. Sanger E. David. 2017. Obama Ordered Wave of Cyberattacks Against Iran - The New York Times. [ONLINE] Available at: http://www.nytimes.com/2012/06/01/world/middleeast/obama-ordered-wave-of-cyberattacks-against-iran.html?pagewanted=all&_r=0. [Accessed 20 September 2017].
40. SearchSecurity. 2017. What is advanced persistent threat (APT)? - Definition from WhatIs.com. [ONLINE] Available at: http://searchsecurity.techtarget.com/definition/advanced-persistent-threat-APT. [Accessed 07 August 2017].
41. Sher-Jan Mahmood. 2015. THE NEW ECONOMICS OF CYBER-CRIME. [ONLINE] Available at: http://www.isaca.org/cyber/cyber-security-articles/Pages/the-new-economics-of-cyber-crime.aspx. [Accessed 8 August 2017].

42. Siboni Gabi, Siman David. 2014. Cyberspace Extortion: North Korea versus the United States. [ONLINE] Available at: http://www.inss.org.il/publication/cyberspace-extortion-north-korea-versus-the-united-states/. [Accessed 20 September 2017].
43. Symantec Security Response. 2017. Ransom.Wannacry. [ONLINE] Available at: https://www.symantec.com/security_response/writeup.jsp?docid=2017-051310-3522-99&tabid=2. [Accessed 17 September 2017].
44. Symantec, (2017), Top 20 countries affected by Petya attack [ONLINE]. Available at: http://i0.wp.com/euromaidanpress.com/wp-content/uploads/2017/06/Top-20-countries.png?zoom=2&resize=652%2C254 [Accessed 17 September 2017].
45. Symantec. 2013. 2012 NORTON CYBER-CRIME REPORT. [ONLINE] Available at: http://now-static.norton.com/now/en/pu/images/Promotions/2012/cyber-crimeReport/2012_Norton_Cyber-crime_Report_Master_FINAL_050912.pdf. [Accessed 7 August 2017].
46. The Economist. 2013. A giant cage. [ONLINE] Available at: https://www.economist.com/news/special-report/21574628-internet-was-expected-help-democratise-china-instead-it-has-enabled. [Accessed 20 September 2017].
47. The Guardian. 2017. Briton who stopped WannaCry attack arrested over separate malware claims. [ONLINE] Available at: https://www.theguardian.com/technology/2017/aug/03/researcher-who-stopped-wannacry-ransomware-detained-in-us. [Accessed 17 September 2017].
48. The Guardian. 2017. Massive cyber-attack could cost Nurofen and Durex maker £100m | Business | The Guardian. [ONLINE] Available at: https://www.theguardian.com/business/2017/jul/06/cyber-attack-nurofen-durex-reckitt-benckiser-petya-ransomware. [Accessed 17 September 2017].
49. U.S.. 2017. Russia's Rosneft says hit by cyber attack, oil production unaffected | Reuters. [ONLINE] Available at: https://www.reuters.com/article/us-russia-rosneft-cyberattack/russias-rosneft-says-hit-by-cyber-attack-oil-production-unaffected-idUSKBN19I1N9. [Accessed 14 September 2017].
50. Violino Bob. 2017. Unseen, all-out cyber war on the U.S. has begun | InfoWorld. [ONLINE] Available at: http://www.infoworld.com/d/security/unseen-all-out-cyber-war-the-us-has-begun-211438. [Accessed 20 September 2017].
51. Wavefront. 2016. A BRIEF HISTORY OF CYBERCRIME. [ONLINE] Available at: http://www.wavefrontcg.com/A_Brief_History_of_Cybercrime.html. [Accessed 20 September 2017].
52. Worth F. Robert. 2017. 'Terror on the Internet,' by Gabriel Weimann - The New York Times Book Review - The New York Times. [ONLINE] Available at: http://www.nytimes.com/2006/06/25/books/review/25worth.html. [Accessed 20 September 2017].
53. Zacks Equity Research. 2017. Cybersecurity Stocks Shoot Up on Petya Ransomware Attack. [ONLINE] Available at: https://www.zacks.com/stock/news/265995/cybersecurity-stocks-shoot-up-on-petya-ransomware-attack?cid=CS-NASDAQ-FT-265995. [Accessed 19 September 2017].

Books:

1. Andress, J., & Winterfeld, S., 2011. Cyber Warfare: Techniques, Tactics and Tools for Security Practitioners. Waltham, MA: Elsevier. ISBN: 978-0124166721
2. Cohen, F., Phillips, C., Painton Swiler, L., Gaylor, T., Leary, P., Rupley, F., & Isler, R. 1998. A Cause and Effect Model of Attacks on Information Systems: Some Analysis Based on That Model, and The Application of That Model for Cyber Warfare in CID. *Computers & Security,* 17(3): 211-221. http://dx.doi.org/10.1016/S0167-4048(98)80312-X
3. Goodman, Danny, 2004. Spam wars : our last best chance to defeat spammers, scammers, and hackers. 1st ed. New York: SelectBooks, Inc. ISBN-13: 978-1590790632
4. Gragido, W., Molina, D., Pierce, J., & Selby, N. 2012. Blackhatonomics: An Inside Look at the Economics of Cyber-crime. Waltham, MA: Elsevier. ISBN: 978-1597497404
5. Korstanje M (2017) English Speaking Countries and the culture of Fear: understanding technology and terrorism". Threat Mitigation and Detection of Cyber Warfare and Terrorism. Chapter 5 (pp. 93-111) IGI Global, Hershey, Pennsylvania, US, ISBN 978-1522519386
6. NATO, (2008). Cyber defence concept MC0571. Brussels, Belgium.
7. OECD (2009), Computer Viruses and Other Malicious Software: A Threat to the Internet Economy, Paris: OECD Publishing, 2009, doi: 10.1787/9789264056510-en

8. OECD (2012), Internet Economy Outlook 2012, Paris: OECD Publishing, 2012, doi: 10.1787/9789264086463-en
9. Pape Robert, 2005 Dying to Win: The Strategic Logic of Suicide Terrorism, New York: Random House. ISBN 1-4000-6317-5
10. Ramzan, Zulfikar (2010). "Phishing attacks and countermeasures". In Stamp, Mark & Stavroulakis, Peter. Handbook of Information and Communication Security. Springer. ISBN 9783642041174.
11. Shakarian, P., Shakarian, J., & Ruef, A., 2013. Introduction to Cyber-Warfare: A Multidisciplinary Approach. Waltham, MA: Elsevier ISBN: 978-0124078147

Academic journals:

1. Acquisti, A., Friedman, A., Telang, R., 2006. Is there a cost to privacy breaches? An event study. Workshop on the Economics of Information Security, Cambridge, UK.
2. Alkaabi, A.O.S., „Combating Computer Crime: An International Perspective‟, An Information Security Institute Paper, Queensland of Technology University, October 2010
3. Anderson, R.,, Moore, T., 2008. Information Security Economics – and Beyond. In Deontic Logic in Computer Science - Lecture note in computer science 5076, 49.
4. Brockett, P.L., Golden L.L., Wolman W., 2012. Enterprise cyber risk management, in Risk management for the future – Theory and cases, Jan Emblemsvag.
5. Brown, Stephen J., and Jerold B. Warner. "Measuring Security Price Performance", Journal of Financial Economics, 1980, 8(3), 205-258.
6. Bureau of Labor Statistics "Issues in labor Statistics" (PDF). U.S. Department of Labor. 1999.
7. Campbell, K., Gordon, L., Loeb, M., Zhou, L., 2003. The economic cost of publicly announced information security breaches: Empirical evidence from the stock market. Journal of Computer security 11, 431-448.
8. Cavusoglu, H., Mishra, B., Raghunathan, S., 2004. The effect of Internet security breach announcements on market value: capital market reactions for breached firms and Internet security developers. International Journal of Electronic Commerce 9, 69-104.
9. Chen, M.Y., 'I Just Did 400 Million Event Studies' – A Study of Market Model Robustness and Deterioration in Times of Crisis (2014). Available at: http://ssrn.com/abstract=2534446
10. Desouza, K., Hensgen, T., 2003. Semiotic emergent framework to address the reality of cyberterrorism. Technological Forecasting and Social Change 70 (4), 385–396.
11. Douglas W. Thomas and Brian D. Loader as cited by Yar M., Cyber Crime and Society, (London: SAGE Publications, 2005), p. 9.
12. Eisenstein, E.M., 2008. Identity theft: An exploratory study with implications for marketers Journal of Business Research 61, 1160–1172
13. Embar-Seddon, A., 2002. Cyberterrorism. American Behavioral Scientist 45 (6), 1033–1043
14. Fama, E.F., Fisher, L., Jensen, M., Roll, R., 1969. The adjustement of stock prices to new information. International Economic Review 10, 1-21.
15. Gadish, O., 2017. Cyber Terror: How It Happens And What We Can Do. 1st ed. Amazon: OGM.
16. Gandhi, R., Sharma, A., Mahoney, W., Sousan, W., Zhu, Q., & Laplante, P. 2011. Dimensions of Cyber-Attacks: Cultural, Social, Economic, and Political. *IEEE Technology and Society Magazine*, 30(1): 28-38.
http://dx.doi.org/10.1109/MTS.2011.940293
17. Geers, K., 2010. The Challenge of Cyber Attack Deterrence. Computer Law & Security Review 26 (3), 298- 303.
18. Gengler, B., 1999. Politicians speak out on cyberterrorism. Network Security 1999 (10), 6
19. Gordon, L.A., Loeb, M.P., Lucyshyn W., 2003. Information security expenditures and real options: a wait- and-see approach. Computer Security Journal 19 (2), 1-7.

20. Gordon, S., Ford, R., 2002. Cyberterrorism? Computer & Security 21 (7), 636–647
21. Grau, D., & Kennedy, C. 2014. TIM Lecture Series – The Business Of Cybersecurity. *Technology Innovation Management Review,* 4(4): 53–57.
http://timreview.ca/article/785
22. Hovav, A., D'Arcy, J., 2004. The impact of virus attack on the market value of firms. Information System Security 13 (3), 32-40.
23. Howard, J. D. 1997. An Analysis of Security Incidents on the Internet 1989–1995. Doctoral Thesis, Carnegie-Mellon University, Pittsburgh, PA.
24. Iheagwara, C., Blyth, A., Singhal, M., 2004. Cost effective management frameworks for intrusion detection systems. Journal of Computer Security 12, 777-798.
25. Ishiguro, M., Tanaka, H., Matsuura, I., Murase, I., 2007. The effect of information security incidents on corporate values in the Japanese stock market. In Workshop on the Economics of Securing Information Infrastructure, Arlington.
26. Janczewski Lech J. and Andrew M. Colarik, ed., Cyber Warfare and Cyber Terrorism, Hershey (PA): Information Science Reference, 2008.
27. Kannan, A., Rees, J., Sridhar, S., 2007. Market reaction to information security breach announcements: an empirical analysis. International Journal of Electronic Commerce 12, 69-91.
28. Kundur, D., Feng, X., Mashayekh, S., Liu, S., Zourntos, T., Butler-Purry, K.L., 2011. Towards modelling the impact of cyber attacks on a smart grid. International Journal of Security and Networks 6 (1), 2-13.
29. MacKinlay, A. C. "Event Studies in Economics and Finance," Journal of Economic Literature Vol. XXXV, Issue 1 (March 1997). Available at:http://www.jstor.org/stable/2729691.
30. Odulaja, G.O, Wada, F., 2012. Assessing Cyber crime and its Impact on E-Banking In Nigeria Using Social Theories. African Journal of computing & ICTs 4 (2), 69-82
31. Parton T., „Cyber Crime: Protecting Against the Growing Economic Crime", PWC Crime Survey, Nov.2011, p. 5.
32. Power, R., 2002. CSI/FBI 2002 Computer Crime and Security Survey. Computer Security Issues and Trends 18 (2), 7-30.
33. Prichard, J.J. & MacDonald, L.E. (2004). Cyber Terrorism: A Study of the Extent of Coverage in Computer Security Textbooks. *Journal of Information Technology Education, 3*, 279-289. Retrieved September 20, 2017 from https://www.learntechlib.org/p/104592/.
34. Shackelford S.J., 2008. From Nuclear War to Net War: Analogizing Cyber Attacks in International Law. International Law 27 (1), 191-251
35. Stanton, J.J., 2002. Terror in cyberspace. American Behavioral Scientist 45 (6), 1017–1032.
36. Wehde, E., 1998. US vulnerable to cyberterrorism. Computer Fraud & Security 1998 (1), 6–7.
37. Winn, J., Govern, K., 2009. Identity theft: risks and challenges to business of data compromise. Journal of Science Technology & Environmental Law 28 (1), 49-63.

Appendix

List of companies included in the sample:

List of companies affected by WannaCry ransomware attack

1.	Portugal Telecom
1.	Renault
2.	Telefonica

List of companies affected by Petya ransomware attack

1.	AP Moller Maersk
2.	Beiersdorf AG
3.	Deutsche post
4.	Merck Co
5.	Reskitt Benckiser
6.	Rosneft
7.	Saint Gobain
8.	WPP

List of analysed antivirus companies

1.	Cisco
2.	FireEye
3.	Palo Alto Networks
4.	Sophos
5.	Symantec
6.	Science Application International Corporation

Significance testing for abnormal returns after WannaCry attack are shown below:

Table: Parametric T-test for Abnormal returns of company Portugal Telecom

Event time t	Abnormal returns	T-test	Significance as AR/St.err > 1.96
0	0.009286303	0.161994581	no
1	-0.011536812	-0.201253504	no
2	0.011702021	0.204135491	no
3	0.012357789	0.215575015	no
4	0.058941402	1.028201201	no
5	-0.040761441	-0.711061521	no

Table: Parametric T-test for Abnormal returns of company Renault SA

Event time t	Abnormal returns	T-test	Significance as AR/St.err > 1.96
0	-0.00009932	-0.008726026	no
1	-0.005941316	-0.008726026	no
2	0.006570021	0.57722116	no
3	-0.005952787	-0.522992917	no
4	-0.002582904	-0.226925702	no
5	0.006685292	0.587348477	no

Table: Parametric T-test for Abnormal returns of company Telefonica

Event time t	Abnormal returns	T-test	Significance as AR/St.err > 1.96
0	-0.003149432	-0.542166828	no
1	0.001979183	0.340711378	no
2	0.003973393	0.684009629	no
3	0.00165334	0.284618407	no
4	0.012772073	2.198680518	yes
5	-0.007657277	-1.318181174	no

Significance testing for abnormal returns after Petya attack are shown below:

Table: Parametric T-test for Abnormal returns of company AP Moller Maersk

Event time t	Abnormal returns	T-test	Significance as AR/St.err > 1.96
0	0.010438339	0.739108308	no
1	0.027693207	1.9608752	yes
2	0.006101664	0.432041039	no
3	0.014682199	1.039603661	no
4	0.01384812	0.980544953	no
5	-0.001335777	-0.094582502	no

Table: Parametric T-test for Abnormal returns of company Beiersdorf AG

Event time t	Abnormal returns	T-test	Significance as AR/St.err > 1.96
0	-0.0099527	-1.580276593	no
1	-0.001971398	-0.313015998	no
2	-0.008836269	-1.40301116	no
3	0.012408963	1.970278924	yes
4	-0.011641429	-1.84841079	no
5	-0.006323674	-1.004064724	no

Table: Parametric T-test for Abnormal returns of company Deutsche Post

Event time t	Abnormal returns	T-test	Significance as AR/St.err > 1.96
0	-0.004665667	-0.558775968	no
1	0.002235296	0.267706508	no
2	0.002663665	0.319009496	no
3	0.00308226	0.369141845	no
4	0.009366199	1.121727437	no
5	-0.004720549	-0.565348792	no

Table: Parametric T-test for Abnormal returns of company Merck & Co

Event time t	Abnormal returns	T-test	Significance as AR/St.err > 1.96
0	0.003091886	0.380080397	no
1	-0.004401232	-0.541036153	no
2	-0.002782283	-0.342021396	no
3	-0.003139228	-0.385900089	no
4	0.000701666	0.086254695	no
5	0.013317477	1.637095377	no

Table: Parametric T-test for Abnormal returns of company Reckitt Beckinser

Event time t	Abnormal returns	T-test	Significance as AR/St.err > 1.96
0	-0.005460418	-0.53545545	no
1	-0.01170437	-1.14774522	no
2	-0.00733574	-0.719351909	no
3	0.002689948	0.263779689	no
4	-0.0033653	-0.33000554	no
5	-0.00086645	-0.084965216	no

Table: Parametric T-test for Abnormal returns of company Rosneft

Event time t	Abnormal returns	T-test	Significance as AR/St.err > 1.96
0	0.008055879	0.804554626	no
1	0.010138474	1.012547001	no
2	0.026942149	2.690759207	yes
3	0.021876424	2.184836497	yes
4	0.037871017	3.782244205	yes
5	0.032792211	3.275015087	yes

Table: Parametric T-test for Abnormal returns of company Saint Gobain

Event time t	Abnormal returns	T-test	Significance as AR/St.err > 1.96
0	0.00006318	0.01026002	no
1	0.00106083	0.172267103	no
2	0.008611983	1.398491565	no
3	0.013774224	2.236783067	yes
4	-0.004264671	-0.692535861	no
5	0.001854229	0.301106459	no

Table: Parametric T-test for Abnormal returns of company WPP

Event time t	Abnormal returns	T-test	Significance as AR/St.err > 1.96
0	0.025431621	2.169859059	yes
1	0.012953271	1.105189974	no
2	0.009987417	0.852139469	no
3	0.01476821	1.26004291	no
4	0.023430289	1.999102813	yes
5	0.010045643	0.85710737	no

Significance testing for antivirus companies` abnormal returns after Petya attack are shown below:

Table: Parametric T-test for Abnormal returns of company Cisco

Event time t	Abnormal returns	T-test	Significance as AR/St.err > 1.96
0	-0.000282169	-0.04169867	no
1	-0.010758565	-1.589889566	no
2	0.006818287	1.007599405	no
3	-0.008428954	-1.24562208	no
4	-0.013751168	-2.032133333	yes
5	0.007981186	1.179451429	no

Table: Parametric T-test for Abnormal returns of company Fireeye

Event time t	Abnormal returns	T-test	Significance as AR/St.err > 1.96
0	-0.010969401	-0.681340376	no
1	-0.018437638	-1.145213539	no
2	0.011246688	0.698563431	no
3	-0.026109348	-1.621725084	no
4	-0.011864406	-0.736931663	no
5	-0.014031815	-0.871555485	no

Table: Parametric T-test for Abnormal returns of company Science Application International Corp.

Event time t	Abnormal returns	T-test	Significance as AR/St.err > 1.96
0	-0.008090586	-0.502071112	no
1	-0.012106929	-0.751310112	no
2	0.01585601	0.983963902	no
3	-0.019623318	-1.217748743	no
4	0.004425247	0.274614083	no
5	0.007434621	0.461364421	no

Table: Parametric T-test for Abnormal returns of company Sophos

Event time t	Abnormal returns	T-test	Significance as AR/St.err > 1.96
0	0.001608114	0.079904606	no
1	0.003012463	0.14968441	no
2	-0.053600961	-2.663345158	yes
3	0.001722199	0.085573304	no
4	-0.00688808	-0.34225755	no
5	0.011224653	0.557734881	no

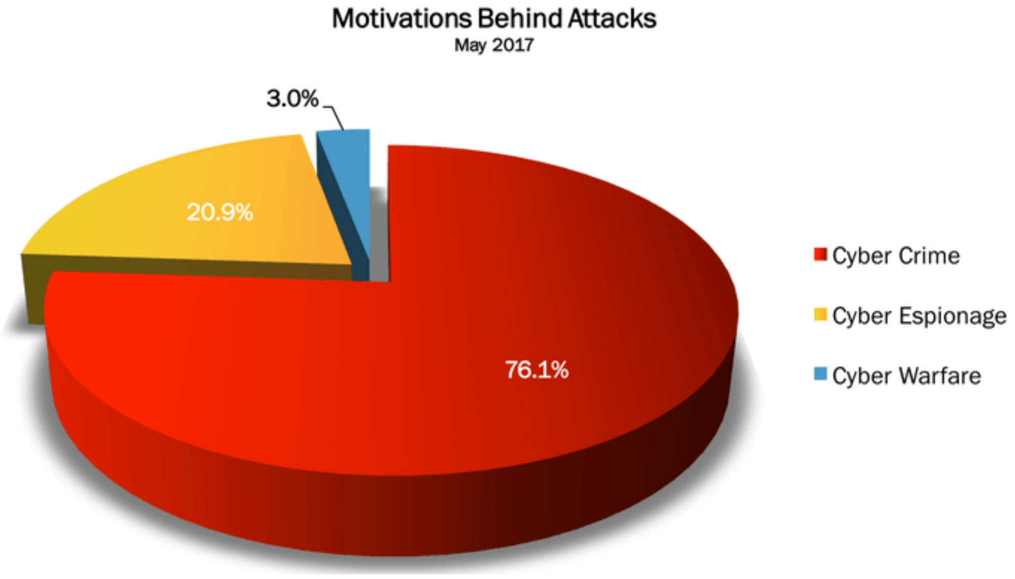
Table: Parametric T-test for Abnormal returns of company Symantec

Event time t	Abnormal returns	T-test	Significance as AR/St.err > 1.96
0	0.013090757	1.221594671	no
1	-0.019241514	-1.795567054	no
2	0.022111843	2.063418486	yes
3	-0.023788467	-2.219876598	yes
4	0.001902558	0.177541618	no
5	-0.032623457	-3.044334442	yes

Content list

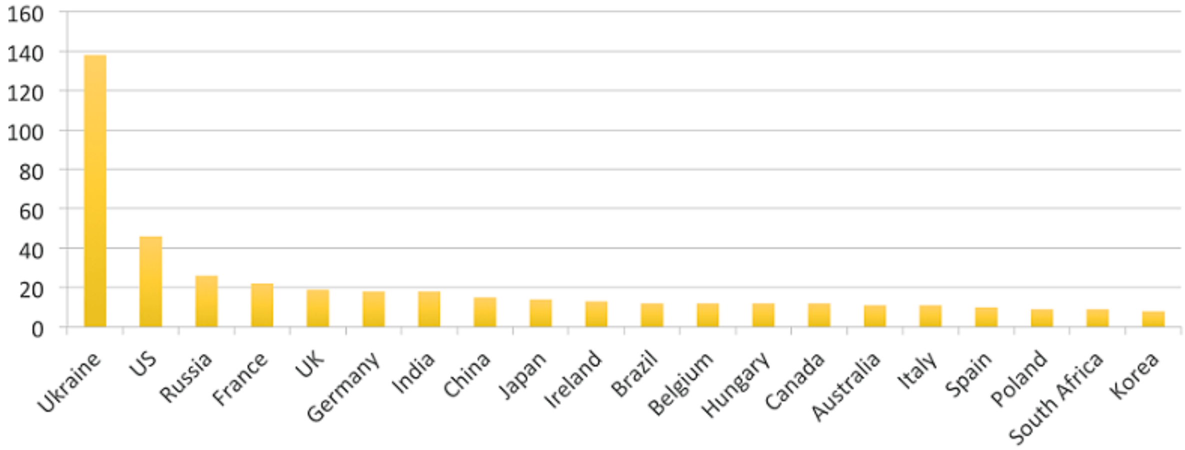
Pictures:

Picture 1: Motivations behind cyber-attacks



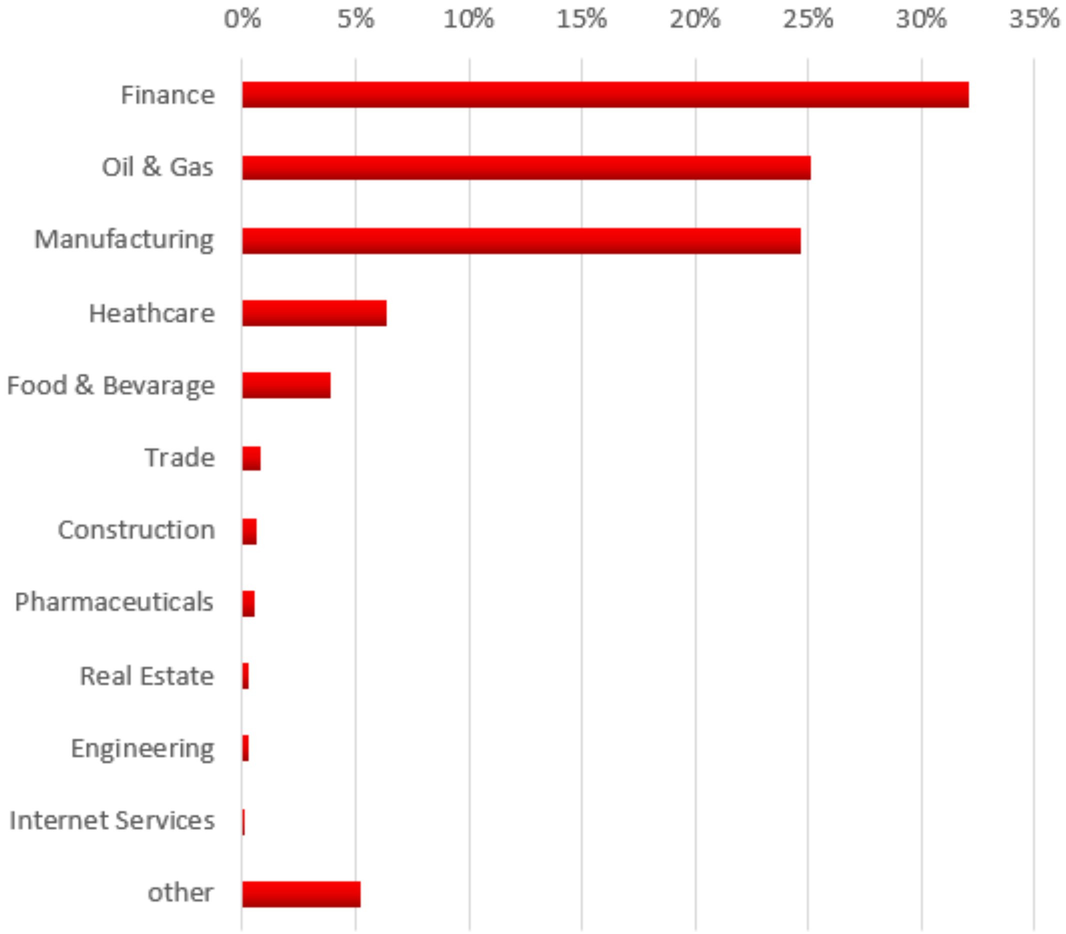
Source: Paolo Passeri, (2017), May 2017 Cyber Attacks Statistics

Picture 2: Top 20 countries affected by Petya attack



Source: Symantec, (2017), Top 20 countries affected by Petya attack

Picture 3: The most affected industries



Source: Kaspersky Security Networks, (2017), Petya targets by industry

Tables:

Table: Test statistics for CAARs for the sample during Wannacry attack:

Event window	No of firms	Mean CAR	T-test	P-value	T-critical
(-20;20)	3	-0.005286779	-0.186057714	0.565219325	2.91998558
(-10;10)	3	0.017351469	2.622463566	0.05991289*	1.885618083
(-5;5)	3	0.042276027	0.996448228	0.212009619	2.91998558
(-3;3)	3	-0.005897352	-0.396965906	0.6351262	2.91998558
(-1;1)	3	-0.005413494	-0.445182742	0.650132923	2.91998558

*Statistically significant at 10% (one-tailed test)
**Statistically significant at 5% (one-tailed test)
***Statistically significant at 1% (one-tailed test)

Table: Test statistics for CAARs for the sample during Petya attack:

Event window	No of firms	Mean CAR	T-test	P-value	T-critical
(-20;20)	8	0.201577856	2.459042634	0.02176318**	1.894578605
(-10;10)	8	0.124208463	2.839810491	0.012525706**	1.894578605
(-5;5)	8	0.065094935	2.50134103	0.020455932**	1.894578605
(-3;3)	8	0.043474614	2.994467186	0.010049426**	1.894578605
(-1;1)	8	0.017436205	1.874678375	0.051483898*	1.414923928

*Statistically significant at 10% (one-tailed test)

**Statistically significant at 5% (one-tailed test)

***Statistically significant at 1% (one-tailed test)

Table: Test statistics for CAARs for the sample of antivirus companies during Petya attack:

Event window	No of firms	Mean CAR	T-test	P-value	T-critical
(-20;20)	6	0.09322324	1.894773386	0.058321556*	1.475884049
(-10;10)	6	0.011234323	0.318483173	0.381495942	1.475884049
(-5;5)	6	-0.012900289	-1.410426493	0.891256276	1.475884049
(-3;3)	6	-0.008141476	-0.974711192	0.81276539	1.475884049
(-1;1)	6	-0.015548948	-3.507612907	0.991427835	1.475884049

*Statistically significant at 10% (one-tailed test)

**Statistically significant at 5% (one-tailed test)

***Statistically significant at 1% (one-tailed test)

Charts:

Stock prices after the attack for period 06/27/2017 - 07/27/2017

Chart 1: CISCO stock prices after the attack:

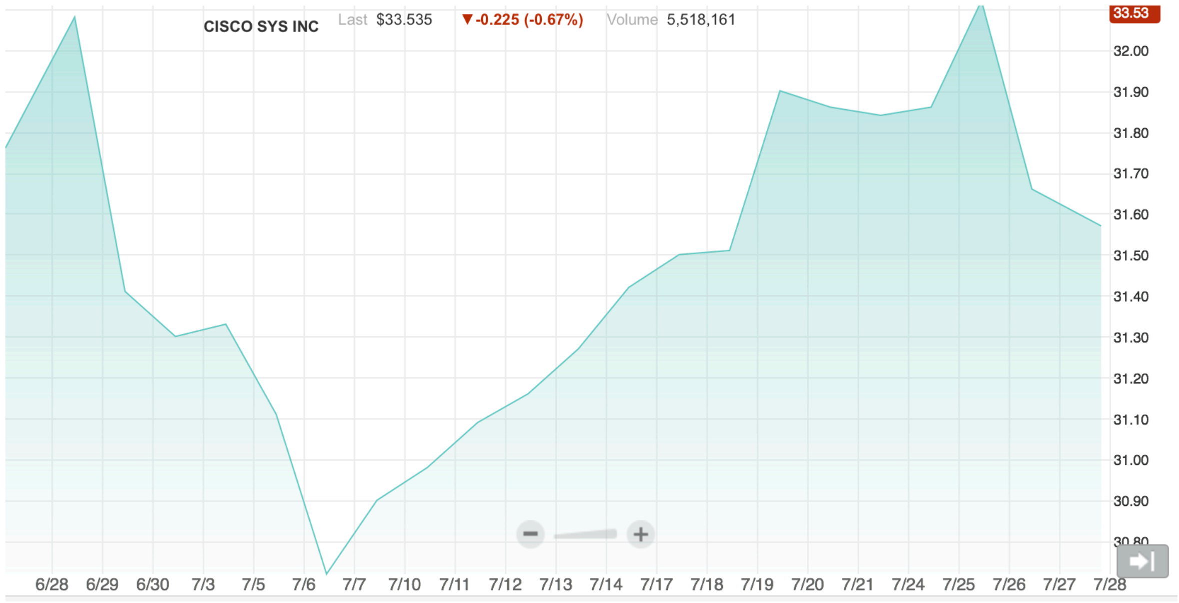


Chart 2: Palo Alto Networks stock prices after the attack:

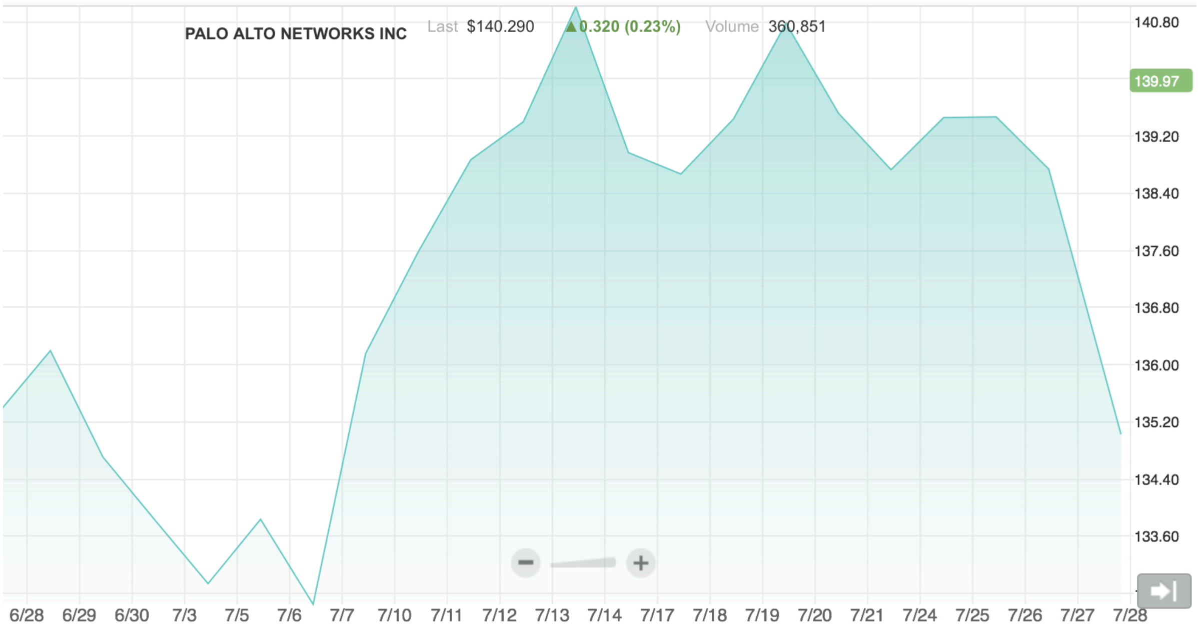


Chart 3: Science Application International Corporation stock prices after the attack:

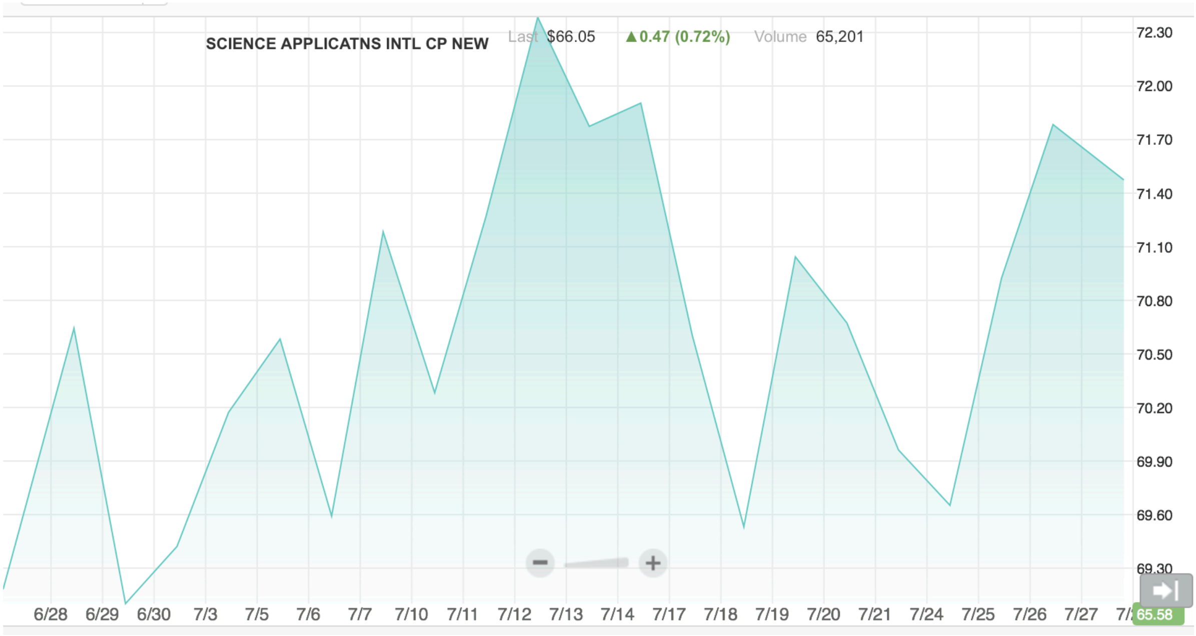


Chart 4: Sophos Group stock prices after the attack:

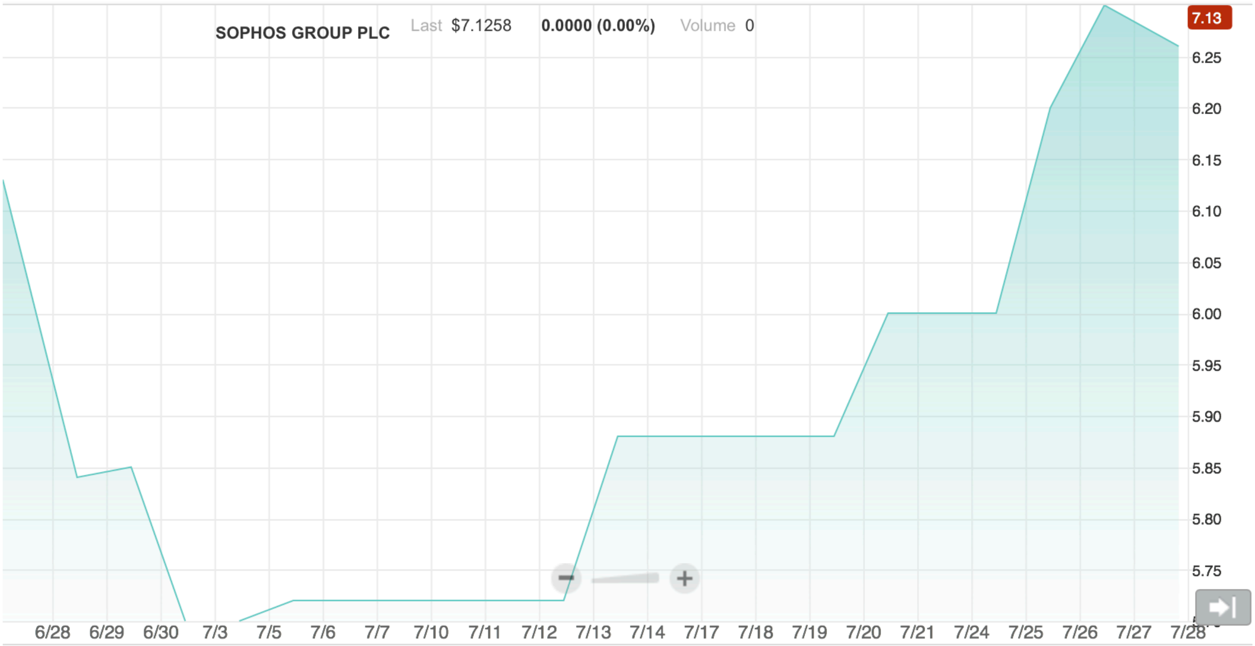


Chart 5: FireEye Inc. stock prices after the attack:

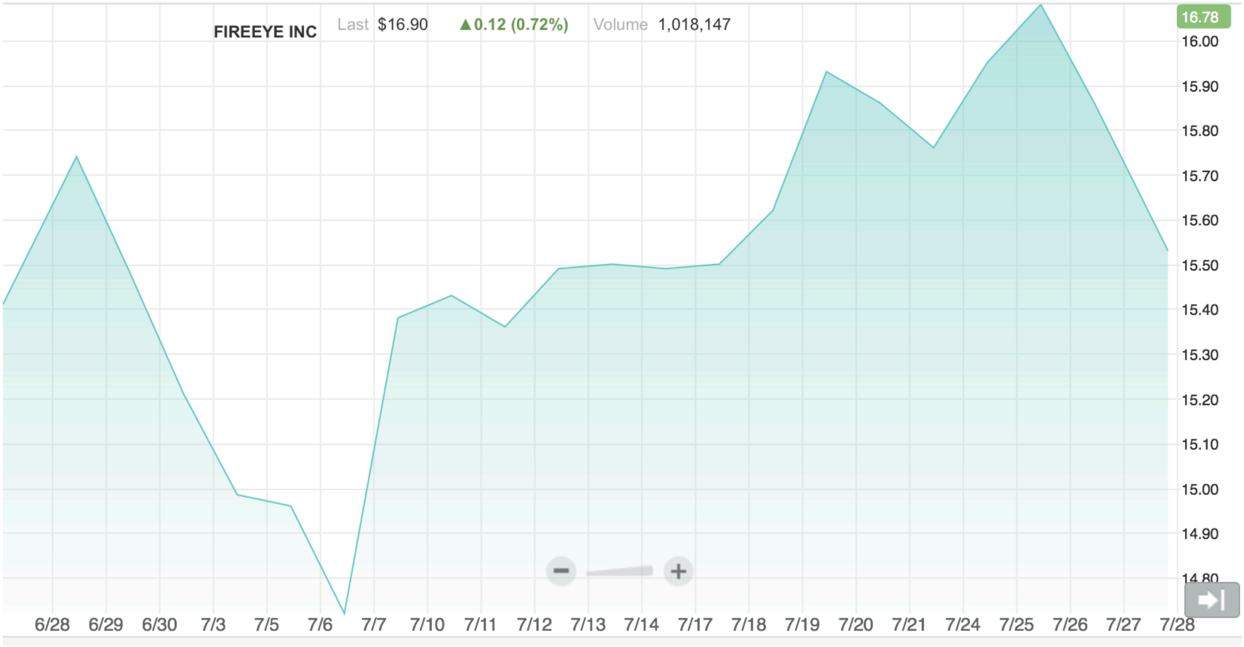
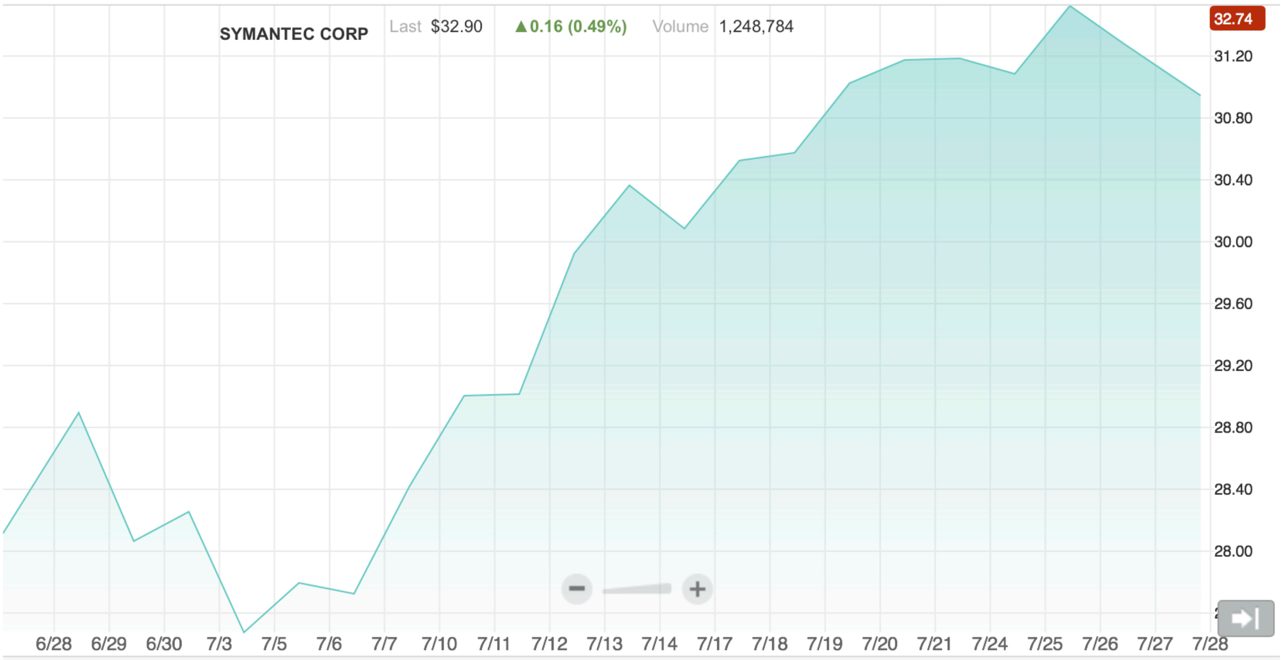


Chart 6: Symantec stock prices after the attack:



Source: NASDAQ interactive charts