Aggregate Analysis of Security Surveys

Bindu Dodiya
Institute of Computer Science
Vikram University Ujjain

Umesh Kumar Singh, PhD
Institute of Computer Science
Vikram University Ujjain

Vivaan Gupta
Suncity Institute
Gurgaon, Haryana

ABSTRACT
IT environment is becoming more complex, cybercriminals are getting better at identifying and targeting the intrinsic weaknesses. In 2020 criminals have taken advantage of the disruption caused by the pandemic. While organizations were vulnerable and distracted, hackers developed new ransomware samples and advanced existing tools to attack critical infrastructure including vital research labs and health care organizations. In this regard analysis of emerging vulnerability, attack trends can be helpful in planning proper counter measures to ensure security. There are various surveys and reports available which provide statistical information on security trend and issues and also studies are available which provides information about defence mechanism and tools to protect an organization .Better understanding of Current information and security trends and issues can be gained by doing comparative and aggregate analysis of these reports. In order to have a holistic picture of current state of information security landscape, In this paper data from NVD, and seven other sources which conducted survey in last two years has been analysed .Results are obtained by analysing recent survey reports to present a comprehensive view of current information security landscape.

Keywords
Security survey, Vulnerability trends, Attack trends, Security countermeasures.

1. INTRODUCTION
In the era of the Internet of Things (IoT), where digitally connected devices are encroaching on every aspect of lives, including homes, offices, cars and even our bodies. With the advent of IPv6 and the wide deployment of Wi-Fi networks, IoT is growing at a dangerously fast pace. Interconnected IT systems are beneficial to an organization because of their functionality, connectivity and accessibility, but also they are susceptible to attacks from both outsiders and internal users. Furthermore, in recent years, there is huge diffusion of new technologies .Communication networks are used to transfer increasingly sensitive information that can be valuable and confidential, requiring protection against misuse. Moreover, attackers have evolved from computer enthusiasts to professional hackers. However, the attacks made by the cyber criminals are getting smarter and they use new methods and technology for successful attacks. They often find the security holes and breaches in the secured system and steal information or damage the system in less time .[1] Hacking community created freely available hacking tools and hence attackers changed from using worms and viruses to more sophisticated attacks. This has resulted in information security threats like identity theft, Phishing/Vishing/Smishing/Pharming, social engineering etc. Simple attacks have matured to become sophisticated, automatic, subtle and very hard to detect. With rise in scale and complexity of security incidents, It is very clear that IT infrastructures are vulnerable and attackers are always ready to exploit these vulnerabilities. Therefore, It requires innovative ideas and insightful analysis of security issues to appropriately respond to the challenges posed by technological development. Security is often viewed as an arms race between attackers, who try to exploit vulnerabilities and security administrators, who try to protect system against these attacks. It is therefore desirable to know emerging trends in security in order to be able to think about countermeasures before these emerging trends become large-scale problems. Despite several studies aimed at providing much needed statistical information on security trends and issues, there is still need to find one that is complete and reliable. Skybox, CSI/FBI, Flexera, Microsoft, Verizon and IBM are some well known names that had been gathering statistics and trends on information security for many years and produce surveys on yearly basis. A good understanding of the current information security trends and issues can be gained by using results of these surveys. To develop a good understanding of current state of information security landscape, this paper made an analysis of the six well known information security surveys conducted in year 2020: skybox research report [4], flexera vulnerability review report 2020[5], Microsoft Security Intelligence report [6], CSI/FBI Internet Crime Complaint Center (IC3) Report[7], Verizon Data Breach Investigations Report 2020[8],IBM X-Force Threat Intelligence Index 2021[9]. Further, results are presented by aggregating and analyzing these survey reports to present a complete and comprehensive picture of current information security landscape. Objective is to identify need of proactive security solutions in current information security landscape.

The organization of the paper is as follows. Section 2 discusses security trends in terms of vulnerability trends, attack trends and preferred security countermeasures, based on statistics and trends analyzed from selected set of surveys. Section 3 presents discussion derived from this analysis. Finally, conclusion is presented in section 4.

2. SECURITY TRENDS
"Global Village" became a Reality ,Internet has made real what in the 1970's that visionary of the communications Marshall McLuhan (1911-1980) called the "Global Village". One of the most significant changes over the past few decades has been the rise of information technology and security as important, integral parts of everyday activities and communication. For example, there are 5,168 million worldwide Internet users till march 2021 which is 65.6% of world population [12].Networking has evolved from dedicated point to point connections to ubiquitous communication between people, platforms and applications . The Covid-19 pandemic has caused massive disruptions in how individuals and enterprise operates on a day-to-day basis. At a time when remote work has become essential, the cloud has also become a reliable platform in keeping business operations functioning despite lockdowns and travel restrictions. Indeed, reliance on cloud computing has

skyrocketed in 2020 and the dependency on this technology is bound to continue. In fact, a recent Forrester report predicts that the use of cloud-native technology will increase, stating that in 2021 alone, the global public cloud infrastructure will grow 35%[13] .Increased use of Internet, intranets and other open systems also increases potential security risks in the networked information system environment. Vulnerabilities are the major contributor to the risks that people and organizations face when working in such kind of open environment connected to Internet. Vulnerabilities are the major attack vector that opens the door for unauthorized system access and compromise. Cybercriminals and attackers use refined methods to identify and exploit vulnerable systems connected to the Internet in an automated fashion and on a large scale. Thus, proper mitigation of vulnerabilities is necessary in order to ensure the security. In current scenario, one of the big concerns for security administrator is the identification and remediation of vulnerabilities in the networked information system environment. Recent security trends are presented in this section, to justify the rising need of proactive security solutions that can help security administrator in vulnerability mitigation in optimal manner.

2.1 Vulnerability Trends

One may think that over time, security is getting better and systems are less vulnerable, but this is not always true as it has been witnessed by increasing number of vulnerabilities and attacks in past few years that vulnerabilities are increasing year by year. Fig.1 presents vulnerability statistics of last fifteen years, collected from most popular and genuine vulnerability data source: National Vulnerability Database (NVD) [2] .NVD is U.S. government repository of standards based vulnerability management data. NVD currently contains 159435 CVE vulnerabilities. CVE (Common Vulnerabilities and Exposures) [3], is a dictionary of publicly known information security vulnerabilities and exposures. CVE has become a de facto industry standard used to uniquely identify vulnerabilities which is widely accepted in security industry. In the year by year view of vulnerabilities, it is clear that vulnerability is increasing every year there was a 128% increase from year 2016 to 2017.Number of vulnerabilities reported in year 2016 was 6447 and in year 2017 was 14714.Vulnerabilities are increasing every year. Total 19249 Vulnerabilities reported in year 2020. The ramp up in vulnerabilities between 2016 and 2017 can be seen as a continuation of an upward trend that began years earlier .This increasing number raise need for an intelligent and more automated approach to remediation.

Besides vulnerability counts, it is also important to investigate the evolution and distribution of important vulnerability aspects, such as the criticality, the impact, the attack vector and availability of patches[16] .The Common Vulnerability Scoring System (CVSS) [14] provides a way to capture the principal characteristics of a vulnerability, and produce a numerical score reflecting its severity, as well as a textual representation of that score. The numerical score can then be translated into a qualitative representation such as low, medium, high, and critical to help organizations properly assess and prioritize their vulnerability management processes. Fig.2 presents Total CVE distribution by their CVSS V3 score. Out of total processed 76319 vulnerabilities only 15 % vulnerabilities are of low severity 44% vulnerabilities are of medium severity, 39 % of vulnerabilities are of high severity and 2 % of vulnerabilities are of critical severity. severity spread for new vulnerabilities reported in the first six months of 2020 is very similar to 2019's figures [4]. Although organizations generally focus on vulnerabilities with high and critical severity this can allow attackers to take advantage of any exposed vulnerabilities with medium severity. Criminals know that medium severity flaws can remain unpatched within an organization's systems for a long period. Depending on existence of flaws, attacker can gain access to a critical asset or enable lateral movement. Although CVSS scores are useful for understanding the properties of vulnerability in isolation, they are created without contextual understanding of an individual organization's security environment. This is context that needs to be focused in the way that security programs are run, security teams need to understand which of their vulnerabilities are unprotected by security controls.[4]

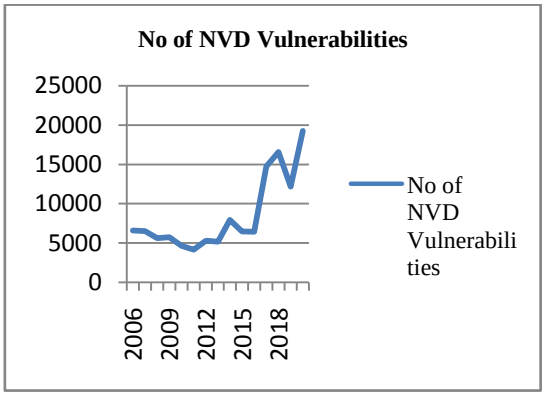

Fig1.Vulnerability Statistics

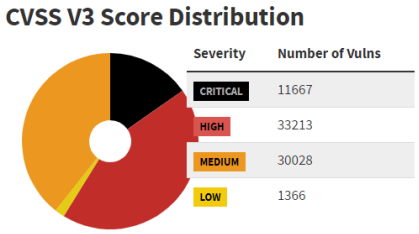

Fig 2.CVSS score distribution

Table2 shows list of the top 10 vulnerabilities exploited in 2020. Which belongs to Path Traversal, Execute Code, Improper Input Validation, OS Command Injection, Improper Authorization, Improper Input Validation and SQL Injection CWE Categories. It is notable that Only two of these vulnerabilities were actually disclosed in 2020. Threat actors were more likely to exploit a vulnerability from 2019 or earlier, probably based on the difficulty associated with exploiting many of the vulnerabilities revealed in 2020 and the difficulty in patching older vulnerabilities that many organizations encounter[9]. OWASP stands for the Open Web Application Security Project[10], an online community that produces articles, methodologies, documentation, tools, and technologies in the field of web application security, provides the list of the 10 most common application vulnerabilities as OWASP top 10. It also shows their risks, impacts, and countermeasures. Updated every three to four years, the latest OWASP vulnerabilities list was released in 2018.which are Injection, Broken Authentication, Sensitive Data Exposure, XML External Entities (XXE),Broken Access control, Security misconfigurations, Cross Site Scripting (XSS),Insecure Deserialization, Using Components with known vulnerabilities, Insufficient logging and monitoring. The Attack vector metric of CVSS 3.0 reflects the context by which vulnerability exploitation is possible. This metric value

(and consequently the Base Score) will be larger the more remote (logically, and physically) an attacker can be in order to exploit the vulnerable component. The assumption is that the number of potential attackers for a vulnerability that could be exploited from across a network is larger than the number of potential attackers that could exploit a vulnerability requiring physical access to a device, and therefore warrants a greater Base Score. Possible values for this metric are Network,Adjacent,Local and physical.[14] Value Network depicts that the vulnerable component is bound to the network stack and the set of possible attackers extends beyond the other options for the metric, up to and including the entire Internet. Such a vulnerability is often termed as "remotely exploitable" .It can be thought of as an attack being exploitable at the protocol level one or more network hops away (e.g., across one or more routers). An example of a network attack is an attacker causing a denial of service (DoS) by sending a specially crafted TCP packet across a wide area network [14]. It has been observed that Attack vector value for all top 10 vulnerabilities is Network ,depicts that all top 10 vulnerabilities are "remotely exploitable .Further With a 60.55 percent share, the primary attack vector used to trigger a vulnerability for all products in 2019 was via remote network There is a slight increase of 5.25 percent since 2018, via local network is 30.59% and via local system is 8.86% .The fact that over half of all vulnerabilities could be exploited remotely, it is an element of concern for the security of systems. The proportion of vulnerabilities with attack vector "local network" has decreased, from 32.94 percent in 2018, to 30.59 percent in 2019. Local system decreased by 1.09 percent (to 8.86 percent of all vulnerabilities) in 2019.[5]These clearly indicates that a system in a Network is more vulnerable. At the same time, the number of vulnerabilities whose publish date was more than a full year after its ID year increased by two orders of magnitude from 54 to 2825 between the first halves of 2016 and 2017, then settled down to just over 1000 in 2018 H1, and continued along that trajectory with 377 in 2019 H1. These facts taken together suggest that there was substantial catching up in processing older vulnerabilities beginning in 2017. Higher vulnerability counts can further complicate an organization's prioritization and remediation processes. To deal with the inevitable increase of vulnerability occurrences within an organization, There is need to establish processes to contextualize vulnerabilities based on exposure, exploitability and other factors to keep remediation focused on critical risks.[4]

Table.1 Top 10 Vulnerabilities exploited in 2020

CVE ID	Description	CWE Name	Publication date
CVE-2019-19781	Citrix Application Delivery Controller	Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	12/27/2019
CVE-2018-20062	None CMS Think PHP Remote Code Execution	Execute Code	2018-12-11
CVE-2006-1547	Action Form in Apache Software Foundation (SAF) Struts	Other	03/30/2006
CVE-2012-0391	Exception Delegator component in Apache Struts	Improper Input Validation	01/08/2012
CVE-2014-6271	GNU Bash Command Injection	Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	09/24/2014
CVE-2019-0708	"Bluekeep" Microsoft Remote Desktop Services Remote Code Execution	Use After Free	05/16/2019
CVE-2020-8515	Draytek Vigor Command Injection	Improper Neutralization of Special Elements in Output Used by a Downstream Component ('Injection')	02/01/2020
CVE-2018-13382, and CVE-2018-13379	Improper Authorization and Path Traversal in Fortinet Forti OS	Improper Authorization	06/04/2019
CVE-2018-11776	Apache Struts Remote Code Execution	Improper Input Validation	08/22/2018
CVE-2020-5722	HTTP: Grandstream UCM6200 SQL Injection	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	03/23/2020

The Common Weakness Enumeration (CWE) identified the Top 25 Most Dangerous Software Errors and their score. To create the 2020 list, the CWE Team leveraged Common Vulnerabilities and Exposures (CVE) data as well as the CVSS scores associated with each CVE. A formula has been applied to the data to score each weakness based on prevalence and severity . Fig .3 shows top 12 CWE with score more than 10 from top 25 list of CWE. The major

difference between the 2019 and 2020 CWE Top 25 lists is the increased transition to more specific weaknesses as opposed to abstract class-level weaknesses. While these class-level weaknesses still exist in the list, they have moved down in the ranking. The biggest movement up the list involves four weaknesses that are related to Authentication and Authorization.[6] Due to COVID-19, pandemic Enterprises are now more dependent on the VPN for Work-from-Home Model, where employees can connect as a VPN client to the corporate infrastructure and access internal network services. However, the major threats and attacks have been massively introduced in this pandemic period only. The real fact is that VPN clients can't always be "trusted," due to which organization is affected by a large number of data breaches around the globe. As the VPN ports are always open for Clients, it has been exploited by hackers and attackers easily with various attacks.

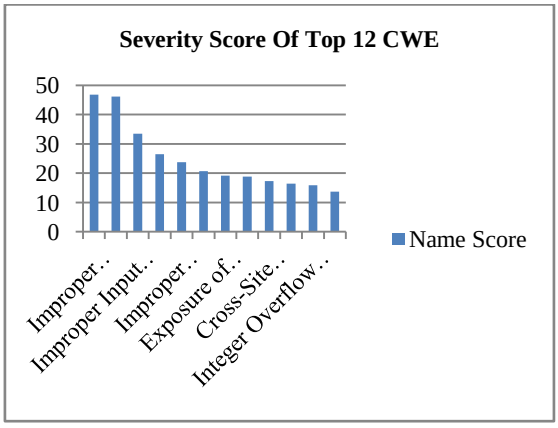

Fig.3 Top12 CWE with score more than 10

2.2 Attack trends

A greater understanding of risk can be gained by identification of attacks exploiting the vulnerabilities and frequency of these attacks. Understanding the attack landscape can assist security teams in prioritizing resources, drilling for the most likely scenarios, and identifying shifts in attacker techniques. Keeping this point in mind recent attack trends are presented in this section. In 2020 criminals have taken advantage of the disruption caused by the pandemic . A time that has also seen a significant increase in exploits taking advantage of Remote Desktop Protocol (RDP). Credential theft, social attacks (i.e., phishing and business email compromise), and errors cause more than 67% breaches in 2020 .Personal data was involved in 58% of breaches, nearly twice the percentage in last year's data. This includes email addresses, names, phone numbers, physical addresses and other types of data that one might find hiding in an email or stored in a misconfigured database. [8] In 2020, attackers focused more of their effort on developing Linux crypto-miners and ransomware, likely due to more organizations transitioning their servers to the cloud and the expandable processing power that cloud environments provide. The creation of new ransomware and malware samples has soared during the COVID–19 crisis, ransomware continued its surge to become the number one threat type, representing 23% of security events in 2020. Ransomware attackers increased the pressure to extort payment by combining data encryption with threats to leak the data on public sites. Threat actors carried out ransomware attacks predominantly by gaining access to victim environments via remote desktop protocol, credential theft, or phishing. Ransomware actors are finding greater success in attacks by expanding their attack chain ,59% of ransomware attacks used a double extortion strategy. Since organizations can opt to recover from backups and not pay the ransom, attackers have shifted tactics to not only encrypt data and render it impossible to access. They also stole it, and then threatened to leak sensitive data if a ransom was not paid. Certain ransomware providers even held auctions on the dark web to sell their victims' stolen sensitive information. The top two ransomware types observed in 2020 included Sodinokibi which caused 22% of all ransomware incidents and Nefilim which cause 11% of all ransomware incidents .Both Sodinokibi and Nefilim blend data theft with ransomware attacks. Sodinokibi ransom revenue was $123 million in 2020. Ransomware attacks were the most common threat to Operational technology. Ransomware attacks made up 33% of all attacks on OT in 2020. [4] Ransomware attacks are often described in terms of their payload. However, it has been observed that multiple ransomware payloads being deployed by cybercriminals using the same infrastructure for concurrent campaigns. The selection of which payload and tools used was largely dependent on the terrain the cybercriminals landed in, choices were based on which security tools were present, whether the network had good cybersecurity basics in place, and which data the cybercriminals wanted to infiltrate from the network. Payloads can also be varied by cybercriminals to avoid attribution. If a certain ransomware has been reported in the news and there's heightened awareness of it, switching to a different payload can reduce the pressure on cyber criminals and their concern about the possibility of getting disrupted. In April 2020, It is observed by Microsoft that a prolific ransomware criminal responsible for more than 100 major incidents suddenly switch to using the infamous WannaCrypt payload at the end of their typical attack pattern, after attacking hospitals and healthcare organizations during the COVID-19 crisis.RDP Brute force is most common entrance point for human operated ramsomware. Over 70% of human-operated ransomware attacks in 2020 originated with Remote Desktop Protocol (RDP) brute force.[6]

The Internet Crime Complaint Centre (IC3),[7] provides the American public with a trustworthy source for information on cyber criminal activity, and a way for the public to report directly to IC3 when they suspect they are a victim of cyber crime. IC3 received a recorded 7,91,790 complaints in 2020 ,with reported losses exceeding $4.1 billion. This represents a 69% increase in total complaints from 2019 .IC3 also asks respondents about type of attacks they have experienced ,this part of survey is very helpful in understanding current attack landscape. It is depicted in fig.4. The most prevalent crime type reported in 2020 were Phishing/Vishing/Smishing/Pharming, Non-Payment/Non-Delivery, Extortion, Personal Data Breach. The top three crime types with the highest reported losses were BEC/EAC, Confidence fraud , Investment. It is also important to have a note of financial losses incurred due to these attacks experienced by the organisations , In 2020 Financial losses Reported by IC3 is $4.2Billion which is 31%. more than 2019. and highest loss of $1,866,642,107 reported for BEC/EAC attacks.These complaints address a wide array of internet scams affecting victims across the globe. Fig.5 shows financial losses for last three years for 12 types of attacks for which maximum loss were experienced in 2020 .

In 2020 maximum loss occurred was $1,86,66,42,107 due to BEC/EAC Attacks. Which shows 5% increase from 2019.For Financial Losses occurred due to Ransomware attacks reported by IC3 cost were $29,157,407. This number does not include estimates of lost business, time, wages, files, or

equipment, or any third-party remediation services acquired by a victim. In some cases, victims do not report any loss amount to the FBI, thereby creating an artificially low overall ransom ware loss rate. Total loss by ransomware may be much more . Every day, Gmail blocks more than 100 million phishing emails. In April 2020, Google blocked 18 million daily malware and phishing emails related to Coronavirus.[12] new attack kill chains were also seen that combine to deliver more sophisticated kill chains.

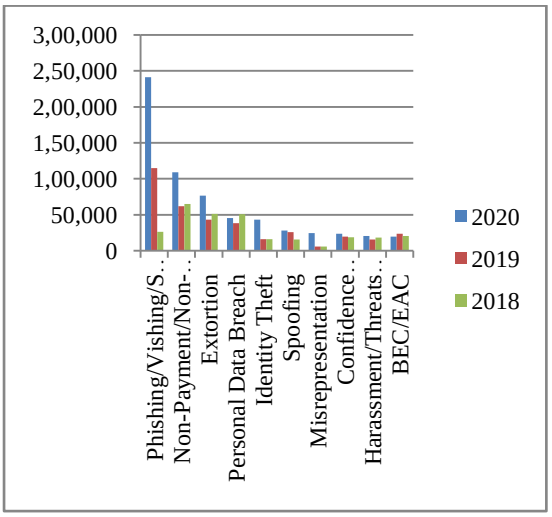

Fig.3 IC3 Most prevalent crime types

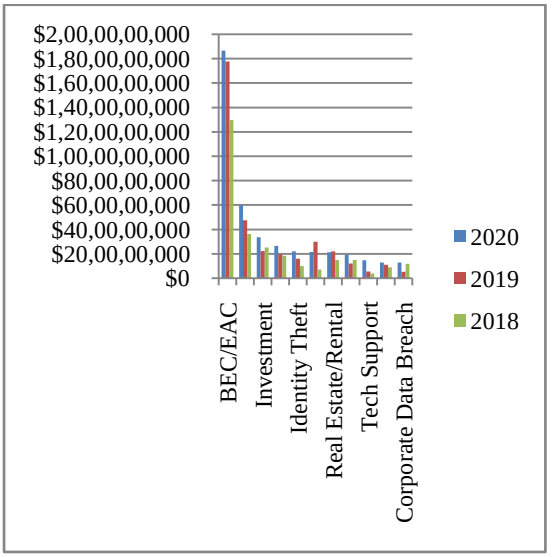

Fig 4.Financial losses for last 3 years.

2.3 State Of security Countermeasures

This section Presents current scenario of security countermeasures taken by organizations which are Reported In CRAE Index [15].The cyber security Resource Allocation and Efficacy (CRAE) Index is a quarterly Tracer of momentum in cybersecurity investment and sentiment about the impact of cyberscurity programs .CRAE index for second quarter of 2020 shows that organizations are emphasized proactive security measures to protect assets and detect breaches .The index also showed that security professionals who took proactive measures were significantly more satisfied with the impact of their efforts than those who did not. The CRAE Index provides report for the overall focus and direction of organizations' cybersecurity activities, spending, and perceived progress over time. It comprises two composite indices Resource/Spending and Efficacy .The first index resource allocation/spending used to monitor the state of organizations' allocations and spending on cybersecurity activities .The second index efficacy monitors organization's perceptions about the efficacy of these measures. Fig 5 shows data for two composite indices Resource/Spending and Efficacy for Q2-2020 to Q1-2021 It is clear that efforts has been increased more than spending . According to one survey from the Ponemon Institute, 60% of breaches in 2019 involved unpatched vulnerabilities. Although More than 80 percent of vulnerabilities have patches available on the day of disclosure. In short, patch management is a continuous process of identifying, prioritizing, remediating, and reporting on security vulnerabilities in systems. This is particularly important if an organization has a need to burn down a backlog of vulnerable systems. This confirms businesses must maintain continuous visibility of software assets and the vulnerabilities affecting them, and have optimized processes to ensure critical issues are addressed before exploitation risk increases. Zero-day vulnerabilities those exploited prior to public disclosure remain rare. This highlights the fact there is time to remediate most vulnerabilities before exploitation risk increases.

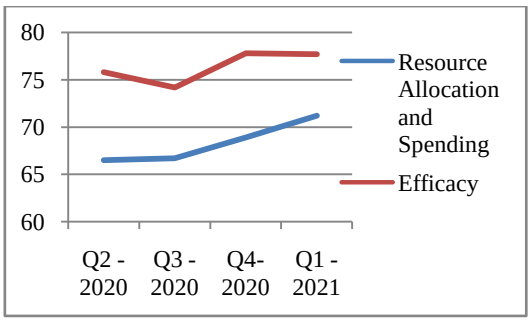

Fig.5 CRAE Index, All Regions (Q2-2020 to Q1-2021)

3. DISCUSSION

Key Findings from the analysis of six well established security surveys published in 2019 and 2020 are mentioned in this section. Vulnerabilities are increasing every year , there was a 128% increase from year 2016 to 2017.Number of vulnerabilities reported in year 2016 was 6447 and in year 2017 was 14714. The ramp–up in vulnerabilities between 2016 and 2017 can be seen in this context as a continuation of an upward trend that began years earlier .In 2020 ,Out of total processed 76319 vulnerabilities 44% vulnerabilities are of medium severity .organizations generally focus on vulnerabilities with high and critical severity this can allow attackers to take advantage of any exposed vulnerabilities with medium severity. When a High severity vulnerability is reported, security teams are likely to focus their energies on it more while neglecting medium severity vulnerabilities for longer periods of time. However, the severity scale only determines the possible impacts of a single vulnerability in isolation. It does not include the risk or exposure an organization faces due to a vulnerability. Therefore, it is possible that a neglected medium severity vulnerability is a bigger risk for an organization, compared to a high severity vulnerability. Due to this factor of neglect, attackers are more attracted towards medium severity vulnerabilities. Hence, incorporating the factors of risk and exposure in vulnerability management become necessary. Fig 6 shows vulnerabilities of last to years by their severity .Further Over half of all vulnerabilities could be exploited remotely, it is an element of concern for the security of systems. The proportion of vulnerabilities with attack vector "local network" has

decreased. I has been observed that The 2020 CWE Top 25 list shows increased transition to more specific weaknesses as opposed to abstract class-level weaknesses

Attacks on Health care organizations and Pharmaceutical industries has also been increased in year 2020. As the healthcare sector continues to offer life-critical services while working to improve treatment and patient care with new technologies, criminals and cyber threat actors look to exploit the vulnerabilities that are coupled with these changes . The Report of Top 10 industries by attack volume, 2020 vs. 2019 shows that Healthcare jumped from last place in 2019 to seventh place in 2020, probably driven by COVID-related healthcare attacks and a barrage of ransomware attacks against hospitals. There were nearly 600 healthcare data breaches in 2020, a 55% jump from 2019, a new report shows. Not only did the number of data breaches spike in the past year, but the average cost per breach increased by about 10%. [9] The healthcare industry is plagued by a myriad of cybersecurity-related issues. These issues range from malware that compromises the integrity of systems and privacy of patients, to distributed denial of service (DDoS) attacks that disrupt facilities' ability to provide patient care. Ransomware has become a popular form of attack in recent years growing 350% in 2018 and representing 23% of security events in 2020. It is hard to ignore the recent increase in reporting of hospitals victimized by ransomware. Ransomware has become such an issue that the MS-ISAC, along with National Health Information Sharing and Analysis Center (NH-ISAC) and Financial Services Information Sharing and Analysis Center (FS-ISAC), teamed up to host trainings on how to defend against it. When Ransomware occurs in the healthcare industry, critical processes are slowed or become completely inoperable. Hospitals are then forced to go back to utilizing pen and paper, slowing the medical process and ultimately soaking up funds that may otherwise have been allocated to the modernization of the hospital. [7]

Organizations are emphasizing on being proactive about defence when dealing with incidents than they have been in past years. Focusing on sheer number of vulnerabilities is not enough, but knowing what to patch is even more important. As, approximately, 80% reduction in risk can be achieved by patching most critical programs. Challenge is to identify and patch right vulnerabilities..[4]

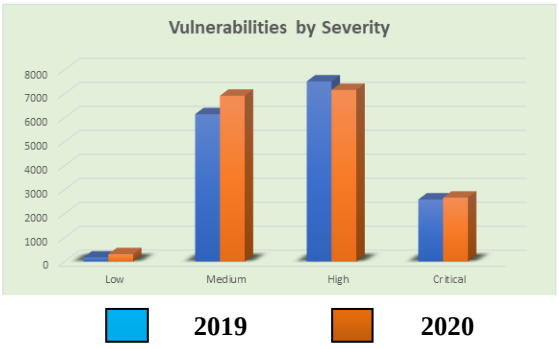

Fig 6.Vulnerabilities by severity

4. CONCLUSION

comprehensive picture of the current state of information security landscape is presented based on study of security surveys from well known and established sources like skybox, flexera, Microsoft ,CSI/FBI Internet Crime Complaint Center (IC3) ,Verizon,IBM . Further, need of preventive security technologies also identified. Recent trends indicate that number of Internet users, vulnerabilities and attacks that exploit these vulnerabilities are increasing year by year. Moreover, targeted attacks and sophistication of attacks are also increasing. This recommends that vulnerabilities as being the root cause of security incidents are required to be mitigated to control increasing number of attacks. Further, trends show that organizations are now focusing more on deploying proactive security technologies. Vulnerability/patch management is prominently used security technology but, satisfaction level with vulnerability/patch management solutions is not good, hence, need to be improved.

5. REFERENCES

[1] Chowdhury A. "Recent cyber security attacks and their mitigation approaches–An Overview". In International conference on applications and techniques in information security, Springer, Singapore. 2016; pp 54-65.

[2] National Vulnerability Database (NVD), [Online] Available: http://nvd.nist.gov/scap.cfm (Accessed on 05-03-2021).

[3] The MITRE Corporation. "Common Vulnerabilities and Exposures (CVE)," [Online] Available: http://www.cve.mitre.org/, (Accessed on 27-05-2021).

[4] Sky box research report "Vulnerability and threat trends 2020" [Online] Available :https://www.skyboxsecurity.com/blog/2020-vulnerability-and-threat-trends-report-mid-year-update-key-findings/(Accessed on 25-06-2021).

[5] Flexera "Vulnerability Review 2020 Global trends" [Online] Available: https://info.flexera.com/SVM-REPORT-Vulnerability-Review-2020. (Accessed on 25-06-2021).

[6] Microsoft Digital Defense Report,September 2020, [Online] Available: https://www.microsoft.com/enin/security/business/security-intelligence-report. (Accessed on 25-06-2021).

[7] FBI IC3 "Internet Crime Report 2020", [Online] Available: https://www.ic3.gov/Media/PDF/AnnualReport/2020_IC3Report.pdf. (Accessed on 25-06-2021).

[8] Verizon 2020 Data Breach Investigations Report, [Online] Available :https://enterprise.verizon.com/content/verizonenterprise/us/en/index/resources/reports/2020-data-breach-investigations-report.pdf, (Accessed on 25-05-2021).

[9] IBM X-Force Threat Intelligence Index 2021,[Online] Available: https://www.ibm.com/security/data-breach/threat-intelligence. (Accessed on 25-05-2021).

[10] https://owasp.org/www-project-top-ten/

[11] https://cwe.mitre.org/top25/archive/2020/2020_cwe_top25.html.

[12] Internet world Stats ,"Usage And Population statistics" [Online] Available: https://www.internetworldstats.com/stats.htm.

[13] Trend Micro Cloud App Security Threat Report 2020[Online] Available: https://www.trendmicro.com/vinfo/in/security/research-and-analysis/threat-reports/roundup/trend-micro-cloud-app-security-threat-report-2020.(Accessed on 10-06-2021)

[14] Common Vulnerability Scoring System v3.0: Specification Document (Qualitative Severity Rating Scale)". First.org (accessed on 10-07-2021).

[15] Cybersecurity Resource Allocation & Efficiency Index Q2-2020 Report [Online] Available: https://www.cyberriskalliance.com/wp-content/uploads/2020/08/CRAE-Index.pdf

[16] A. Tripathi and U.K. Singh," Aggregate Analysis of Security Surveys in Quest of Current Information Security Landscape" International Journal of Computer Applications • Volume 51– No.17, August 2012