Cyber supply chain security a cost benefit analysis using net present value

Cyber Supply Chain Security: A Cost Benefit Analysis Using Net Present Value

Abel Ofori-Yeboah[1]
School of Computing and Engineering
University of West London
London, UK
abel.yeboah-ofori@uwl.ac.uk

Ronald Addo-Quaye[2]
School of Business and Law
Central Queensland University
Australia
ronald.addoquaye@cqumail.com

WaheedOseni[3]
School of Computing and Engineering
University of West London
London,UK
waheed.oseni@student.uwl.ac.uk

Prince Amorin[4]
Graduate School MIS
Coventry University / GCTU
pi.amorin@yaahoo.com

Conrad Agangmikre[5]
School of Computing and Engineering
University of West London
21463769@student.uwl.ac.uk

Abstract-Cyber supply chain (CSC) security cost effectiveness should be the first and foremost decision to consider when integrating various networks in supplier inbound and outbound chains. CSC systems integrate different organizational network systems nodes such as SMEs and third-party vendors for business processes, information flows, and delivery channels. Adversaries are deploying various attacks such as RAT and Island-hopping attacks to penetrate, infiltrate, manipulate and change delivery channels. However, most businesses fail to invest adequately in security and do not consider analyzing the long term benefits of that to monitor and audit third party networks. Thus, making cost benefit analysis the most overriding factor. The paper explores the cost-benefit analysis of investing in cyber supply chain security to improve security. The contribution of the paper is threefold. First, we consider the various existing cybersecurity investments and the supply chain environment to determine their impact. Secondly, we use the NPV method to appraise the return on investment over a period of time. The approach considers other methods such as the Payback Period and Internal Rate of Return to analyze the investment appraisal decisions. Finally, we propose investment options that ensure CSC security performance investment appraisal, ROI, and business continuity. Our results show that NVP can be used for cost-benefit analysis and to appraise CSC system security to ensure business continuity planning and impact assessment.

Keywords: Cyber Supply Chain, Cost Benefit Analysis, Net Present Value, Cyber Security, Business Continuity

I. INTRODUCTION

Balancing cyber supply chain security spending in an operationally effective manner to protect organizations and third-party assets have been challenging due to inadequate cost benefit analysis [1] [2]. Investing adequately in CSC security has not always been the priority of various organizations, especially in third party systems leading to various cyberattacks and risks [3], with many deciding to invest after a breach [18].

Cyberattacks are deploying various attacks on supplier inbound and outbound chains through third party systems to gain access to major organizational systems [4] [5]. There have been several cyber supply chain attacks, such as the Dragonfly 2011 Cyber Espionage group targeting companies through their supply chain [6] Shylock Banking Trojan in 2014: Man in a Browser attack deployed to compromised eBanking, e-Products and e-Process service websites [6]. Third Party Data Store Attack 2013: use botnet to exfiltrating data linked to the public internet [6], indicating the need for threat analysis in CSC security [7]. Havex 2014. targeted energy sector companies by spreading malware, indicating the need for threat predictions [8] [9]. Watering Hole attack: uses (RAT) attack to target CSC website [10]. Recent ransomware attacks such as the JBS Food Chain and US pipeline attacks [11] that impact various organizations and third parties in multiple countries in the CSC environment provide us with some of the scales of investment appraisals required for our study. Thus, there is the need to consider the economics of scale for CSC security that provide optimum investment levels to improve security goals.

There are existing works of literature that have considered modelling the economics of scale in cybersecurity investments [1], [2], [18] [22] to provide state of the art analysis and investment models to improve CSC security control mechanisms. However, the rate of cyberattack detections from third-party vendors, vulnerability assessment and assets controls have not been addressed adequately and cost-effectively to improve optimum operational performance on the supplier inbound and outbound chains. Additionally, investment appraisal decisions are required to determine the return on investments (RoI).

The paper explores the cost-benefit analysis of investing in cyber supply chain security to improve security. The contribution of the paper is threefold. First, we consider the various existing cybersecurity investments and the supply chain environment to determine their impact. Secondly, we use the NPV method to appraise the return on investment over a period of time. The approach considers other methods such as the Payback Period and Internal Rate of Return to analyze the investment appraisal decisions. Finally, we propose investment options that ensure CSC security performance investment appraisal, ROI, and business continuity. Our results show that the NVP method can implement cost benefit analysis and appraise CSC system security to ensure business continuity planning and impact assessment.

II. STATE OF THE ART

This section discusses the start of the art and related works in cyber supply chain security and considers CSC

978-1-6654-7878-6/21/$31.00 ©2021 IEEE
DOI 10.1109/ICSIoT55070.2021.00018

systems security's various cost benefits analysis concepts.

A. Cyber Supply Chain Security

Cyber Supply Chain Security involves protecting the supply chain systems and information accessed and transmitted via the internet or through any computer network in the supply chain environment. CSC seeks to ensure the following key objectives in the supply chain. First, shield the exclusivity and confidentiality of individual entities information. Secondly, it safeguards the integrity comprises accuracy, structure, reliability, and cogency of supply chain data. Thirdly, CSC security ensures that supply chain information is available and only accessed on demand when given the requisite permissions. Human resource and technical expertise are crucial in achieving impenetrable security in coordinated and uncoordinated attacks in CSC systems [1]. However, achieving these resource levels often requires capital investment in environments with competing demands for capital allocation in an organization.

CSC security requires implementing and configuring firewalls, access controls, intrusion detections, and encryption. However, Procuring and implementing any of these technologies for safeguarding supply chain networks require capital investment. Furthermore, employees, suppliers and contractors working in the supply chain network need to have the requisite training to develop the competency and behaviours to prevent attacks and data breaches.

The most significant incentive for any private or public organization is to invest in cybersecurity activities. It will serve as a motivation to increase the organization's value to its owners and the stakeholders. This paper aims to synthesize existing literature to explain why a more holistic approach is required for cybersecurity investment.

B. Risk Associated with Cybersecurity

The difficulty associated with cybersecurity investments deals with the risks (or uncertainty) related to such investments. It is significant to identify at the beginning that 100% security is hardly practicable in a practical sense and not cost-beneficial in an economic sense. Consequently, it is vital to realize that cybersecurity investments are envisioned to lessen the risk of cybersecurity breaches. Nevertheless, determining the reduction in the probability of a particular breach taking place, let alone a string of breaches taking place, as a result of a cyber investment is enormously challenging to evaluate. However, in estimating the benefits from cybersecurity investments, it becomes compulsory to associate those benefits with the probability of the incidence of security breaches. In other words, the "expected" cost savings (i.e., expected benefits) from cybersecurity investments are derived by multiplying the possible cyber losses by the difference between the probability of the cyber security losses occurring prior to the cybersecurity investment and the probability of the cybersecurity losses occurring after the investment [12].

Cybersecurity investment does not generate direct cash returns. Thus, a business case for cybersecurity investments is often more difficult than making the business case for many other investments. There are at least three aspects to this difficulty. Primarily, the benefits derived from cybersecurity investments are challenging to measure. Additionally, the risks associated with cybersecurity investments are also challenging to measure. Finally, there are externalities associated with cybersecurity investments [13].

C. Defence Cybersecurity Investment Cost

Investment in defence costs and security controls aims to protect the asset of an organization. When this fails, expenses related to damages and losses are incurred [14]. These two cost streams are explored to understand better how to categorize and quantify such costs. For instance, Brecht and Nowey (2012) established a model for quantifying cybersecurity costs for increasing accuracy, objectivity, and comparability. Their principle for cost-benefit calculation: costs for managing information security costs related to information security measures, costs incurred by information security incidents and cost of capital induced by information security risks. Subsequently, the authors recommended the information security management system (ISMS)-layers approach to information security cost quantification, 1319 Cybersecurity economics which takes the perception of information security management [14]

D. Measurement the Effectiveness of Cyber Security Controls

The purpose of measuring the efficiency of security controls is to recognize how a set of applied controls translates to a loss probability. The marginal development of adding one to a set of controls is already in operation. Ideally, security improvements may be expressed in terms of the impact of VaR. NIST [15] [16]; Pagett,´ 2010) provide approaches but fail to link to loss prospects and marginal improvements for new controls. Pagett (2010) argue that standards-based IT governance models such as COBIT, NIST and ISO27004 are more focussed on "what" needs to be measured rather than "how". In response, they propose an information security effectiveness framework to address the "how", with effectiveness measured based on control characteristics [16] to measure the efficacy; that way seems promising. However, the proposal focuses on what a designated policy recommends, such as how many computers have an antivirus installed. What if the strategy is flawed, but the characteristics otherwise score thoroughly? That may lead an organization to be tricked into a false sense of security.

D. Derived Benefits from Cyber Security Investment.

The first difficulty related to cybersecurity investments is recognizing and assessing the benefits derived from such investments. The main benefits pertaining to cybersecurity investments are the future "cost savings" derived from the prevention of losses due to cybersecurity breaches [3]. However, if breaches were prevented, the actual losses would not occur and would not be observable. The better the security, the less an organization, will observe the losses resulting from cybersecurity breaches. Thus, organizations need to estimate the potential losses from cybersecurity breaches in order to evaluate the benefits derived from cybersecurity investments. Faced with an opportunity to

invest in more protection, it is beneficial to understand how to calculate the benefits from security investments and get guidance on finding the optimal level to invest. Gordon and Loeb (2006) postulate that cost-savings result from the potential losses from incidents, the loss probability, and its reduction from an investment [18]. The authors propose an approach to determine the optimal level of investment by a loss probability function with an investment level and a vulnerability level. Expected losses are generated by threat probability and monetary losses to an asset. The calculation may be conducted without historical attack data; the investment level is the only decision variable. However, the vulnerability level and expected losses still need to be derived somehow. By contrast, Huang et al. (2008) discuss the use of expected utility theory to identify the security investment level that maximizes the utility of the investment. The framework presented is like the [20] used but with different boundary conditions and assumptions. To compute the optimal security investment, the security team must determine the probability of a security incident occurring in each time frame, an investment level, a potential loss and a risk-aversion coefficient. The authors applied classical economic theories to compute an optimal security investment to protect an asset. As an input, historical data to determine the loss probability are needed and a risk-aversion coefficient [20].

All the existing literatures are relevant to cyber security and supply chain investments. However, non of the literature applied the NPV method to cyber supply chain security investments for cost-benefit analysis and investment appraisals.

III. APPROACH

The proposed approach considers the Present Net Value (NPV) model to determine the cost benefit analysis and the return on investments within the CSC network security systems domain. We used the NPV algorithm to determine the rate of returns over a period of time. Further, the approach considers other methods such as the Payback Period and Internal Rate of Return to analyze the investment appraisal decisions. The cyberattack and cyber supply chain security phenomenon requires a systematic approach to utilize, monitor the phenomena to arrive at a conclusion, and evaluate the hypothesis [23]. The most daunting challenge for organizations is determining which cyber supply chain investment is worthwhile. Thus, we consider existing work and models to identify gaps and propose a model that could analyze the investment appraisal decisions for CSC security investments [1], [18], [22].

Cost benefit analysis compares the cost of an activity to benefits that would arise from performing such activity. The comparison output informs or guides investors in an efficient allocation of resources and in decision-making regarding which assets are critical and worthy of investing in that organization or third party [18]. We use the Net present value formula below for our work.

Net Present Value (NPV)

$$NPV = I_o + \sum \frac{F_t}{(1 + r + p_t)^t}$$

A. Cost benefit analysis and Cyber Supply chain

The cost-benefit analysis method compares an activity cost to the benefits derived from that activity to ensure economic and efficient distribution of limited capital resources. In the Cyber supply chain environment, cost benefit assessment means weighing the cost of added cyber supply chain safeguarding activity with the benefits that emanate from that activity. As the outcome of the benefit from implementing a cyber supply chain security activity exceeds its cost, it is a classified investment worth pursuing. When the cost outweighs the benefit, that activity should not be pursued further or implemented.

This work seeks to illustrate how to efficiently manage supply chain security resources using the cost versus benefit comparison to make decisions on required capital investment in supply chain setup.

B. Calculating Return on Investments in CSC Security

A return on CSC Security involves investment in expertise, state of the art technology and security controls.

Return is calculated using formular below :

$$\text{Return} = \textit{Income from investment} + \frac{\textit{Capital Gain}}{\textit{Cost of Investment}} \qquad (1)$$

Calculating Return on investments can be expressed as follows:

$$\text{ROI} = \textit{(Current value of investment} - \frac{\textit{Cost of capital)}}{\textit{Cost of Investment}} \qquad (2)$$

$$\text{Return on Investment ROI} = \frac{\textit{(Gain on investment)}}{\textit{Cost of Investment}} \qquad (3)$$

C. Costs in Supply Chain Security

A key component of Cyber Supply chains expenditure originates following activities undertaken to reduce the likelihood of security breaches. Practical examples include associated expenditures for implementing firewalls and intrusion detection systems. On the other hand, necessary expenditures also arise from activities required to correct and restore the system to a normal operational working state.

D. Benefits of Cyber Supply Chain security

Cyber supply chain security includes implementing security control mechanisms, policy formulations and third-party auditing activities to safeguard the cyber physical, cyber digital and physical or human element of the network system. Implemented appropriate security on the supply inbound and outbound chains deliver long term cost savings to the organization. That includes eliminating the cost incurred when cyberattacks and breaches occur. It ensures confidentiality, integrity, availability to the network systems. Further, the CSC security ensures safeguards to the organizational requirements, business processes, data structures and provide information assurance, customer confidence, reliability, and trust to the organization and

E. Operational Cost vs Capital Investments

The total costs of expenditures from cyber supply chain security investment are categorized into

Operational and Capital Investments. Operational costs or expenditure consist of spending that benefits a specific duration time frame. These are cost elements that are charged to the time frame/period. Such costs include investments in robust security systems, expertise and the rollout of software patches internally to avoid breach occurrence. Capital Investments refers to expenses that would benefit an organizations operation for a duration of years. These types of costs can appear on balance sheets.

IV. IMPLEMENTATION

This section considers the NPV model for the implementation approach discussed in section 3 and compares the method to the IRR model for our investment appraisal. We consider the following three steps for calculating the NPV using the two scenarios for our implementation. First, calculate the total value of the investment on the CSC assets. NPV ensures that if the investment return is positive, then it means that the discounted present value of all investments related to the security investment will be positive and safeguarded. We estimate the future investments required for each period and determine the correct discount rate.

A. Case Study of JBS Food Packaging

We consider the ransomware case study of the JBS food chain [11] to illustrate the application of NPV we look at cyber supply chain giant organization such as JBS food product that experienced a ransomware attack that affected its IT systems and operations and impacted on business in Australia, Canada and the USA. JBS paid $11m (£7.8m) in ransom to the cyberattacks. We assume this organization requires investing in its CSC network systems security to prevent the latest attack. The attack may be deployed through Island hopping, Remote Assess Trojan (RAT). The latest model version of an Intrusion detection system. Table 1 assumes that an initial capital security investment of £10,000.000 was made. The cost of the $10,000.000 raised from bank consortium at 15% per annum. The initial investment is implemented at the commencement of the first period from the recent attached cost reported in [11]. We assume that the initial investment has a five years life. The benefits of the annual cost savings derived from the investment made on CSC security will probably prevent the payment of the $11m or the £7.8mpaid to the cyberattacks and invest the annual operating cost of $100,000. Thus, the net benefits (excluding the initial investment) are estimated to save millions of dollars for the organizations.

B. Calculating Cost vs Benefits Using NPV

The costs involved in these activities are often quite enormous. In addition, organisations will also incur costs in detecting and correcting breaches that could have been prevented. Therefore, all the Cyber supply chain benefits are associated with cost savings (also called cost avoidance) associated with preventing breaches and compromises to the CSC.

Net Present Value (NPV) Calculations Over Five Years

$$NPV = I_o + \sum \frac{F_t}{(1 + r + p_t)^t}$$

Where:
I_o = Cost of Investment
F_t = net cash flow over a period of time
t = Period of time
r = required rate of return
$\mathbf{P_t}$ = Inflation rate during t

Year 1

$$NVP = 10{,}000{,}000 + \sum \frac{200{,}000{,}000}{(1 + 0.15 + 0.08)^1}$$

$$= 10{,}000{,}000 + \sum \frac{200{,}000{,}000}{(1.23)^1}$$

$$= 10{,}000{,}000 + 162{,}601{,}626$$

NPV = 172,601626

Year 2

$$NPV = 10{,}000{,}000 + \sum \frac{200{,}000{,}000}{(1.23)^2}$$

$$= 10{,}000{,}000 + \frac{200{,}000{,}000}{1.5129}$$

$$= 10{,}000{,}000 + 132{,}196{,}443$$

NPV=142,196,443

Year 3

$$NPV = 10{,}000{,}000 + \sum \frac{200{,}000{,}000}{(1.23)^3}$$

$$= 10{,}000{,}000 + \frac{200{,}000{,}000}{1.8608}$$

$$= 10{,}000{,}000 + 107{,}480{,}653$$

NPV=117,480,653

Year 4

$$NPV - 10{,}000{,}000 + \sum \frac{200{,}000{,}000}{(1.23)^4}$$

$$= 10{,}000{,}000 + \frac{200{,}000{,}000}{2.2888}$$

$$= 10{,}000{,}000 + 87.382{,}034$$

NPV = 97,382,034

Year 5

$$NPV = 10{,}000{,}000 + \sum \frac{200{,}000{,}000}{(1.23)^5}$$

$$= 10{,}000{,}000 + \frac{200{,}000{,}000}{2.8153}$$

$$= 10{,}000{,}000 + 71{,}040{,}386$$

NPV= 81,040,386

Internal Rate of return model

$$I_o = \sum_{n=1}^{t} \frac{ACF_t}{(1 + IRR)t}$$

IRR provides a simple managerial decision rule for accepting or rejecting incremental cyber supply chain security activities. The rule is to:

- Reject the additional cybersecurity activities if the IRR is smaller than the organization cost of capital.

- Be indifferent to additional cyber security inflation rate during supply chain security activities if IRR is equal to the organization cost of capital.
- Accepted if the additional cyber supply chain security activities of the IRR is greater than the organization cost of capital.

Table 1. Presents the Net Value Calculations for JBS CSC Security Investments

Year	Net Cash Flow ($)	Formulae	NPV ($)
0	10,000,000	$PV = I_o + \sum \frac{F_t}{(1+r+p_t)^t}$	10,000,000
1	10,000,000	$NVP = 10{,}000{,}000 + \sum \frac{200{,}000{,}000}{(1+0.15+0.08)^1}$	172,601626
2	10,000,000	$10{,}000{,}000 + \sum \frac{200{,}000{,}000}{(1.23)^2}$	142,196,443
3	10,000,000	$10{,}000{,}000 + \sum \frac{200{,}000{,}000}{(1.23)^3}$	117,480,653
4	10,000,000	$10{,}000{,}000 + \sum \frac{200{,}000{,}000}{(1.23)^4}$	97,382,034
5	10,000,000	$10{,}000{,}000 + \sum \frac{200{,}000{,}000}{(1.23)^5}$	81,040,386

D. Results

The results in table 1 indicate that suppose an initial organization investment in an organization is $200,000.000. The strategic management team decides to invest $10,000.000 in security, at 15% required rate of return and 8% Inflation rate during the time (5years period) in critical areas such as expertise, penetration testing, vulnerability assessments, appropriate security tools, regular updates and patches, investment in third party auditing and controls to mitigate threats and risks in the event of attacks, the invest, in the long run, will be cost-effective to the organizational goal.

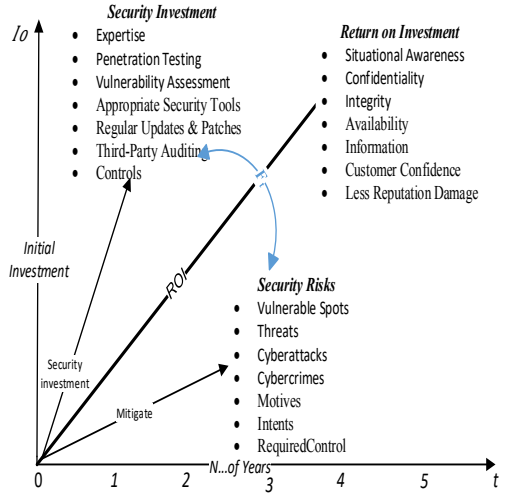

Fig. 1. Appraisal of CBA and Return on Investment

Fig. 1 provides an investment appraisal model of how an organization can use a cost benefit analysis and a return on investment over a period of time in a CSC system to derive the appropriate level of security. The model considers three valuable components and findings. Security investment, security risks and return on investment. The model express that should an organization invest in securing key areas as part of the initial investment (I_o), such as expertise, penetration testing, vulnerability assessments, appropriate security tools, regular updates and patches, investment in third party auditing and controls over a period.

Although cyberattacks cannot be prevented entirely, the investment will positively impact security risks such as identifying vulnerable spots, threats, cyberattacks, cybercrime, motives, intents and implementing required controls mitigated with time.

Subsequently, that will ensure secure business processes and information flows on supply inbound and outbound chains and reduce attacks. Eventually, that will create situational awareness, assuring confidentiality, integrity, availability, information assurance, customer confidence, trust, and reputation in the long run.

Thus, applying cost benefit analysis on cyber supply chain security implementations from an investment standpoint provides a proactive security investment approach for strategic management decision-making, information assurance, and improves parallel security on third party systems over a period of time.

V. DISCUSSIONS

The cost of investment in security is not tangible and does not generate cash flow returns. Implementation of CSC security using CBA is relevant in providing ROI in situational awareness, and ensuring confidentiality integrity, availability, information assurance and customer confidence and minimizing reputational damage. NPV appraisal methods are not utilized prior to sanctioning such scopes. The cost benefit analysis (CBA) assist in integrating the requirements and objectives of a security policy with organizational goal and security goal. CBA provides strategic management with the necessary information relating to CSC security investments and the cost of alternatives for cyber threat mitigations. For instance, CBA results are used to compare the expected cost of a ransomware attack on an asset against the cost of investment in securing the assets against threats and vulnerabilities and its cascading impact. CBA in the cyber supply chain environment identifies threats, vulnerabilities, and the probable risks to the assets on the

supply inbound and outbound chains and quantifies the cascading impact for budget purposes.

We appraised the value of the organizational assets by analyzing using impact assessment to ensure cost-effective safeguards are implemented. The value of an asset on the CSC determines the direct effects and the level of security required to protect it. Implementing CBA will ensure that the annual cost of security investment on the various integrated network nodes does not exceed the annual cost of overall assets lost in the event of an attack. For instance, JBS Products paid the attacks £7.8 million in bitcoins after it experienced a Ransomware attack. That could have been avoided suppose the organization has implemented hot backups to restore the system to its operational use in the event of an attack and carried out third-party auditing to ensure that their systems comply with parallel security policies. Cyber supply chain security investment appraisal considers three objectives that ensure safeguarding: asset value protection, preventing information and protecting data from integrity flaws.

VI. CONCLUSIONS

Due to the dynamic, invincibility and fuzzy nature of cyber attacks, implementing cyber supply chain security on the supply inbound and outbound chains has been challenging in safeguarding the network systems. Threat actors deploy various tactics, techniques, and procedures to penetrate, infiltrate, manipulate, exfiltrate and obfuscate the network leading to various breaches.

Thus, applying cost benefit analysis on cyber supply chain security implementations from an investment standpoint provides a proactive security approach, third party auditing, and improves parallel security on the organization and third party system.

In this paper, we have used a case study of the JBS food chain for our implementation and the net present value method to calculate the cost of investments, return on investments and cost of alternatives over a period of time to determine the cost benefit analysis and for strategic investment decision makings to safeguard the cyber supply chains systems in parallel security implementation. Future works will include the calculation of the Payback Period and Initial Rate of Return to determine future investment trends,

REFERENCES

[1]. J. Simon and A. Omar, "Cybersecurity investments in the supply chain: Coordination and a strategic attacker" European Journal of Operational Research, Volume 282, Issue 1, 2020, Pages 161-171, ISSN 0377-2217, doi.org/10.1016/j.ejor.2019.09.017.

[2]. S. Ekelund, and Z. Iskoujina, "Cybersecurity economics – balancing operational security spending", Information Technology & People, Emerald 2019, Vol. 32 No. 5, pp. 1318-1342. https://doi.org/10.1108/ITP-05-2018-0252

[3]. R. L. Kumar, and S. Park, "A portfolio approach to supply chain risk management." Decision Sciences, 2019. 50 (2), 210–244.

[4]. C. Williams, "Security in the cyber supply chain: Is it achievable in a complex, interconnected world?" Technovation, 2014. 34 (7), 382–384.

[5]. S. B. Modi, M. A. Wiles, and Mishra, S. (2015). Shareholder value implications of service failures in triads: The case of customer information security breaches. Journal of Operations Management, 35, 21–39

[6]. National Cyber Security Centre." Example of Supply Chain Attacks." NCSC. 2018. [Online] Available: https://www.ncsc.gov.uk/collection/supply-chain-security/supply-chain-attack-examples.

[7]. A. Yeboah-Ofori, and S. Islam, "Cyber Security Threat Modelling for Supply Chain Organizational Environments." MDPI. Future Internet. 11, (3), 63, March 2019. doi: 10.3390/611030063.

[8]. B. Woods, and A. Bochman, "Supply Chain in the Software Era" Scowcroft Center for Strategic and Security. Atlantic Council: Washington, DC, USA, May 2018.

[9]. A. Yeboah-Ofori et al., "Cyber Threat Predictive Analytics for Improving Cyber Supply Chain Security," in IEEE Access, vol. 9, pp. 94318-94337, 2021, doi: 10.1109/ACCESS.2021.3087109.

[10]. US-Cert. "Building Security in Software & Supply Chain Assurance." 2020. [Online] Available: https://www.us-cert.gov/bsi/articles/knowledge/attack-patterns.

[11]. BBC News "Meat Packaging Giants JBS pays $11m in Ransom to Resolve Cyber-attack" (assessed 12 October 2021) https://www.bbc.co.uk/news/business-57423008

[12]. B. Atkins, "Board focus on cyber security: a director's perspective." Corporate Governance Advisor, 2013, 21(4), 24–26.

[13]. R. Young., and J. Windsor, (2010). Empirical evaluation of information security planning and integration. Communications of the Association for Information Systems, 26(1), 245–266.

[14]. Y.-W., Wu, Y.-L., Wang, Y.-S. and Chen, C.-L. (2017), "Investigating the post-adoption stage of voice over internet protocol (VoIP) telephony diffusion: a use-diffusion approach", Information Technology & People, Vol. 30 No. 4, pp. 753-784.

[15]. NIST (2008), "Performance measurement guide for information security", available at: http://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-55r1.pdf/ (accessed 19 September 2018).

[16]. J. Pagett, and S. Ng, (2010), "Improving residual risk management through the use of security metrics", available at: https://cdn.ttgtmedia.com/searchSecurityUK/downloads/RHUL_Pagett_v2.pdf/ (accessed 19 September 2018)

[17]. Campbell, K., L. Gordon, M. Loeb, and L. Zhou. "The Economic Cost of Publicly Announced Information Security Breaches: Empirical Evidence from the Stock Market." Journal of Computer Security. 2003.11(3):431-448.

[18]. L. Gordon and Martin Loeb. "Managing Cyber Security Resources: A Cost-Benefit Analysis." 2006 New York: McGraw Hill.

[19]. L. Gordon, M, Loeb, and Zhou, L. "Investing in Cybersecurity: Insights from the Gordon-Loeb Model." Journal of Information Security, 2016. 7, 49-59. doi: 10.4236/jis.2016.72004.

[20]. C. D. Huang, Q. Hu, and R. S. Behara, "An economic analysis of the optimal information security investment in the case of a risk-averse firm" International Journal of Production Economics, Elsevier, Volume 114, Issue 2, 2008, Pages 793-804, doi.org/10.1016/j.ijpe.2008.04.002.

[21]. B.R., Rowe, & M.P. Gallaher, "Private Sector Cyber Security Investment: An Empirical Analysis". 2006 WEIS.

[22]. V. Jacobs, J. Bulters, and M, van Wieren, "Modeling the impact of cyber risk for major Dutch organizations", 2016. in Koch, R. and Rodosek, G. (Eds), Modeling the Impact of Cyber Risk for Majo Dutch Organizations, "European Conference on Cyber Warfare and Security" at Bundeswehr University, Munich, 7–8 July, Academic Conferences International Limited, Reading, pp. 145-154.

[23]. U. Sekaran, (2003), Research Methods for Business: A Skill Building Approach, John Wiley & Sons, Danvers, MA. Shih,