Indian Journal of Economics and Business (ISSN: 0972-5784)
Vol. 20 No.2 (December, 2021)
Copyright@ Ashwin Anokha Publications & Distributions
http://www.ashwinanokha.com/IJEB.php

The Role of Vendor Risk Management in Threat Landscape

Kalpana Singh
Department of Applied Sciences IIMT College of Polytechnic Greater Noida, India,

Sankalp Raghuvanshi
Precisely, Noida, India

**Corresponding Author*

Email addresses - Sankalpraghuvanshi35@gmail.com (Sankalp Raghuvanshi) , kalpanasankalp@gmail.com(Kalpana Singh).

Received date: 10th March 2021
Revised date: 2nd July 2021
Accepted date: 30th September 2021

Abstract: Nowadays cases involving threat landscape by vendors or third parties are occurring at a rapid rate. Most of the organizations are facing complex and tedious cyber-attacks. most cybercriminals are equipped with the best tools and skills, they are organized and have a good amount of funding from external sources than before. It is found that both organizations and vendors lack a comprehensive understanding of what information is considered to be a threat; therefore, more research is needed to define the role of Vendor risk management in Threat Landscape (VRM in TL). Recently the role of vendor risk management in threat landscape has developed into a most crucial and important topic of concern for cybersecurity experts. This paper aims to study the role of VRM in TL related work through the literature review process which involves a comparison of existing techniques, processes involved in establishing Vendor risk management programs and strategies for successful vendor relationship management. This paper also described the role of VRM in threat landscape challenges such as Malware threat, ransomware threat, Blue keep, IoT, and EOL. These Threats will have to be continually anticipated and managed through technology, continued action, and Vigilance, properly trained security personnel, combined with good Strategic practices. New opportunities for mitigation arise through automation, big data machine learning, and artificial intelligence. This research paper gives insights into the role of VRM in threat Landscape.

Keywords- Vendor risk management in threat Landscape, Malware threat, ransomware threat, Blue keep, IoT,EOL, big data machine learning and artificial intelligence.

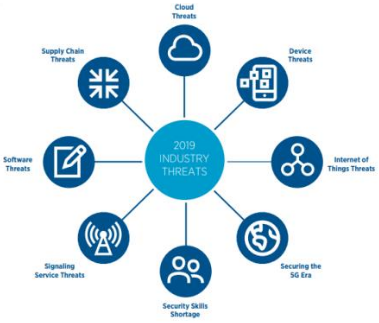


Fig 1. Industry Threat i2019 -21

1.0. Introduction

In today's times, most of the companies depend on third-party vendors for their different types of services. The vendors give different kinds of cloud-based software, operational support, and infrastructure on a day to day basis. The third-party vendors increase the overall efficiency thereby allows the companies to save a large amount of cost and hence achieve the growth. There have been some efforts done by vendors or third parties to address computer security and privacy risks with technologies in an Information and Communication Technology for Development (ICTD) environment, e.g., (Ben-David et al., 2011, Corrigan-Gibbs and Chen, 2014, Reaves et al., 2015),

Yet giving out data related to business to the vendors can be risky. A recent Cost of Data Breach Study conducted by the Ponemon 2018 reveals that breach in data done by third party sources can cost over $13 for every record that is lost or compromised. This reveals that data breaches done by vendor networks are much costlier as compared to the ones which occur by extensive consequences.

Implementation of vendor risk management programs will help the industry to protect their data from any harm and also avoid costly disruption to the overall functioning of the industry.

In today's time cyber threats can come up from everywhere, risk related to business is at an all-time high. Still, security teams are given the task to protect the important data and the assets are forced to perform and execute at a much faster rate than before [Antonio Robleset al. 2020]to protect against cyber thefts companies, have to increase the process of identifying unknown threats, make a fast decision, and finally reduce the risk. To amplify and increase the impact, most of the teams related to security have started to use a security intelligence philosophy with the help of which intelligence can be applied all over the organization and hence protect the organization from cyber-attacks [A.M. Elhady et al.,2013].

This will help the organization and industries to monitor manage and survey the potential risk which might result from third party suppliers, IT services, and products[V. *George et al2017].* It involves an overall brief plan for identifying and reducing the potential uncertainties to business which might lead to cyber-attacks or theft in an organization. The outsourcing of VRM has made it even more crucial and important for the organization. Most organizations lose their control of the workflow since they trust the workflows to the third party and hence are forced to trust the third party to do their work well.

There are multiple benefits of outsourcing like focus the core tasks, reduction in cost, promotion of growth, maintenance of operational control, flexibility to staff, provide continuity and management related to risk. But even with multiple benefits and advantages related to outsourcing, if there is a lack of strong protection and restriction from vendor's end there are chances that the organization can be exposed to risk related to reputations or even operational regulatory [R.Hu. et al., 2014].

Due to lack of academic literature discussing Vendor risk management and threat landscape, this paper will serve as a guide for researchers to better understand Vendor risk management by identifying the standard and protocol using in the selection of Vendor or third parties (Section 1)

Section 2 of this paper describes the methodology that being implement for this literature review. Section 3 describes various techniques used by organizations for effective VRM Section 4 presents and describes various processes covered by the research community. Section 5 describes the strategies for successful vendor relationship management.

Section 6 presents the available standard and framework that is used in vendor risk management and threat landscape. Section 7 identifies major challenges and future perspectives of VRM in the threat landscape. In conclusion, we provide a discussion and recommendation for future research in the field of vendor risk management in the threat landscape.

1.1. Advantages of vendor risk management- Setting up a strong vendor risk management procedure will allow organizations to accomplish the following advantages:

1.1.1 Helps to improve the vendor acquisition strategies—
Although NCUS has not completely removed the outsourcing as operational strategies of credit unions. it has given out some guidelines which define how to approach and evaluate the decision to outsource. A good VM program can reduce the total no of vendors required. in place of taking in three to four partners who are specialized in one area it is better to hire a single experienced and capable partner who can manage a variety of services single headedly and thereby reduce the potential risk involved with the operation of outsourcing. Decreasing the overall strength of the vendor also increases the overall efficiency which may result in cost-saving for the organization.
1.1.2. A well-developed vendor risk management program will reduce the overall risk. there is a risk that third-party vendors that handle sensitive and important data might expose the important data of industries and may lead to the risk of a breach, financial penalties, and damage to reputation.
1.1.3. Reduce the cost of operation – a HOC vendor risk management can be ineffective and even some times costly, but without the use of vendor risk management the overall cost related to data loss compliance fines, etc will increase, and hence it will be somewhat more expensive.
1.1.4. Understanding risk over time- A well-built vendor risk management program develops good metrics to compare scores related to risk between the vendors and hence provide simple, repeatable, and reliable metrics for checking the overall level of risk of the vendors. This can be useful not only during the initial selection of the vendor but also for renewal and contact recompetes. By getting to know about the risk score of vendors, it will become easier to award contracts to "low hassle" vendors. Theses "low hassle vendors" will have a good track record of internal control and mechanism of protection of data. [Macaulay et al., 2012]

2.0 RESEARCH METHODOLOGY
2.1. Search Strategy and Selection Criteria
In an attempt to better understand and bring more detailed acumen to the phenomenon of vendor risk management in threat landscape (VRM in TL). The collection of targeted literature reviews for analysis in this paper based on keyword searches. We performed information gathering on the definition, issue, and challenge to cyber threat intelligence. Figure 1, shows the outlines of our research approach. We started to review the literature from academic databases [5] such as the ACM Digital Library and IEEExplore. The main set of scientific papers was formed from the searches run on SCOPUS, ACM, Web of Science, and IEEE Explore, as recommended in Kitchen ham and Brereton[B. Kitchenham et al 2013]. We also identified literature by searching databases such as Google scholar, research gate, using search terms such as "Vendor risk management ", "threat Landscape"," Prevention", "Challenges and its future perspective. We followed-up citations and references in this literature to extend the number of relevant sources. We searched for articles in peer-reviewed journals, books and grey literature (documents issued by government agencies e: g; federal, state, or corporate consultancies, non-governmental agencies, and private organizations) [Md Sahrom Abu et al 2018]
2.2. Data Analysis -Role of Vendor risk management and threat landscape are a new topic, so reports from CERTS, software vulnerabilities, and open data sharing platforms were also searched for authentic information. The methodical review conducted using narrative synthesis by summing up, comparing, and contradicting the data for literature review since 2012.
2.3. Inclusion and Exclusion Criteria - The keyword search process created a remarkable number of results. To guarantee that only appropriate sources were incorporated for the survey, articles found by the search procedure were estimated against a few standards. Each source needed to meet at least one or more of the requirements. First, the source directly addresses at least one specific aspect of vendor risk

management in the threat landscape. Second, the source is not directly related to vendor risk management but defines one or all. These requirements are utilized to achieve the paper's aim of providing a concise introduction to the immediate challenges and issues facing by Vendors or third parties.

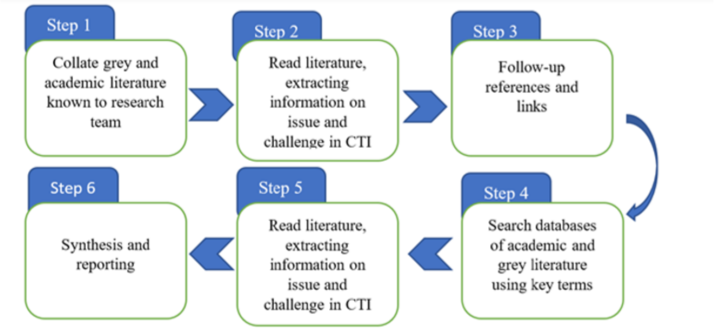
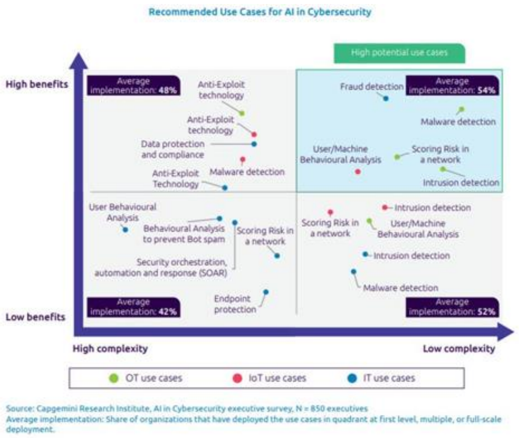

Step 1
Collate grey and academic literature known to research team
Step 2
Read literature, extracting information on issue and challenge in CTI
Step 3
Follow-up references and links
Step 4
Search databases of academic and grey literature using key terms
Step 5
Read literature, extracting information on issue and challenge in CTI
Step 6
Synthesis and reporting

Figure 2. Research Approach Overview **Techniques**

3.0Techniques: To assess current threat landscape, the technique such as real-time intelligence enables to exactly evaluate the vendor risk management — both current and historic, which is caused by each third party, and keep these evaluation up-to-date as conditions change and new threats emerge.

3.1. Sorting the data via machine learning and Automation

This technology helps to manage the risk of the parent company or own organization as well as the third party or vendor companies from the open web, the dark web, technical and new sources, and discussion forums. To productively manage the dangers for the organization, we need to evaluate a large amount of data related to the threat from the dark web, technical and news sources, open web, and discussion forum. The same can be applied to evaluating the risk related to third parties. But this will equate to data points worth of billions [Maria T. Vullo, 2017] This would create problems for security teams while analyzing the risk data. Hence an intelligent machine is very important for creating objectives for third party entities to prioritize the threats by evaluating and collecting third-party risk data.


Recommended Use Cases for AI in Cybersecurity

Source: Capgemini Research Institute, AI in Cybersecurity executive survey, N = 850 executives
Average implementation: Share of organizations that have deployed the use cases in quadrant at first level, multiple, or full-scale deployment.

Figure 3: OT and IOT use cases have higher rate of adoption

3. 2. Threat Landscape Index (TLI)

It was designed to bring an ongoing barometer for total malevolent activity across the internet. In general, TLI is based on the assumption that the involvement of third parties creating a big risk and a wide variety of threats that have been detected by TLI based sensors. *[Kure, H.et al 2018] [Figure 4]*

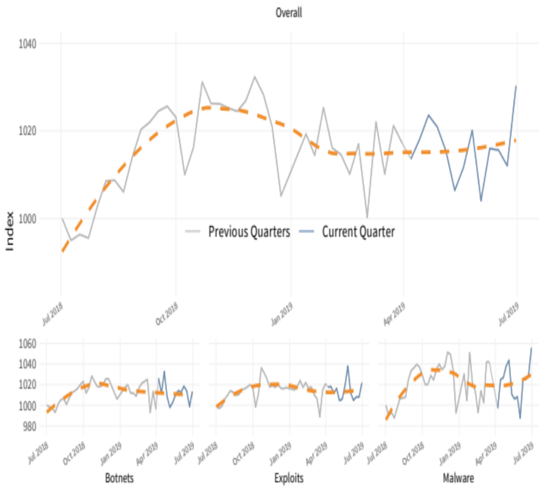


Figure 4: Fortinet Threat Landscape Index (top) and sub-indices for botnets, exploits, and malware (bottom).

3.3. Use of Bigdata to access Vendor risk management

Collection of data such as financial reports from third parties can help, improve, and evaluate the risk assessment by using Big data techniques is gradually become very popular. Third-Party Risk Intelligence (TPRI) solutions utilize data science and algorithms to reveal uncover hidden patterns and anomalies to enhance data significance, attribution, and risk measurements. Some solutions leverage advanced data science techniques for risk analysis, such as data clustering, data externalization technologies and other forms of artificial intelligence (AI) [YouceFlmine et al,2020].Such techniques track the external network traffic of an organization and the dark web chatter to determine attributes such as patching cadence, device security posture, and vulnerability indicators [Claire O'Malley et al .,2017] . The following capabilities represent the cyber risk scoring market to vendors or third parties (Figure 5)

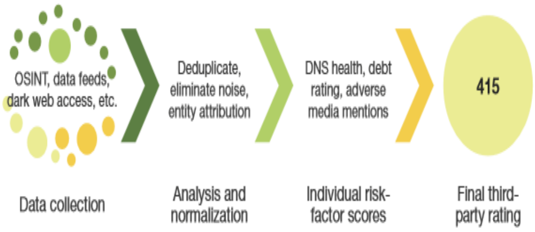
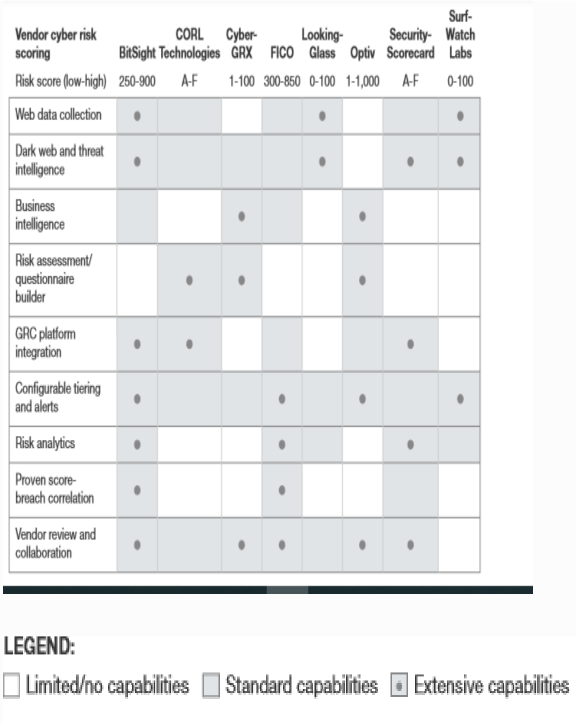

OSINT, data feeds, dark web access, etc.
Deduplicate, eliminate noise, entity attribution
DNS health, debt rating, adverse media mentions
415
Data collection
Analysis and normalization
Individual risk-factor scores
Final third-party rating

FIGURE 5: Common Vendor Risk Management Data Collection Process



Vendor cyber risk scoring	BitSight	CORL Technologies	Cyber-GRX	FICO	Looking-Glass	Optiv	Security-Scorecard	Surf-Watch Labs
Risk score (low-high)	250-900	A-F	1-100	300-850	0-100	1-1,000	A-F	0-100
Web data collection	●	▨	□	▨	●	□	▨	●
Dark web and threat intelligence	●	▨	▨	▨	●	□	●	●
Business intelligence	▨	□	●	▨	□	●	□	□
Risk assessment/ questionnaire builder	□	●	●	□	□	●	□	□
GRC platform integration	●	●	□	▨	□	▨	●	□
Configurable tiering and alerts	●	▨	▨	●	▨	●	▨	●
Risk analytics	●	□	□	●	▨	□	●	▨
Proven score-breach correlation	●	□	□	●	□	□	▨	□
Vendor review and collaboration	●	▨	●	●	▨	●	●	□

LEGEND:
□ Limited/no capabilities ▨ Standard capabilities ● Extensive capabilities

Figure6:Vendor or Third-Party Cyber Risk Scoring Solution Comparison

3.4. Artificial Intelligence

The biggest advantage for AI is the improvement in the level of threat detection (69%), followed by an expansion in the containment of infected endpoints/devices and hosts (64%). Since AI reduces the time needed to respond to cyberattacks companies will potentially save more than $2.5 million in operational costs on average. AI will increasingly become a core part of the strategies of many financial companies to Enhance customer service, improve serviceeffectiveness and organizational performance So they get a strategic advantage.A recent Deloitte survey of over 3,000 C-Suite Executives partnership with the European Financial Management Association (EFMA), [Tom Bighamet al 2017] reveals that Activities and functions which companies believe AI could have the greatest impact on threat detection. [Figure 7]

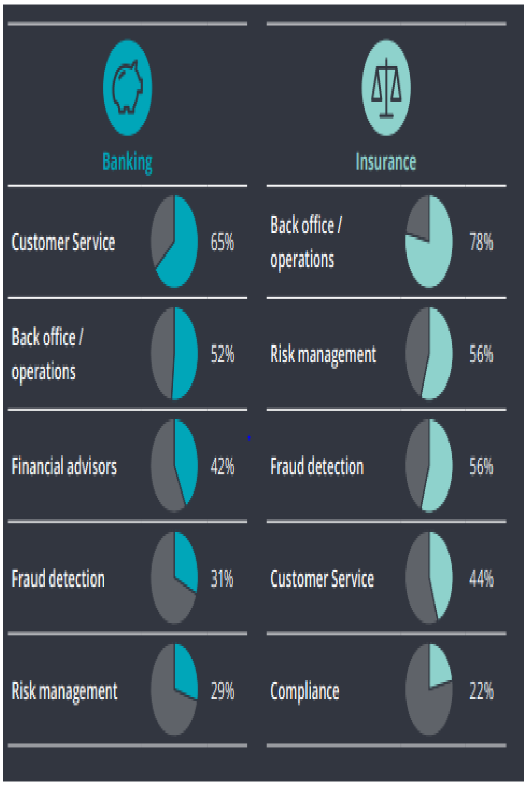


Figure 7: Impact of Artificial Intelligence in Vendor risk management crisis

4.0. Processes involved in Establishing vendor risk management Program

4.1. Generic third-party risk management process model

Many organizations finally go to great lengths to handle their third-party such as suppliers, vendors, and business partners risk, usually through a proper management process such as the generic model [Bryan Cline, Nov 2016] While the actual implementation of VRM differs from one organization to another, they will typically address each step of the process in some way. Step 1: INITIATE Step 2: COLLECT Step 3: QUALIFY Step 4: ACCEPT Step 5: SELECT Step 6: MONITOR

4.2. Vendor risk management Process

4.2.1. Development of policy, procedure, and program –

It is one of the most crucial parts of vendor risk management. for the success of the vendor risk management program, a well-documented policy, procedures must be maintained properly.

4.2.2. Must have a well-defined and thorough vendor selection process

For the successful relationship between organization and vendor is important to form a defined vendor vetting process. Some of the points which must be considered are- Issue of request for proposal (RFP), Comparison of the given vendor with the competition, and completion of assessment related to risk and other requirements.

4.2.3. Establishment of contractual standards –

Before establishing any sort of contractual standards and finalizing a contract draft there should be a lot of understanding as well as a lot of talking between both the parties.

4.2.4. Vendor risk management audit process must be defined internally—

Internal audit means surveying and checking the overall risk management in the organization so that all the risks can be caught and fixed well in time before an examiner arrives on site. [C. Sillaber et al 2016]

4.3.5. Access to comprehensive, detailed, and robust reporting-

Many times, it is seen that reporting to senior management and board via excel spreadsheets is very difficult. Establish vendor risk management provides an option to access and check the customizable reports. These reports are quite easy to check and present in front of the executive's management teams as well as boards.

5.0. Vendor relationship management-

To analyse vendor risk management, we need to have a good vendor relationship management. When evaluating a vendor, it's crucial to recognize how the vendor will adjust to the overall context of the organization's goals and projects.

5.1. Strategies for successful vendor relationship management

5.1.1. Communicate often

Most of the business fails due to poor communication, hence it is one of the most important aspects of poor communication, the incapacity to send or receive important and crucial information from the supplier's end can result in shaking the base of vendor management process [IsmailGölgeci et al.2020]. To transmit the requirements and get a much better understanding of the capabilities of the suppliers, corporate buyers are required to communicate with the vendors regularly.

5.1.2. Build partnerships-

By moving out of a transactional relationship and shifting to strategic relationships between buyer and seller, one can have better and efficient vendor management [Cristin Quintana et al. 2020] the first and foremost rule is to treat your suppliers as an important partner.

This will not only increase their trust but also provide other benefits like preferential treatment and many more [Youce fImine et al 2020]

5.1.3. Creating a Win-Win situation-

Chasing short term cost savings will prove to be disadvantageous for the industries in long run and hence create a considerable amount of impact on the quality [Sankalp Raghuvanshi et al.2020] So, in place of forcing the suppliers to cut down his cost, it will be better to study the business of the vendor.Rather than resorting to strong-arm tactics, it is better to negotiate based on good faith and values.

6.0Challenges and Future perspectives of Vendor Risk Management

6.1. Strategic Sourcing: A 2014 Deloitte global survey [Deoitte.,2014] was expected to challenge organizations on outsourcing as a business model by growing costs, increased regulation, and concerns regarding cyber fraud, data security, and privacy [L. Beard et al,2013]. Challenges are expected to increase in retained company hiring and handling suppliers and contractors, which in turn are expected to improve creativity, soft skills and generate greater market value

6.2. The Effect of emerging technologies

The rapid development of new technologies would trigger more regulatory attention and increase the effect of Risks on third parties. Gartner,2015, predicts the adoption of hybrid cloud technologies will dominate 2015. These will escalate the status of cloud-related technology providers from third parties to a critical level, a shift that will bring significant risks. Essential Concerns surrounding the security, privacy, and resilience of cloud data and applications will remain – with significantly Improved ramifications of any breach or security incident [Figure8]. Data ownership and privacy continue to be key Concerns, alongside, as well as lack of clarity as to who exactly is the data owner and who is the data processor under different privacy? Legal issues will include confusion about legal jurisdiction, which will get blurred and compliance with the contract is going to get even more complicated [P. Hinton et al., 2011], [J. Armour et al.,2010].

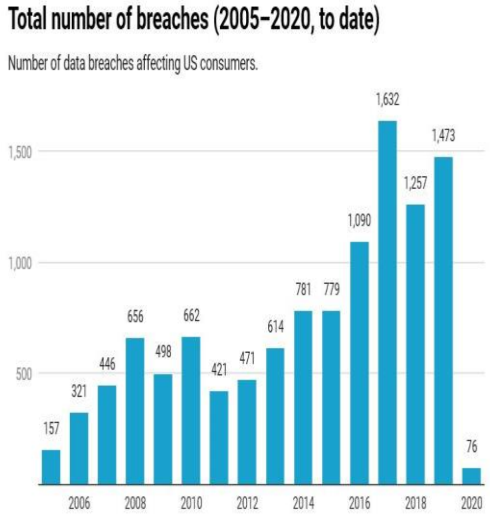
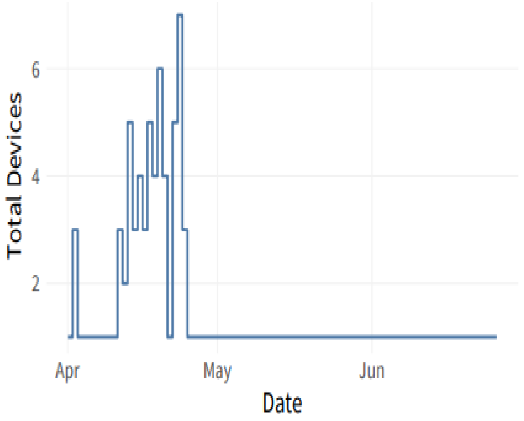


Figure8: Total number of data breaches affecting US consumers from 2005 -2020

6.3. The Ransomware Threat: A large number of high-profile incidents occurred during the last year highlight the growing impact of ransomware attacks for organizations and third-party vendors that are not prepared to deal with them. Due Ransomware attack disrupted critical services for weeks and forced officials to execute manual workarounds for tackling real estate transactions, property taxes, utility payments, and other critical functions in the city of Baltimore [N. Kossovsky, 2012]. Another Ransomware attack has been seen in Florida where cybercriminals disrupted critical services. It uses several evasion tactics as well as destroying its encryption key and deleting shadow copies on an infected system. and finally settled by paying $490,000 to cybercriminals to avoid disruption[Lena Y et al 2019]. Such payments as prone to just encourage more ransomware assaults sooner rather than later in the future even though companies without proper data backup and recovery processes might consider it as the only reasonable option.e.g. WannaCry ransomware.



.Figure 9: Devices detecting Ryuk variants

6.4.The malware's Threat: The malware's attack includes the ability to paralyze Windows services which prevent data encryption and cut off from shared drives.Malware spread independently from one vulnerable system to another disrupted critical services of the organizations. [Cristina Quintana et al 2020] [Figure 10]

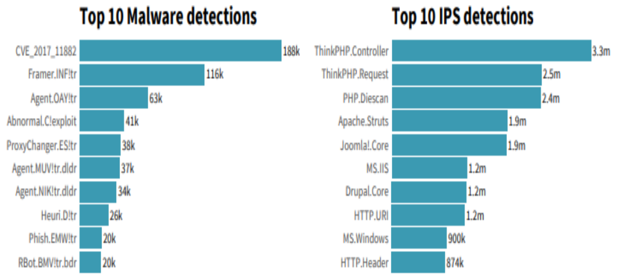


Figure 10: Most common malware variants and IPS detections by device in Q2 2019.

6.5. Blue Keep -Microsoft has portrayed Blue Keep as being "worm able". It is a critical defect in the Remote Desktop Services work in various more seasoned forms of Windows. The defect (CVE-2019-0708) permits an unauthenticated client to associate with a helpless framework using Microsoft's exclusive Remote Desktop Protocol (RDP) and assume responsibility for it to take accreditations and information and for planting ransomware and other malware. [Elahi, 2013] Microsoft alerted the organizations about the Blue Keep and the role of third parties because the IPs belonged to third-party customers and outsider clients and not the organization itself. [Figure 9]

6.6. Impact of COVID-19:

Crisis on Vendor Risk Management: A study by the Institute for Supply Management (ISM) reveals that nearly 75% of all supply chains are experiencing interferences brought about by the Covid-19 outbreak. This phenomenon anticipates escalating, as several nations are seriously influenced by the Covid-19 infection. Under this scenario, the strength of the organization's operational exercises is set at the cutting edge and putting organizations in a difficult circumstance by the dependency on Vendor or third-party organizations. Along these lines, the COVID-19 emergency has focused on the significance of business coherence designs. Effective VRM is intended to provide clear instructions to limit the negative impact on the company [Jessica Boyd,2020]. Vendor or Third-party crisis management starts before the crisis with the pre-crisis phase, followed by the crisis management phase, and ending with a post-crisis phase. [Figure 11]

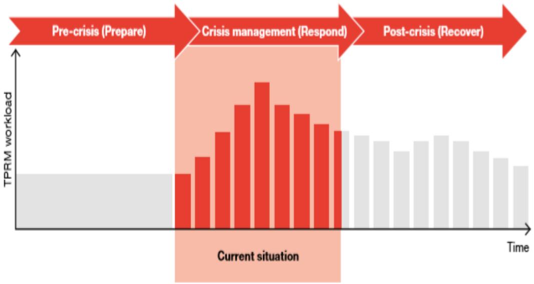


Figure 11: Navigating through the Covid-19 crisis with VRM crisis

6.7. Use of IoT and EOL: IoT devices and services will be developed and deployed with security from third parties. If an IoT device with a dependency on cloud-based security signatures and threat intelligence from a third party is launch in the market and the third party or vendor terminates operations or blends or simply redesigns an interface, at that point the IoT device may no longer approach the knowledge they have to keep up a worthy security posture. [Leila Alinaghian et al., 2020] Given that numerous IoT devices and services won't be promptly upgradeable and the danger of being stranded by inheritance security partners and third party or vendor companies are significant., for example, Cisco, HP, and Intel: all have suspended or sold off significant security items in the last few years. Typically, these items will be upheld for up to three or in some cases even five years under the terms of End of Life (EOL) guarantees to clients. In any case, if an IoT device has an amortization (EOL) time of 10 years or more, the risk is that IoT service providers to wait out to complete the EOL (End of Life) period before going to major security updates. The number of IoT devices being added to botnets increased in 2019 and a change in attack vectors to target enterprise IoT devices has been identified Shodan is a search engine for Internet-connected devices and it reports a 15,000 growth of insecure MQTT devices in 2019.

A simple example of this is the sale of the IBM laptop business to a Chinese company named Lenovo. Almost immediately, many organizations stopped procuring the Lenovo laptops for corporate use, although they appeared and functioned indistinguishably but with a branding. The IoT's flexibility and durability challenge is that supply chain products –though available on the same terms as before – are unusable due to ownership. The ownership at issue raises concerns about danger agents like state-sponsored or corporate surveillance or sabotage. Most organizations rely heavily on third-party vendors for services to save costs.

Conclusion –

The role of vendor risk management in the threat landscape has become a major challenge as it is still in the early stages and it requires research and development needs to make full use of its potential. This paper examines the literature available which discusses the role of VRM and threat landscape in the current scenario. While outsourcing has great benefits, as businesses increase their use of outsourcing, risk management by VRM and third parties are becoming an increasingly important part of any business risk management system. Organizations entrust third parties with more of their business processes, so they can focus on what they do best. This means that they will ensure the protection of information security, data security, and cybersecurity by third parties. In this article, we covered the best ways to identify operational regulatory, financial, and reputational risk when vendors lack strong, security controls and how to prevent and mitigate those risks. It is important to look at this as future research. The authors anticipate the concerns that these issues may hold the potential in contributing to future research studies.

Conflicts of Interest: The authors declare no conflict of interest.

References:

1. Abel Yeboah-Ofori and Shareeful Islam [*] Cyber Security Threat Modelling for Supply Chain Organizational Environments, *Future Internet* **2019**, *11*(3), 63; **https://doi.org/10.3390/fi11030063**

2. A.M. Elhady,A.AbouElfetouh,H.M.El-bakryetal.,"Generic Software risk management framework for SCADA system," International Journal of Computer Applications, vol. 70, no. 3, pp.45–52,2013.
3. Antonio Robles-González,Javier Parra-Arnau,Jordi Forn ''A LINDDUN-Based framework for privacy threat analysis on identification and authentication processes'' Computers & Security, Volume 94, July 2020,101755 https://doi.org/10.1016/j.cose.2020.101755

4. Armour, J., Mayer, C., & Polo, A. (2010). Regulatory sanctions and reputational damage in financial markets. Available at: http:// papers.ssrn.com/sol3/ papers.cfm?abstract_ id=1678028; accessed on 6 May 2015. Oxford University Centre for Corporate Reputation:

5. Bryan Cline, October 2019 ,HITRUST Third-Party Risk Management (TPRM) Methodology:
6. Bryan Cline, Ph.D., Chief **Research** Officer. The Qualification Process, HITRUST **Third-Party Risk Management Methodology**.

7. B. Kitchenhamand Brereton," A systematic review of systematic review process research in software engineering," Information and Software Technology, vol.55,no.12,pp.2049– 2075,2013

8. B. Reaves, N. Scaife, A. Bates, P. Traynor, K.R.B. Butler**Mo(bile) money, Mo(bile) problems: analysis of branchless banking applications in the developing world**
9. USENIX Security (2015) [Google Scholar] [CrossRef]

10. Beard, L. and York, M. (2013), Strategic Sourcing: The Future Is Now, In Analyst Insight Aberdeen Group, Boston, MA

11. Claire O'Malley and Nick Hayes October 20, 2017, Vendor Landscape: Third-Party Risk Intelligence Products Vie To Augment Your Survey-Based Program by Forrester Research,

12. Cristina Quintana, García CarlosG. Benavides-ChicónMacarenaMarchante-LaraDoes a green supply chain improve corporate reputation? Empirical evidence from European manufacturing sectors.9 January 2020

13. CAPGEMINI RESEARCH INSTITUTE, REINVENTING CYBERSECURITY WITH ARTIFICIAL INTELLIGENCE - THE NEW FRONTIER IN DIGITAL SECURITY (28 PP., PDF, NO OPT-IN)

14. Deloitte. (2014). Global Outsourcing and Insourcing Survey Results. Available at http:// www2.deloitte.com/ content/dam/Deloitte/ us/Documents/strategy/ us-sdt-2014-globaloutsourcingInsourcingsurvey_051914.pdf; accessed on 6 May 2015
15. *Deloitte, 2017 "Third-party Governance and Risk Management,". (https://www2.deloitte.com/uk/en/pages/ risk/articles/third-party-risk.html).*
16. ErezMetula,,Defending against MCRs(chapter9), Hooking into Runtime Environments ,2011, Pages 261-290

17. Ernst & Young Global Limited. Cyber Threat Intelligence - How To Get Ahead Of Cybercrime. Insights on Goverance, Risk and Compliance. 2014. 27. Watkins K-F. M-Trends 2017: A view from the front lines. Vol. 4, Premier Outlook. 2017.
18. Elahi, E. (2013). Risk management: the next source of competitive advantage. Foresight, 15(2), 117-131
19. Generic Third-Party Risk Management Process Model Bryan Cline,Nov[https://hitrustalliance.net/content/uploads/TPRM-Methodology.pdf]

20. Gartner, Top 10 Strategic Technology Trends for 2015. Available at: http:// www.gartner.com/ technology/research/top10-technology-trends; accessed on 6 May 2015
21. *George V. Hulme, "Equifax Rated 'F' in Application Security Before Breach," Security Boulevard, September 11, 2017 (https://securityboulevard.com/2017/09/equifax-rated-f-application-security-breach/).*

22. Hinton, P., & Patton, R. (2011). Trends in Regulatory Enforcement in UK Financial Markets. NERA Economic Consulting, London
23. H. Corrigan-Gibbs, J. Chen Flash patch: spreading software updates over flash drives in under-connected regions

24. Hu. R. Dou. W,, & Liu, J. (2014) '' Challenges in 5G: how to empower SON with big data for enabling 5G . IEEE Network. 26(6). 27–33. SLR_79

25. IsmailGölgeci,OlliKuivalainenDoes social capital matter for supply chain resilience? The role of absorptive capacity and marketing-supply chain management alignment, Volume 84, January 2020, Pages 63-74https://doi.org/10.1016/j.indmarman.2019.05.006

26. John Pirc ,David DeSanto, Iain Davison ,Will Gragido ,Leveraging Big Data for Predictive Analysis 2016, Pages 17-27 chapter(2) Threat Forecasting

27. *Jeanne Whalen, "McKesson to Pay $150 Million for Failing to Report 'Suspicious' Drug Orders," The Wall Street Journal, January 17, 2017 (https://www.wsj.com/articles/mckesson-to-pay-150-million-for-failing-to-reportsuspicious-drug-orders-1484699478).*

28. Jessica Boyd, COVID-19 Survey: Impacts On Global Supply Chains,*MARCH 11, 2020*

29. Kossovsky, N. (2012). Reputation, Stock Price, and You: Why the Market Rewards Some Companies and Punishes Others. Apress

30. Kaur Sahi Asst S. A Study of WannaCry Ransomware Attack. Int J Eng Res Comput Sci Eng. 2017;4(9):7–9.

31. *Kure, H.I.; Islam, S.; Razzaque, M.A. An Integrated Cyber Security Risk Management Approach for a Cyber-Physical System. Appl. Sci. 2018, 8, 898. [CrossRef]*

32. .Leeflang. P. S. Verhoef. P. C. Dahlstrom. P. &Freundt T. (2014). Challenges and solutions for marketing: in a diaital era. European Management Journal.

33. LenaY. ConnollyDavidS.Wall "The rise of crypto-ransomware in a changing cybercrime landscape: Taxonomizing countermeasures ,Computers & Security Volume 87, November 2019, 101568 ,https://doi.org/10.1016/j.cose.2019.101568

34. LeilaAlinaghian 'YusoonKimJagjitSrai **A relational embeddedness perspective on dynamic capabilities: A grounded investigation of buyer-supplier routines** ,Industrial Marketing Management,Volume 85, February 2020, Pages 110-125 https://doi.org/10.1016/j.indmarman.2019.10.003Get rights and content

35. Md Sahrom Abu, Siti RahayuSelamat, AswamiAriffin,,Robiah Yusof , Cyber Threat Intelligence – Issue and Challenges Indonesian Journal of Electrical Engineering and Computer Science Vol. 10, No. 1, April 2018, pp. 371~379 ISSN: 2502-4752, DOI: 10.11591

36. Maria T. Vullo, "23 NYCRR 500: Cybersecurity Requirements for Financial Services Companies," New York State Department Of Financial Services, March 1, 2017 (http://www.dfs.ny.gov/legal/regulations/adoptions/dfsrf500txt. pdf).

37. Sillaber C, Sauerwein C, Mussmann A, Breu R. Data Quality Challenges and Future Research Directions in Threat Intelligence Sharing Practice. Proc 2016 ACM Work Inf Shar Collab Secure. 2016;65–70.

38. Sankalp Raghuvanshi, Kalpana Singh, 2020, Light Fidelity: The Future of Data Communication, INTERNATIONAL JOURNAL OF ENGINEERING RESEARCH & TECHNOLOGY (IJERT) Volume 09, Issue 05 (May 2020),

39. T.MacaulayandB.L.Singer,CybersecurityforIndustrialControl Systems,CRCPress,BocaRaton,Fla,USA,2012.
40. Tom Bigham,Suchitra Nair ,Sulabh Soral ,Alan Tua ,Valeria Gallo ,Michelle
41. ''AI and risk management Innovating with confidence'' *Deloitte, 2017*
42. UthayasankarSivarajahMuhammad MustafaKamalZahirIraniVishanthWeerakkody.Critical analysis of Big Data challenges and analytical methods Journalof Business Research(Elesveir),Volume 70, January 2017, Pages 263-286
43. WEBROOT, KNOWLEDGE GAPS: AI AND MACHINE LEARNING IN CYBERSECURITY PERSPECTIVES FROM THE U.S. AND JAPANESE IT PROFESSIONALS (PDF, 9 PP., NO OPT-IN)

44. Wallace, M. Mitigating Cyber Risks in IT Supply Chain; The Global Business Law Review; 2016. Cleveland-Marshal College of Law. Library. Cleveland State University. Available online: https: //engagedscholarship.csuohio.edu/gblr/vol6/iss1/2 (accessed on 10 September 2018).

45. Y. BenDavid, S. Hasan, J. Pal, M. Vallentin, S. Panjwani, P. Gutheim, J. Chen, E.A. Brewer **Computing security in the developing world: a case for multidisciplinary research**

46. NSDR '11, ACM, New York, NY, USA (2011), pp. 39-44[**Google Scholar**] [**CrossRef**]

47. YoucefImine, Ahmed Lounis, Abdelmadjid Bouabdallah ''An accountable privacy-preserving scheme for public information sharing systems '' **Computers & Security**Volume 93, June 2020, 101786,https://doi.org/10.1016/j.cose.2020.101786
48.Mathiassen, L., Saarinen, T., Tuunanen, T., & Rossi, M. (2007). A contingency model for requirements development. Journal of the Association for Information Systems, 8(11), 569-597.