2018

Economics-Based Risk Management of Distributed Denial of Service Attacks: A Distance Learning Case Study

Omer Keskin
Old Dominion University

Unal Tatar
Old Dominion University

Omer Poyraz
Old Dominion University

Ariel Pinto
Old Dominion University

Adrian Gheorghe
Old Dominion University

Original Publication Citation

Keskin, O., Tatar, U., Poyraz, O., Pinto, A., & Gheorghe, A. (2018) Economics-based risk management of distributed denial of service attacks: A distance learning case study. In J. S. Hurley & J. Q. Chen (Eds.), *Proceedings of the 13th International Conference on Cyber Warfare and Security: ICCWS 2018* (pp. 343-352). Academic Conferences Ltd.

Economics-Based Risk Management of Distributed Denial of Service Attacks: A Distance Learning Case Study

Omer Keskin, Unal Tatar, Omer Poyraz, Ariel Pinto and Adrian Gheorghe
Dept. of Engineering Management & Systems Engineering, Old Dominion University, Norfolk, USA
okeskin@odu.edu
utatar@odu.edu
opoyraz@odu.edu
cpinto@odu.edu
agheorgh@odu.edu

Abstract: Managing risk of cyber systems is still on the top of the agendas of Chief Information Security Officers (CISO). Investment in cybersecurity is continuously rising. Efficiency and effectiveness of cybersecurity investments are under scrutiny by boards of the companies. The primary method of decision making on cybersecurity adopts a risk-informed approach. Qualitative methods bring a notion of risk. However, particularly for strategic level decisions, more quantitative methods that can calculate the risk and impact in monetary values are required. In this study, a model is built to calculate the economic value of business interruption during a Distributed Denial-of-Service (DDoS) attack to help decision-makers for selecting the most effective mitigation strategy (i.e., acceptance, avoidance, transferal or control). The model is applied to a simulated DDoS attack targeting a distance learning system of a higher education institution. The simulation results show when it is appropriate to accept the risk, buy cyber insurance as a method of risk transfer, or buy DDoS prevention system as a method of risk control.

Keywords: economics of cybersecurity, cyber insurance, DDoS, risk quantification, business interruption

1. Introduction

Cyber risk has become a top agenda item for businesses all over the world and is listed as one of the top three global risks with significant economic implications for businesses (Allianz, 2016). Cybersecurity risk score of companies is a recently emerging indicator of investment assessments (Bloomberg, 2014). CISOs are playing more critical roles in companies' managerial boards as they are not only responsible for securing organizations from cyber threats but also providing strategic guidance to other board members, especially on effectiveness and efficiency of cybersecurity investments. Managerial board of a company relies on CISO for information about the company's cybersecurity posture in a language that they can understand – risk, cost, and benefits – and how cyber risk maps to dollars instead of the latest purchase of an IT security product (Rifai, 2017). To transform cyber risk management from a technical issue to a business issue, cyber risk has to be quantified as monetary value. Valuation of cyber risk will eventually be integrated into Enterprise Risk Management frameworks (Ruan, 2017). Consequently, cyber risk management has become an emerging and vital part of the enterprise risk management.

Cyber defence aims to adjust organizations to comply with standards and best practices and is an extensively expensive task, which requires investment in people, processes, and technology (Tatar et, al., 2014). Investments in the cyber domain are subject to constraints that may be similar with those in more traditional domains – such as cost and effectiveness. However, cyber is a dynamic domain where effectiveness and functionalities of investments are more unpredictable. For example, not all vulnerabilities will be exploited, but the potential of exploitation remains – until updates or patches have been successfully performed. These situations create questions for organizations on whether, how much, when and how to invest in cybersecurity.

Traditionally, higher education is held in classrooms with professors lecturing their courses. In recent decades, this convention has been changing in some degree with the asynchronous (e.g., CD-ROM) and synchronous distance learning education methods. Before the wide use of the internet, institutes employed televised delivery methods through satellites for synchronous distance learning. Later, this approach was almost completely abandoned, and the internet has become the platform for distance learning courses. Institutes of higher education have started offering their courses and programs online to reach more students and increase their income from tuition. Many higher education institutes offer distance learning degrees or at least some distance learning courses. According to the U.S. Department of Education, National Center for Education Statistics (2016), "In fall 2014, there were 5,750,417 students enrolled in any distance education courses at degree-granting postsecondary institutions."

Distance learning programs help to deliver higher education to anyone who has an internet connection anywhere in the world. However, distance learning highly depends on the internet. Quality of the classes is easily affected by low bandwidth and unreliable internet service. The bandwidth issue is attributed more to the student end. However, the reliability of internet service is much more important at the university end. Given that the universities that provide distance learning have the internet infrastructure to provide a sufficiently good quality stream, no problems are expected. Nevertheless, parallel to developments in the internet and technology, cyber attacks have also evolved over time. Universities are among the top targets of the Distributed Denial-of-Service (DDOS) attacks (Cloudbric, 2017; McMurdie, 2017), which result in business interruption. As well, according to the researchers at Akamai Technologies, U.S. colleges and universities are facing an increase in DDoS attacks (Walker, 2017).

In this study, an economics-based framework to manage the risks of DDoS attacks is developed. The framework is applied to a distance learning system of a higher education institute.

2. Research problem

Distance learning programs have become popular. However, distance learning requires continuous, high-quality internet connection. This step into the cyberspace also generates the risk of cyber attacks. DDoS attacks can disrupt course delivery and cause financial consequences. Decision-makers in the university management need a method to choose the best risk mitigation strategy to withstand the impact of DDoS attacks. Accordingly, the research question is: *"How to select the most efficient risk management approach against DDoS attacks targeting a distance learning infrastructure?"*

Quantifying cybersecurity risk in monetary values would help make better decisions while choosing a risk mitigation strategy. There are several methods of cybersecurity risk mitigation: risk control (i.e., reducing the consequence or likelihood), risk acceptance, risk avoidance, and risk transferal (Pinto & Garvey, 2012). This approach will also increase temporal accuracy in acquisition roadmaps, precision on requirements management, and effective financial planning.

In this study, the framework is provided to help decision-makers choose the most efficient risk mitigation approach against DDoS attacks that target distance learning systems through calculating the economic value of the availability of the services.

3. Literature review

Economics of information security and cybersecurity investment have been studied for a long time. However, in recent years, the number of publications have been increasing due to escalating expenditures and loss from security breach apart from the technical problems. Scholars suggest different methods to help decision-makers decide how to invest in cybersecurity to protect operational excellence and intellectual property. Specific prominent studies to increase the efficiency in cybersecurity risk management are reviewed below.

One relevant study was presented by CAPT Erickson (2016) on cybersecurity figure of merit. Erickson states that "The Navy is unable to measure and express cyber program of record wholeness, platform cyber readiness, and the impact of programmatic and budgetary decisions on cyber readiness, or to quantify the value of specific cybersecurity standards or controls. Without an accepted means of holistically scoring risk within a system of systems construct, the Navy cannot consistently shape cybersecurity investment priorities to optimize value in a resource constrained environment." The main research problem of Erickson is "how to optimize complex cybersecurity investment combinations to provide the maximum value in terms of operational risk reduction in resource-constrained environments." Morse and Drake (2012) developed a methodology to cope with acquisition risk. In order to have more realistic and objective risk assessment, they proposed a methodology to quantify acquisition risks through data-driven monetization. Cybersecurity is not within the scope of their study, but the core is calculating risk in monetary values as in this research.

Shultz and Wydler (2015) studied the integration of cybersecurity into acquisition life-cycle, a shift from bolt-on security to built-in security. Shultz and Wydler described how the government is moving from compliance-based requirements to a risk-based cybersecurity management framework to integrate cybersecurity into program acquisition and execution support. Kaestner, Arndt, and Dillon-Merrill (2016) focused on embedding cybersecurity during acquisition process to reduce the product life-cycle costs because of the reduced need to fix vulnerabilities in the systems later. To attain this goal, the acquisition community must be aware of cyber threats and have an understanding of risk assessment. In the recommendations section of their article, Kaestner et al. (2016) state that "Risk management experts agree that the first step to take is to assess the financial risk of a security breach. This requires a detailed inventory of the organization's assets at risk that will be used to assess the financial risk." The recommendation of Kaestner et al. (2016) is the goal of this study.

There have been studies to compare different methods to determine optimal amount to invest in cybersecurity. There are comparison works on the economics of cybersecurity, such as game theory, optimization theory, use of real data, and security controls selection. Cavusoglu et al. (2008) and Fielder et al. (2016) utilized game theory and optimization to compare the two for benchmarking efficiency of cybersecurity investments.

Economics of cybersecurity studies employs optimization methods to address several types of problems. For example, an earlier work (Gordon and Loeb 2002) utilized optimization to calculate the optimal amount to invest in cybersecurity, and it showed that a small fractional amount of the expected loss would be enough to invest in cybersecurity.

Arora et al. (2004) suggest taking a risk management approach to evaluate information security solutions. They indicate that security managers should consider risk-based Return on Investment method to decide how to invest in cybersecurity due to so many uncertainties in the cyber domain.

Research on the topics of the economics of cyber risk and cyber insurance –the primary method of risk transference– has grown exponentially after 2010. This highlights the increasing relevance of the topic, from both a practical and an academic perspective (Eling & Schnell, 2016).

Current methods commonly put more emphasis on technology and less on people, process and socio-economic risk factors (Spears, 2005; Tatar, Bahsi and Gheorghe, 2016). Major risk assessment approaches, such as ISO/IEC 27001 and 27002 standards, are designed based on security control domains and focus more on an asset's security posture while ignoring its preparedness towards a set of high-risk loss scenarios (Ruan, 2017). One of the major problems of actuaries working in insurance sector or enterprise risk management is the quantification of cyber risk. Almost all the security companies keep incident and loss data as proprietary to have a competitive advantage (Ruan, 2017). Subsequently, there is not enough data to employ statistical methods and mathematical models for appropriate calculations and predictions. This scarcity of data leads analysts to rely on scenario approaches rather than the use of the classical stochastic modelling (Lloyd's, 2015). For Rakes, Deane, and Rees (2012) employing expert judgment to define worst-case scenarios and estimate their likelihood for high-impact IT security breaches is a more efficient approach. Even more so, fast-changing technology environment requires a modelling approach which dynamically measures risk (Eling & Schnell, 2016).

4. Method

Risk management is conducted continuously against the risk events of an organization underexposure. Decision-makers in higher education institutes need to consider different risk mitigation strategies and select the most efficient one for each risk event. In this section, information on different risk mitigation strategies is given and the model to support decision making on risk mitigation strategies is explained.

4.1 Risk mitigation strategies

There are four general risk mitigation strategies (Pinto & Garvey, 2012):

- Risk Acceptance: Possible consequences of a risk event is accepted. No action is taken. After the risk event occurs, the organization accepts the consequences. This strategy is commonly used for low impact risk events.
- Risk Avoidance: Risk avoidance is to stop or cancel/abandon the event or process that causes the risk. For example, stopping production of the risky product, not doing business in risky regions, and deleting the highly vulnerable and unnecessary applications from corporate computers are risk avoidance attempts

(Dorfman & Cather, 2013). This method is relatively more appropriate for medium and high-risk score events.

- Risk Control: Risk Control includes taking precautions to decrease either or both the likelihood and consequences of a risk event. Cybersecurity products and services such as firewalls and antivirus programs are considered risk control activities.
- Risk Transfer: Organizations can choose to transfer the risk of compensating the loss caused by a risk event. Cyber insurance falls under this category. If a cyber attack occurs, the consequences will be transferred to the third-party insurance companies.

4.2 Model

In this study, a model to support decision making on choosing risk mitigation strategies is developed. Decision-makers need to define ways of action by predicting the possible cost of risk events. The model depends on the predicted Cost of Impact of a DDoS attack. Based on the magnitude of the cost, the model helps to choose different strategies based on The Mitigation Strategy Selection Algorithm is shown in Figure 1.

Condition 1: When the Cost of Impact ($Imp) is less than or equal to the sum of Insurance Deductible ($Ded) and Premium ($Prm), then decision-makers should consider accepting the risk since the impact is negligible.

Condition 2: While the Condition 1 is False, if the sum of Insurance Deductible ($Ded), Premium ($Prm) and the difference between Cost of Impact ($Imp) and Insurance Coverage ($Cov) is less than the Cost of Control ($Ctl), then the decision-makers should consider transferring the risk. Since the Cost of Impact ($Imp) is too much to accept but not high enough to exceed the Cost of Control, transferring the risk is the best option in this situation.

Condition 3: If both Condition 1 and 2 are False, the decision-makers should consider choosing the risk control strategy because the Cost of Impact is too much to be accepted and also too much from the insurance coverage amount. Thus, the best option for this magnitude effects is to control risk.

For this model, risk avoidance is not an appropriate risk mitigation strategy since it is assumed that the higher education institute is determined to continue offering distance learning programs.

```
IF $\$Imp \leq \$Ded + \$Prm$
    Strategy = Accept
ELSE
    IF $\$Ded + \$Prm + \$Imp - \$Cov \leq \$Ctl$
        Strategy = Transfer
    ELSE
        Strategy = Control
    ENDIF
ENDIF
```

Figure 1: The mitigation strategy selection algorithm

Predicting the Cost of impact is an integral part of this model. It depends on the direct impact and indirect impact as shown in Equation 1.

$$\$Imp{:}\ Cost\ of\ Impact = f(Direct\ Impact, Indirect\ Impact) \qquad (1)$$

The *Indirect Impact* includes the cost of reputation damage, legal procedures, productivity decline, customer turnover, personnel time spent addressing and recovering from the outage, incremental helpdesk expenses, and loss of ability to meet the requirements of regulators (Arbor Networks, 2016; Granidello et. al, 2016; Tatar and Karabacak, 2014). Estimating the *Indirect Impact* is harder. Some methods could be developed to estimate the factors that constitute the *Indirect Impact*. For instance, in the scope of the distance learning system, the cost of reputation basically depends on the enrollment along years and is affected by the reputation of the distance learning programs of the higher education institute. Because of the scarcity of data to quantify the *Indirect Impact*, it is out of the scope of this study.

In this study, a model is proposed to gauge the *Direct Impact*. The higher education institutes do not lose money directly when a DDoS attack occurs when compared to an online store or gambling site. However, they need a way of calculating the value of the online service availability. As shown in the Equation 2, *Direct Impact* can be calculated as a function of the duration of the DDoS attack and the number of students who are connected to the distance learning program during the attack.

$$Direct\ Impact = f(DDoS\ Duration, Number\ of\ Students) \tag{2}$$

DDoS duration can be a couple of minutes or may go up to days. The number of connected students depends on the number and type of the courses held during this period (See the Equation 3). Graduate and undergraduate courses typically have a different number of enrolled students and different tuition rates.

$$Number\ of\ Students = f(Number\ of\ Courses, Type\ of\ Courses) \tag{3}$$

Number and type of the courses depend on the course schedule. Hence, the day of the week and the time of the day as shown in the Equation 4.

$$Number\ of\ Courses = f(Day\ of\ the\ Week, Time\ of\ the\ Day) \tag{4}$$

5. Application of the model on distance learning data

The model is applied to the real-world data from Old Dominion University distance learning system.

5.1 Data collection and preparation

Schedule data of distance learning courses in Spring 2017 term is used. According to the Equation 4, Number of Courses depends on the Day of the Week and the Time of the Day. Figure 1 illustrates equation 4 by representing the number of courses offered on each day. There are no courses on weekends and in the late hours. Therefore these hours are not included in the plot.

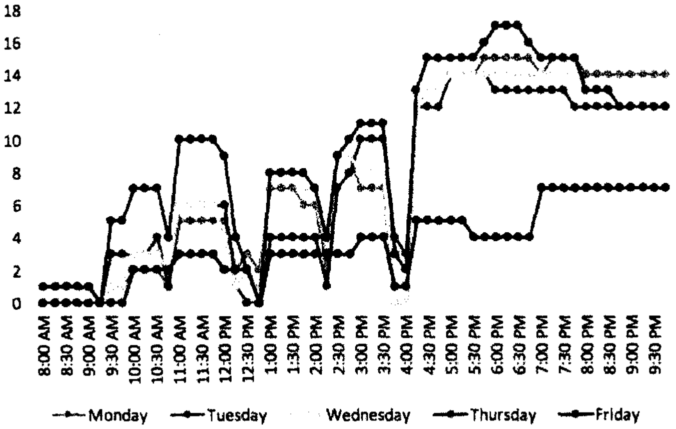

Figure 2: Total number of distance learning courses for each day

In addition to the course schedule, data for enrollment, tuition rates, and domicile is included in the study. Based on the Equation 3, the type of the courses is also needed. The tuition rates are different for undergraduate and graduate students and also differs based on domicile. Commonly, out-of-state students pay more tuition than in-state students (See Table 1).

Table 1: Data for domicile, tuition rates, and types of courses

Domicile	Level	Tuition Rates	Domicile
In-state Students	Undergraduate	$325	91.48%
Out-of-State Students	Undergraduate	$355	8.52%
In-state Students	Graduate	$478	74.39%
Out-of-State Students	Graduate	$516	25.61%

Based on the enrollment data, total student credit hours registered to distance learning courses for this semester are 52,200 for undergraduate level, and 11,388 for graduate level. A course requires three credit hours. There are 81 undergraduate, 76 graduate courses, and 27 courses for both undergraduate and graduate level. Based on these numbers, the average value of a 15-minute period for one course is $1,250.71 for undergraduate level and $428.98 for graduate level. Based on the data given above, the value of stream for 15-minute periods for each day is visualized in Figure 3. This figure shows the direct impact values (mentioned in the Equation 2) for these time periods without considering the duration of the DDoS attacks.

Figure 2 and Figure 3 have some similarities and differences.

Similarities:

- Trends for each day are similar at each graph. If there is no course within a period, the dollar value is also zero (e.g., Wednesday, 3.45 pm; Friday, 8.30 am).
- When the plot in either figures peaks, the related plot in the other figure also reaches a peak (e.g., Thursday, 6 pm).

Differences:

- The vertical axis represents the number of courses in Figure 2 while it stands for the dollar value of each 15-minute-period in Figure 3.
- The plots in Figure 3 has higher values before 4 pm. This is because most of the undergraduate courses are held until 4 pm, and these courses have much more enrolled students in average than the graduate courses. This increases their value even if the tuition rates for the undergraduate level are lower.

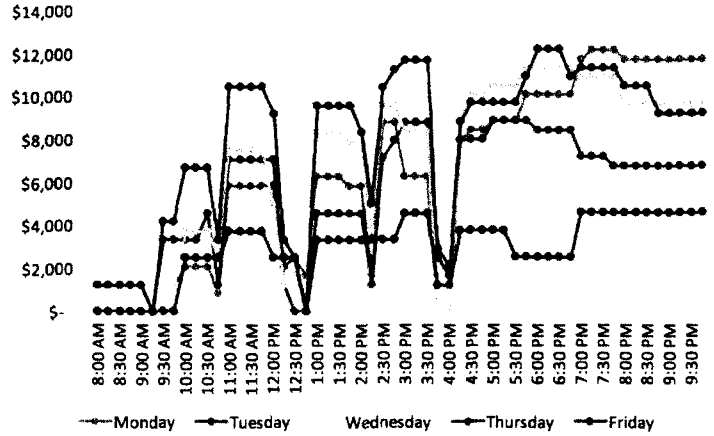

Figure 3: Value of Stream for 15-minute periods for each day (Direct impact without duration information)

The *Direct impact* in Equation 2 is calculated using the duration of the DDoS attack and the number of students. Figure 3 is not a cumulative plot. It gives the value of each specific 15-minute period of service interruption. DDoS attacks commonly last hours, and in some cases, days. In order to calculate the direct impact of the DDoS attack, the point values given in Figure 3 should be cumulatively added.

For example, the direct impact of a DDoS attack with a duration of 12 hours that occurs on Monday between 10 am and 10 pm is $355,955. This value is calculated by cumulatively adding 48 data points within this period. Table 2 presents direct impact values for 12-hour DDoS attacks. Rows specify the start time and the columns specify the day of the week. (+1) in rows indicates that this attack ends on the succeeding day. Darker shading of cells demonstrates the higher impact. Thus, it can be said that the highest impact by a 12-hour DDoS can be reached if it starts on a Thursday morning at 10 am.

Table 2: 12-hour DDoS attack impact

Start - End Times	Monday	Tuesday	Wednesday	Thursday	Friday
10AM - 10PM	$355,955	$309,128	$382,232	$447,0[illegible]	$165,449
1PM - 1AM (+1)	$313,340	$246,950	$327,593	$352,094	$132,931
4PM - 4AM (+1)	$244,618	$178,300	$238,576	$241,029	$91,174
7PM - 7AM (+1)	$142,381	$82,782	$121,227	$123,264	$55,756

Another representation of the values in Table 2 is provided in Figure 4 as a three-dimensional surface plot. Horizontal axes represent the attack start day and time while the vertical axis stands for the direct impact. It can be seen that the highest impact value for a 12-hour DDoS is reached by the attack that starts on Thursday morning. It can be observed that the attacks that start in the afternoon have relatively less impact since there are no classes at night.

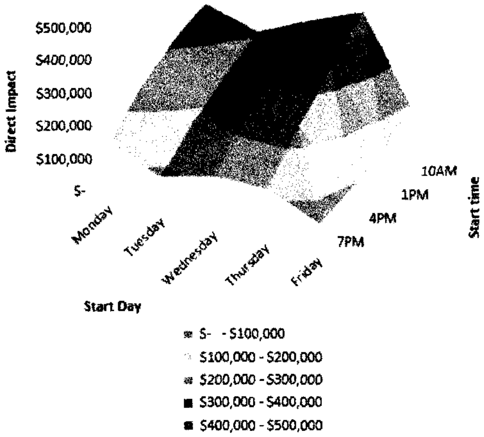

Figure 4: Direct impact of a 12-hour DDoS attack

Figure 5, depicts the direct impact values for 72-hour DDoS attacks. The highest impact, which is almost $M1.16, is reached by the attack that starts on Monday at 7 pm since this attack includes highest demand hours. The impact has lower values for later days of the week because there is no class in the weekend.

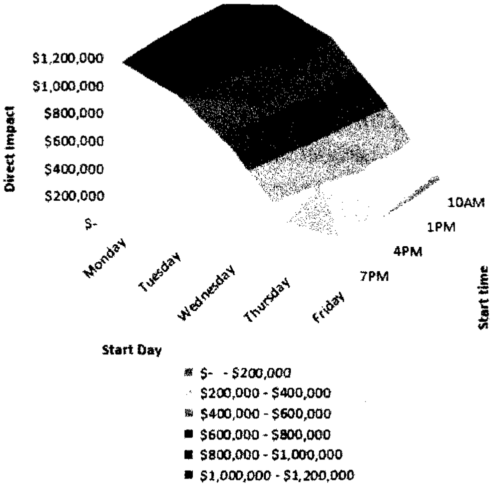

Figure 5: Direct impact of a 72-hour DDoS attack

5.2 Simulation results

To conduct a simulation, the attack is considered to start on Monday at 8 am. Figure 6 represents the Cost of Impact and costs of different risk mitigation strategies. One can compare these functions and choose the best strategy based on the risk tolerance of the organization by using this model and plotting the costs.

For this simulation, the insurance coverage is designated as one million dollars. For simplicity, the deductible and premium amounts are designated as %10 and 1/200 of the coverage, respectively (Skinner, 2017). The average risk control strategy cost is designated as $240,000 (Cdwg, 2017) (See Table 3).

Table 3: Risk mitigation strategy costs

Strategy		Cost
Transfer	Coverage ($Cov)	$ 1,000,000
	Deductible ($Ded)	$ 100,000
	Premium ($Prm)	$ 5,000
Control	Control ($Ctl)	$ 240,000

Eling, M., & Schnell, W. (2016). What do we know about cyber risk and cyber risk insurance?. The Journal of Risk Finance, 17(5), 474-491. http://dx.doi.org/10.1108/jrf-09-2016-0122

Erickson, B. (2016). Cybersecurity Figure of Merit. In Proceedings of the Thirteenth Annual Acquisition Research Symposium (pp. 323–324). Naval Postgraduate School, Monterey, CA

Fielder, A., Panaousis, E., Malacaria, P., Hankin, C., & Smeraldi, F. (2016). Decision support approaches for cyber security investment. *Decision Support Systems*, *86*, 13–23. https://doi.org/10.1016/j.dss.2016.02.012

Gordon, L. A., & Loeb, M. P. (2002). The economics of information security investment. *ACM Transactions on Information and System Security (TISSEC)*, *5*(4), 438–457.

Granadillo, G.G., Motzek, A., Garcia-Alfaro, J. and Debar, H., 2016, August. Selection of mitigation actions based on financial and operational impact assessments. In *Availability, Reliability and Security (ARES), 2016 11th International Conference on* (pp. 137-146). IEEE.

Kaestner, S., Arndt, C., & Dillon-Merrill, R. (2016). *The Cybersecurity Challenge in Acquisition*. Georgetown University Washington United States. Retrieved from http://www.dtic.mil/docs/citations/AD1016746

Lloyd's (2015), "Business blackout – the insurance implications of a cyber attack on the US power grid", available at: www.lloyds.com/news-and-insight/risk-insight/library/society-andsecurity/businessblackout (accessed 6 November 2015).

McMurdie, C. (2017). *"Universities are a top target for cybercriminals" - Charlie McMurdie*. [online] Jisc. Available at: https://www.jisc.ac.uk/news/universities-are-a-top-target-for-cybercriminals-charlie-mcmurdie-03-nov-2016 [Accessed 13 Oct. 2017].

Morse, K.L. AND DRAKE, D.L., 2012. *DATA-DRIVEN MONETIZATION OF ACQUISITION RISK*. JOHNS HOPKINS UNIV LAUREL MD APPLIED PHYSICS LAB.

National Center for Education Statistics. (2017). *Fast Facts*. [online] Available at: https://nces.ed.gov/fastfacts/display.asp?id=80 [Accessed 22 Aug. 2017].

Pinto, C. A., & Garvey, P. R. (2012). *Advanced risk analysis in engineering enterprise systems*. CRC Press.

Rakes, T.R., Deane, J.K. and Rees, L.P. (2012), "IT security planning under uncertainty for high-impact events", *Omega*, Vol. 40 No. 1, pp. 79-88.

Rifai, F. (2017). History is Repeating Itself (In a Good Way) - Corporate Compliance Insights. Corporate Compliance Insights. Retrieved 10 June 2017, from http://www.corporatecomplianceinsights.com/history-is-repeating-itself-in-a-good-way/

Ruan, K. (2017). Introducing cybernomics: A unifying economic framework for measuring cyber risk. *Computers and Security*, *65*(2017), 77–89. https://doi.org/10.1016/j.cose.2016.10.009

Schultz, E. M., & Wydler, V. (2015). *Integrating Cybersecurity into the Program Management Organization*. MITRE Corp McLean VA.

Skinner, L. (2017). *Is cyber insurance worth the cost?*. [online] Investment News. Available at: http://www.investmentnews.com/article/20170115/FREE/170119958/is-cyber-insurance-worth-the-cost [Accessed 10 Oct. 2017].

Spears, J. L. (2005). A holistic risk analysis method for identifying information security risks. In Security management, integrity, and internal control in information systems (pp. 185-202). Springer, Boston, MA.

Tatar, U., Bahsi, H. and Gheorghe, A. (2016). Impact assessment of cyber attacks: A quantification study on power generation systems. *2016 11th System of Systems Engineering Conference (SoSE)*.

Tatar, Ü. and Karabacak, B., 2012, June. An hierarchical asset valuation method for information security risk analysis. In *Information Society (i-Society), 2012 International Conference on* (pp. 286-291). IEEE.

Tatar, Ü., Çalik, O., Çelik, M. and Karabacak, B., 2014, January. A Comparative Analysis of the National Cyber Security Strategies of Leading Nations. In *International Conference on Cyber Warfare and Security* (p. 211). Academic Conferences International Limited.

Walker, R. (2017). *Colleges and universities see an uptick in denial-of-service attacks*. [online] EdScoop. Available at: http://edscoop.com/colleges-and-universities-see-an-uptick-in-denial-of-service-attacks [Accessed 19 Oct. 2017].