UDK 658.1+004.056+65.012

WOOD Katie,
BSc (Hons) PG Cert, Post Grad, SFHEA, IISP,
Senior Lecturer, Programme Team Leader
for Applied Computing,
School of Mathematics and Computer Science,
Faculty of Science and Engineering,
University of Wolverhampton, West Midlands,
England
BIRCH Nigel,
MIoD AMInstKT Research &
Development/Knowledge Transfer Director,
University of Wolverhampton, West Midlands,
England

CYBER SUPPLY CHAIN RESILIENCE MANUFACTURING IMPACT ON THE ECONOMIC SECURITY

Cybersecurity is a prominent threat to businesses, especially in the manufacturing sector as a range of sub-contractors and businesses providing resources to a prime to create a global operational network. Cyber criminals seek opportunities to expose system flaws for their own gain, therefore any weak link in the supply chain IT infrastructure can have a catastrophic impact in terms of reputation, financial and economic value to the businesses and economic impact on the country they are based. This paper focus on the impact of cyber supply chain resilience within the manufacturing sector in relation to impacting the economic security. This paper outlines that within the UK on a national and sector level there is inefficient implementation throughout the whole supplier chain to support and protect economic prosperity.

Keywords: *Cybersecurity, Economic Security, Risk Assessment, Critical National Infrastructure and Enterprise Economic.*

Introduction. Formulation of the problem. "*Resilience is all about being able to overcome the unexpected. Sustainability is about survival. The goal of resilience is to thrive."* [1]

The supply chain within manufacturing is critical for innovation and product development to be achieved. It has been widely documented [2] that the manufacturing sector is now one of the most frequently hacked industry; second only to healthcare. This illustrates the need for supply chain cyber resilience strategies to be embedded throughout the whole supply chain to protect businesses that are directly involved downstream or upstream of the manufacturing ecosystem.

The remainder of this paper is organized as followed: Section II outlines the role or Information Systems and how cyber needs to be acknowledged in advancements of Information Systems. Section III presents an overview of global cyber manufacturing challenges and risk. Section IV specifically focuses on the UK Manufacturing sector and UKs current initiatives in cyber education and improving economic security. Section V focus on resilience through the supply chain which is followed by Section VI that highlighted the gaps in the sector and areas in which work is required. Section VI finally concludes this paper and outlines further work which includes the development on strengthening the Cyber Supply Chain model outlined in this paper.

Analysis of recent research and publications. Information Systems Development. All sectors have been influenced due to the ever changes developing and use of information systems. In the manufacturing sector it is critical that to remain competitive that they adopt different techniques and technologies.

The manufacturing sector use industrial control systems (ICS) that connected to the internet. There is also increase use and dependent on Cloud systems and mobile devices, thus making manufacturing operations increasingly exposed to cyberattacks. Primarily, attackers are keen to breach system vulnerabilities to gain unauthorized access to sensitive systems and data, particularly to seek Intellectual Property. The main argument of this paper is that further work is needed in the integration throughout the supply chain within the manufacturing sector.

Without businesses conducting a cyber risk assessment there is no cyber resilience audit to ensure improvements and suitable action is taken. Through exploiting the vulnerabilities within a supply chain and then using risk migration techniques to migrate this, will ensure greater collaboration understanding and critical mass of migration risk in a complementary way to develop and strength supply chain resilience.

The National Institute of Standards and Technology [3], assurance is defined as being ‘Grounds for confidence that the other four security goals (integrity, availability, confidentiality, and accountability) have been adequately met by a specific implementation. The original stages of growth module, as applied to the field of Information Systems. Gibson and Nolan (1974) [4] have been revisited by several authors to reflect the importance and changes to strategic information systems development and its critical role within business operations. Nolan [5] extended this model to reflect the need to manage the crises in data processing. Other models such as he Greiner Curve Model attempts to predict the six phases and possible crisis trigger phases that a business might experience as they grow. This model supports the need for change management processes to deal with anticipate challenges.

The purpose and objectives of the study – to explore cyber supply chain resilience manufacturing impact on the economic security.

Presentation of the main research material. In such a global operational sector as manufacturing, the prime needs to be ready to adopt and adapt multiple strategies to ensure security. To strengthen the supply chain resilience to cyber, an agile approach is essential, as quick response time is critical to protect and not impact on the economic security. The authors of this paper believe at key attributes of Nolan’s works and The Greiner Curve can be interlinked and be further developed which with a focus on the stages with cyber crisis might be at its highest risk.

The Organisational Cyber Risk Profile model shows the stress points of increase risk of cyber vulnerabilities to due unsalable/high rapid growth. When high growth occurs quickly the supply chain is exposed to risk due to being noncompliance or protection as it is at a stage of unknown direction. The emphasis in the business culture is profile and performance driven to gain outputs. Therefore cyber security is a stress point which will be heighten at certain crisis stages of a growth life cycle.

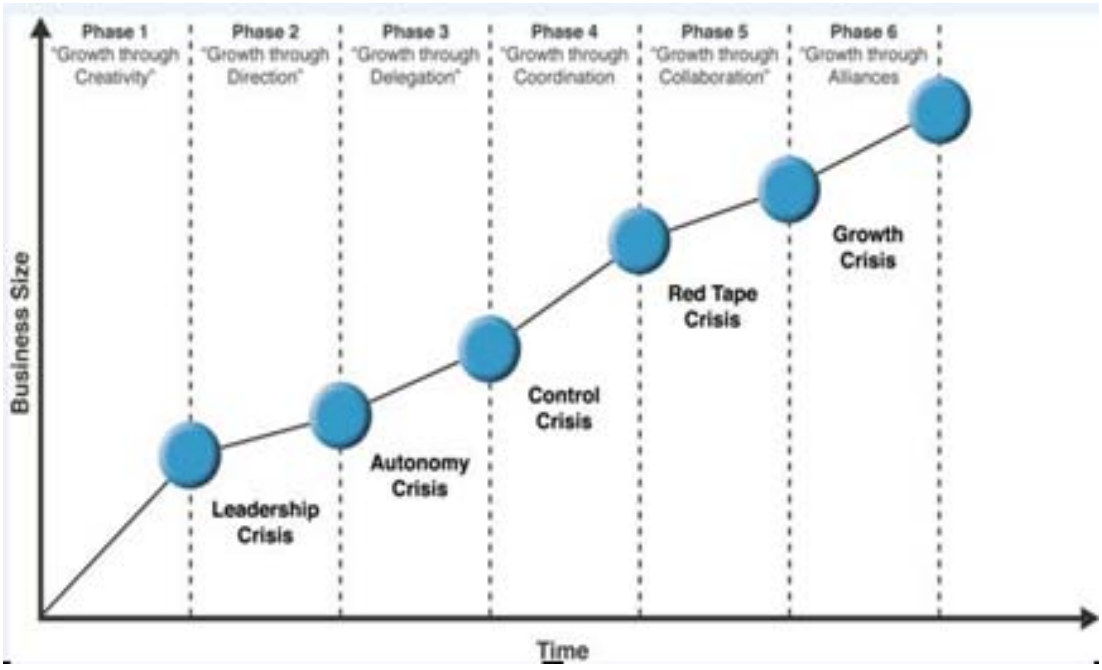

Figure 1. Greiner Curve Model [6]

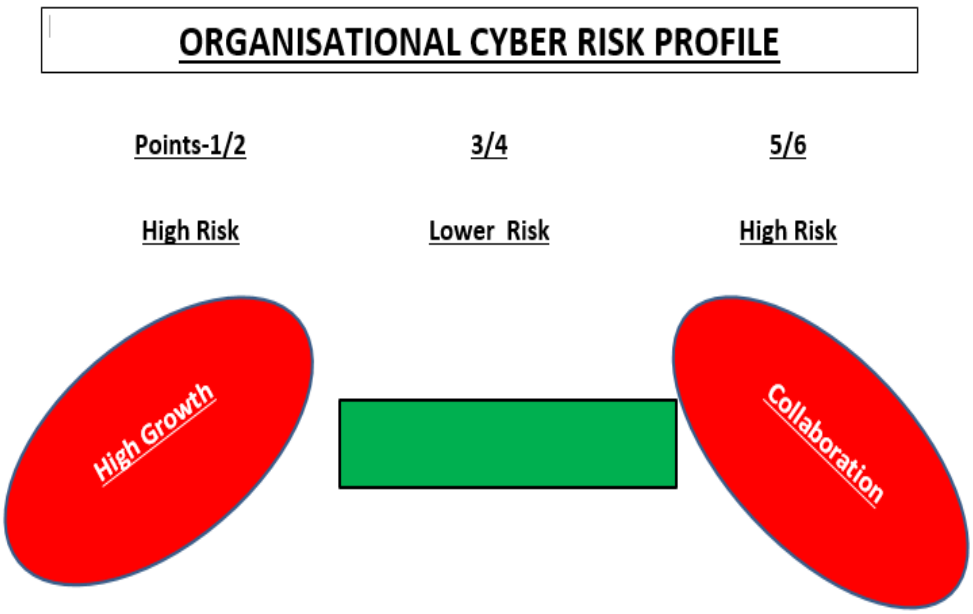

Figure 2. The Organisational Cyber Risk Profile Model

Global Cyber Manufacturing. Manufacturing is a sector that is typically associate with global operations. Globalization has created new concerns, with cyber security often at the mercy of conflicting regulations, no regulations, cultural differences, and varying degrees of national technological maturity. [7]

As highlighted by Delotte [8], in the manufacturing sector systems security has been a lesser issue, compared to performance and safety Therefore this is resulting 'security gaps in production systems.' This is further demonstrated by Qatalyst Global [9] findings showed that 'Manufacturing spends the least on Information Security and has conceivably experienced the worst cyber intrusions.' This point is illustrated and supported by Sikich 2016 Manufacturing Report [10]. The finding found that only 33% of respondents conduct an annual penetration test, 42% do not and more concerning is the 25% of respondents are not sure if they perform annual penetration testing. Given that cyber related attacks are growing in the manufacturing sector, demonstrates the level of cyber illiterates in the sector.

Cyber Status in the UK. Manufacturing contributes £6.7tn to the global economy. UK manufacturing is the world's ninth largest industrial nation. makes up 10% of GVA and 45% of UK exports, and directly employs 2.7 million people. [11]This shows the impact financial economy value that this industry has on shaping the UK economy. The year on year increase of cyber related attacks within the manufacturing supply chain in both hindering cyber resilience of the industry and economic security. Within the UK there has been investment and cyber programmes developed, such as the HM Government Cyber Governance Health Check for 2015 was released in May 2016 which aim was to provide a benchmark for FTSE 350 businesses to look at cyber awareness and preparedness. The National Cyber Security Centre (NCSC) [12] was created in 2016 and set out the importance of government, industry and law enforcement to work in even closer partnership, to defend the UK against Cyber-attacks. [13]

Resilience Through The Supply Chain. Within global high value manufacturing, complex and inter-connected supply chains are increasingly at risk of cyber-attack and Advanced Persistent Threats (APT)s. Attacks are hugely damaging to the individual business and the economy, perhaps the greatest damage is in reputation therefore defining and communicating a Board Information Risk Management action plan becomes central to a organisations strategy. Within the United Kingdom it is reported that 81% of large organisations have experienced a security breach of some sort. The cost to each organisation has averaged between $ 650,000 and $ 1.8 Million, the consequences of possible data breeches and intellectual property theft are

imposable to calculate. The establishment of an effective business governance structure requires a holistic approach throughout the supply chain, many supply chains lack true maturity and compliancy. Therefore the responsibility of corporate risk management falls largely to the prime vendor within the supply chain this approach is unattainable as the supply chain extends requiring organisations to take reasonability for their own risk management regime.

An effective Cyber Risk Management Regime can be characterised in the following

- Establishment of holistic supply chain governance
- Determine a risk dash board to establish the supply chains risk culture, clear reporting of criminal incidents
- Maintain company board and management engagement with the cyber risk
- Develop standard operating procedures and work instructions operationally throughout the supply chain
- Establishment of Monitoring and continues assessment of procedures
- Incident Management – Development of incident response and disaster recovery capability

Within the approach of continues assessment an organisation needs to review that they have the correct skills to effectively manage the cyber risk. This will need to access a broad range of people both from a technical and leadership perspective. Mapping the supply chains risk culture and profile helps to determine the leadership approach. A deep understanding of likely hackers and their capabilities will not only determine the culture of the supply chain but also determine the level of security control required and investment to ensure the supply chain is resilient to attack.

Sector Requirements. There is need to verify the robustness of the cyber defense within the supply chain to ensure cyber threats are dealt with quickly and through an approach that will not hinder the chain, thus not impacting economic security. Through the work undertaken for this paper, there was a realization of risk management is not about just the migration of risk, it needs to be a set of multiple tools to intergraded than being a standalone process to stop risk being ignored within the supply chain. In terms of cyber supply chain resilience, risk assurance needs to be a driving mechanism for improvements within the cultural collaboration within a supply chain to strengthen and reinforce processors and policies before any threat can have a negative impact. Each time a threat penetrates a system, this has already had e negative impact. This can only be possible through improving the collaboration and implementation processes or suppliers in the chain. The major challenge is that there some information that businesses will not want to share with others working in the chain.

To overcome this barrier, the central prime – needs to create a downstream supply chain to gather data which can impact their output. Current approaches to improving cyber awareness and integration within the supply chain are analysed within this paper. These demonstrates that work is being done in the sector as well as nationally to educate about cyber, but further work is needed in terms of integration within the supply chain within the manufacturing sector. Without this, cyber risk assessment cannot be audited and improve countermeasures to improve supply chain resilience in the context on the UK. For this to be achieved this paper discusses the cybersecurity assurance processes that have been identified as core elements which impact assurance. These have resulted in the proposed framework which shall be outlined.

Conclusion and Future Work. The authors of this paper conclude that little emphasis is placed within a supply chain on cyber leadership and future organisational state. A primary need of an organisation is to drive high growth and implement an enterprise culture. Increase awareness of cyber risks through educational awareness programmers are inefficient and ineffective on their own, there needs to be rapid and direct action to implement what has been learnt. There is a need to effectively articulate the cyber –related business case in terms of return on investment and reputational uplift. Organisations that are safe to do business will be required to demonstrate across the supply chain a transparent set of cyber security performance metrics (The dashboard) Culture therefore becomes a critical factor in defining attitudes to risk, experience, aptitude and expertise and how these attributes are valued and prioritized within the

individual organisational capability and within the supply chain. Leadership is the determining factor in the establishment of a cyber-culture.

References

1. Cascio J. (2009). The next big thing: resilience. *Foreign Policy*, *172*, 92.
2. Darkreading [Electronic resource]. – Access mode: http://www.darkreading.com/vulnerabilities---threats/manufacturers-suffer-increase-in-cyberattacks/d/d-id/1325209.
3. National Institute of Standards and Technology. NISTIR 7298, revision 2, glossary of key information security terms (2013) [Electronic resource]. - Access mode: http://csrc.nist.gov/publications: National Institute of Standards and Technology Interagency or Internal Report 7298r2.
4. Nolan R. & Gibson C. (1974) Managing the Four Stages of EDP Growth*, Harvard Business Review*, 52/1 *(Jan-Feb),* 76-78
5. Nolan R. (1979). Managing the Crises in Data Processing, *Harvard Business Review*, *57/2 (Mar-Apr)*, 115-126
6. Exponentialtraining. com 'Greiner's Growth Model' [Electronic resource]. – Access mode: http://www.exponentialtraining.com/Downloads/Resources/Example%20Module%20-%20CBS/page_08.htm.
7. NCSC 'A New Approach for Cyber Security in the U'K (13 Sept 2016) [Electronic resource]. - Access mode : https://www.ncsc.gov.uk/news/new-approach-cyber-security-uk.
8. UK Manufacturing Statistics [Electronic resource]. – Access mode : http://www.themanufacturer.com/uk-manufacturing-statistics/.
9. Delotte [Electronic resource]. – Access mode: http://www.cyberintelligencecentre.com/news/global-cyber-executive-briefing/manufacturing.aspx
10. Sikich 2016 Manufacturing Report [Electronic resource]. – Access mode: http://files.clickdimensions.com/sikichcom-achbg/files/sikich_manufacturing_report_2016.pdf?_cldee=dGhlbWVobGluZ3NAZ21haWwuY29t
11. Qatalyst Global (2016) The State of Cyber Secirty in Critical Manufacturing Industries [Electronic resource]. – Access mode: http://www.qatalystglobal.com/the-state-of-cyber-security-in-critical-manufacturing-industries/.
12. National Cyber Security (2009) Research Development and Challenges: Related to Economics, Physical Infrastructure and Human Behavior.
13. Cyber Essentials 'Protect your business against cyber threats' [Electronic resource]. – Access mode: https://www.cyberaware.gov.uk/cyberessentials/.

Одержано редакцією: 28.04.2017
Прийнято до публікації: 10.05.2017

УДК 330.1

ЄФІМЕНКО Надія Анатоліївна,
доктор економічних наук, професор,
професор кафедри якості,
стандартизації та управління проектами,
Черкаський національний університет
імені Богдана Хмельницького,
м. Черкаси, Україна

ОЦІНКА ЕФЕКТИВНОСТІ ВИКОРИСТАННЯ РЕСУРСНОГО ПОТЕНЦІАЛУ ГАЛУЗЕЙ НАЦІОНАЛЬНОЇ ЕКОНОМІКИ

Розглянуто методичні підходи до оцінки формування та використання ресурсного потенціалу галузей національної економіки. За результатами дослідження з'ясовано, що оцінка ресурсного потенціалу проводиться за його складовими та комплексно, а також з використанням різноманітних методичних прийомів: індексного аналізу, розрахунку інтегрального показника, економіко-математичних методів, економіко-статистичних моделей тощо. Висвітлено цільовий та структурний методологічні напрями оцінки ресурсного потенціалу, з виділенням в останньому динамічного та ймовірного підходів дослідження.

Ключові слова: *ресурсний потенціал, галузі національної економіки, оцінка ресурсного потенціалу, методичні прийоми оцінки, ефективність використання ресурсів, мета та завдання оцінки.*