Journal of Information Systems Engineering and Management
2025, 10(18s)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

Cybersecurity for Entrepreneurs: Opportunities, Challenges and Threats

Ashwini Brahme[1], Sagar Kulkarni[2], Nishant Pachpor[3], Ashwini Chavan[4], Smita Chavan[5], Shivaji Mundhe[6]
[1]*Associate Professor, International Institute of Management Science (IIMS), Pune, India,*
[2]*. Mumbai University*
[3]*Assistant Professor, International Institute of Management Science (IIMS), Pune, India,*
[4]*Assistant Professor, Institute of Management and Entrepreneur Development, Pune, India*
[5]*Assistant Professor, Suryadatta Institute of Business Management and Technology, Pune, India*
[6]*Director, International Institute of Management Science (IIMS), Pune, India,*

ARTICLE INFO

Received: 18 Dec 2024

Revised: 28 Jan 2025

Accepted: 12 Feb 2025

ABSTRACT

Introduction: In today's Internet era Cyber security is challenging task for all the organizations over the globe. Organizations of all types and sizes—ranging from small start-ups and large corporations including healthcare providers, financial institutions, educational organizations, production, non-profit, etc. must evaluate their cyber security mechanism to safeguard against data breaches, financial losses, and reputational harms. All organizations must understand cyber threats, recognize the importance of cybersecurity, and develop effective strategies and measures to counter them. The research is projected on cybercrimes, need of cyber security and role of cyber security in Entrepreneurship

Objectives.

- To study the emerging cybersecurity threats in Entrepreneurship.
- To explore challenges, threats and opportunities for Entrepreneurs.
- To offer guidelines on safeguarding businesses against cyber-attacks and data breaches.
- To design cyber security model for Entrepreneurs.

Methods: The present study elaborated on emerging technological advancement and need of cybersecurity, opportunities and challenges. The present study is confined towards the various types of cyber-attacks on small businesses, start-ups, impact of cyber-attacks on entrepreneur's and the consequences occurred by them.

Results: A researcher has proposed cyber security model for Entrepreneurs to resolve the cyber security problems and run organizations in safe cyber environment. Also, fostering cyber security culture in organization, emerging cybersecurity trends and legal implications are discussed.

Conclusions: An effective internet usage model, significance of cyber insurance and sustainability of Entrepreneurs in the digital era is recommended. The future of cybersecurity is ever-evolving and unpredictable. Individuals who can foresee trends, develop new skills, and adopt emerging technologies will be uniquely equipped to drive and shape the industry's direction

Keywords: Cybersecurity, cyber threat, Cybercrime, cyber-attack, Internet fraud, Entrepreneurs, small business, start-up, cybersecurity model, internet usage model.

INTRODUCTION

Now a days organizations become prime targets for cybercriminals looking to exploit vulnerabilities through data breaches. The increasing reliance on global connectivity and cloud services, such as Amazon Web Services, has amplified both inherent and residual risks. Organizations can no longer depend solely on traditional security measures like firewalls and antivirus software. Cybercriminals are continuously advancing their tactics, making it

essential to implement a comprehensive cybersecurity strategy that addresses all aspects of digital security. Threats can originate from any level within an organization, making cybersecurity awareness training a critical component of risk mitigation. Employees should be educated on common cyber threats, including social engineering, phishing, ransomware (such as WannaCry), and other malicious software designed to compromise sensitive data.

The increasing dependence on digital technologies has greatly amplified cybersecurity risks, and entrepreneurial firms are not exempt from these challenges. As entrepreneurs harness the digital ecosystem, they handle important and ample sensitive data, which is ultimately becoming cyber-attack target in today's internet era. The 2017 global ransomware attack, impacted on 2, 00,000 companies including small medium and large scales businesses which highlights on urgent need to prioritize cybersecurity in entrepreneurship to mitigate the potentially devastating consequences of such threats. [1] Entrepreneurs must prioritize cybersecurity to safeguard their businesses from cyber-attacks and data breaches. Keeping customer's data, financial data, achieving confidentiality, integrity and availability of business data is very challenging task for executing the business in the competitive world. With every click, transaction, and data exchange, new vulnerabilities emerge. The stakes have never been higher, as cybercrime has surged by an astonishing 600% since 2020.

By the year 2025, the financial impact of cybercrimes on companies worldwide is projected to reach an astonishing $10.5 trillion, highlighting the growing threats posed by cyberattack and data breaches in an increasingly digitalized and interconnected global economy. [10]. Small businesses face a range of cybersecurity challenges. The various cyber-attacks faced by the small business are data breach, malware, DoS, Ransomware, phishing, etc. Tailored cybersecurity solutions, such as employee training, network security measures, data encryption, and cost-effective tools, provide small businesses with a strong defence against cyber threats without incurring significant expenses. [16]. Raising awareness about cybercrime, cyber threats, and significance of cyber security culture is essential for all citizens, organizations, and businesses. Entrepreneurs and organizations must also employ skilled professionals to comprehend, combat to avoid becoming victims of these threats. [11][12] Entrepreneurs less concern about the cyber security as compared to the big organizations. Therefore, attackers take privilege of the same due to less security mechanism in small business.

REVIEW OF LITERATURE

From a global perspective, entering the Cybersecurity industry demands innovative approaches to combating cyber threats. To enhance security measures and to defeat an evolving cyber threats, cybersecurity companies have collectively secured funding exceeding $21 billion. Recognizing this potential, an increasing number of entrepreneurs are leveraging such funding opportunities to establish start-ups with ease. However, over three million Cybersecurity opportunities remain untapped due to the talent gap between client expectations and the services currently provided. New entrepreneurs can capitalize on this gap by adopting advanced technologies to address active cyber threats effectively. [3] The researcher has designed conceptual framework focuses on cybersecurity entrepreneurial ecosystem. There are various technological advancement in for cybersecurity entrepreneurship such as AI and Machine learning, block chain, internet of things and security, cloud security, quantum computing m, cryptography, etc. [3]

Cyber security is becoming challenging day by day to individual, organizations, businesses, and nation as well as worldwide. It has examined an increasing trust on technology and digital devices has made it essential to maintain the security of systems, applications, unauthorized access, access controls, protection of important documents and data, data storage and confidentiality. Due to the increasing cyber-attacks the organizations are strongly needed the data security and protection mechanism of sensitive and important data. The study also highlights on need of cyber security in diverse domains and areas. The technological advancement also aimed towards the cyber security in various domain. [4]

The future of cybersecurity embodies a dynamic blend of challenges and opportunities, requiring constant adaptation and innovation. The key areas are AI, ML, IOT, Cloud computing, quantum computing, edge computing, cybersecurity professionals, cybersecurity regulations. There are various opportunities for cybersecurity professionals like developing expertise in emerging areas to become a expert, entrepreneurship which can contribute for innovative ways of cybersecurity solutions and services, leadership to develop and implement cybersecurity strategies and polices. [5]

An article entitled Vincenzo Iozzo entitled “Top 5 Entrepreneurial Opportunities in Cybersecurity Today" discuses on Measuring Risk and Solving the “Market for Lemons” Challenge, Data Analysis, Accessibility, and Curation, Exploring Opportunities at the Crossroads of Cybersecurity and Crypto currency, addressing the Continuous Education Gap, Simplifying the Technology Stack to Manage Complexity. These points serve as essential pillars for entrepreneurial success in the cybersecurity space. [6]

The research paper titled “Recent Trends in Cybersecurity: A Review” focuses on the latest advancements in the cybersecurity field. It provides a thorough survey of key methods and algorithms for tackling security challenges, exploring their associated issues and highlighting recent technological innovations. The study has emphasized on polynomial-based encryption, which shows great promise for the development of next-generation security algorithms. [7]

A study has observed that Cybersecurity has become a top priority for organizations worldwide, given the substantial financial and reputational impact of data breaches. As technology enhances business operations, the growing complexity of cyber threats presents significant challenges. To navigate these risks effectively, organizations need strong cybersecurity partners who go beyond issue resolution to proactively prevent potential threats. Moreover, it plays a vital role in preventing disruptions that could impair system functionality and operations [33]. Social media platforms are commonly used by everyone as social networking sites, providing 24/7 digital access. While these platforms contribute to the sustainability of entrepreneurs, their use also increases the risk of cyberattacks. [35]

Research Gap: The literature review conducted in the domain of cybercrime, cyber-attacks, and its impact on small businesses highlights that small businesses and entrepreneurs are particularly vulnerable to cyber threats. While existing research explores methods to counter cyber-attacks, there remains a gap in developing practical cybersecurity strategies tailored specifically for entrepreneurs. This gap can be recovered by proposing cybersecurity guidelines, models, and preventive measures that entrepreneurs can adopt to safeguard their businesses in the cyber space.

STATEMENT OF THE PROBLEM

The basic need for any organization, business and entrepreneurs, start- up to have their business and work model on internet so that it will be available 24 by 7 to anyone and people can avail the same from anywhere. As the role of internet play significant task there are chances of cyber-attacks and cybercrime in the cyber space. There is need of cyber security for business to be safe in the internet word, to have data protection, to run the business securely [12].

In an increasingly digital world, cybersecurity has become a critical concern for entrepreneurs. Small and medium scale businesses are often targeted by cybercriminals due to their perceived lack of robust security measures. The present study focused on opportunities, challenges, and threats associated with cybersecurity for entrepreneurs, providing insights into how they can protect their businesses and capitalize on cybersecurity advancements.Therefore researcher has made an attempt to study the research entitled “Cybersecurity for Entrepreneurs: Opportunities, Challenges and Threats”.

RESEARCH DESIGN

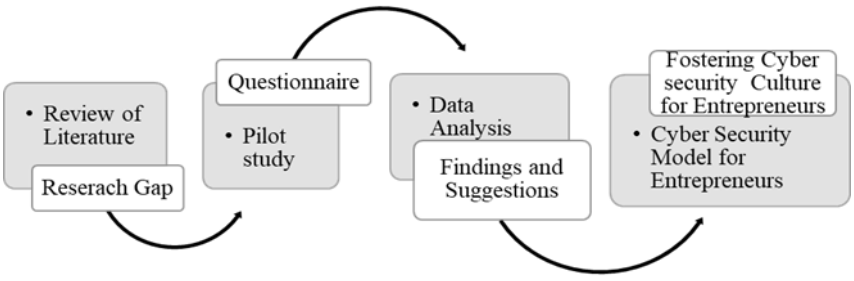

Figure1: Research design of study

This research is exploratory research; carried out as field survey in which the questionnaire is used for collecting the information of entrepreneurs and from small businesses from various organizations.

Sample Size: The data of 30 respondents is collected, objectives and hypothesis are formulated, and the data is cleaned, tabulated and analysed with the help of statistical tools (SPSS). Based on the analysis the result and Interpretation are drawn.

- Primary Data is collected through the questionnaire, group discussion and interview with the entrepreneurs.
- Secondary Data is collected from thesis, white papers, Journals, Magazines, Books, Articles, blogs, social networking sites, Published reports, News Papers, Websites, social Medias, etc.

CYBER-ATTACKS ON SMALL BUSINESS

A study carried out for small business and cyber threats on small business (2021) indicates the increasing rate of cyber-attacks. It has examined that:

- Approximate 60 % small businesses are victims of various types of cyber-attacks.
- Ransomware type of cyber-attack impacted on 82 % of small business and victimized more than 1000 employees.
- The spam and bulk emails, phishing and malware type of cyber-attacks are also impacted on small business and their employees during the day-to-day operations.
- Approximate 350 % of employees of small business has faced the cyber-attacks on higher risk and their impacts result in challenging tasks.
- Approximate 27% of entrepreneurs are not having cyber security related measures, policies and the mechanism of strong security of their sensitive information and data. Due to the same maximum financial frauds are happened and cyber criminals are taking it easy target for the same. [18], [21].
- The statistics of different cyber-attacks on small business and the faced by an entrepreneurs. It has resulted that, 18% of cyber-attacks are of malware type , 17 % are phishing , 16 % are data breaches , 15 % are website hacking , 12 % are DDoS attacks , 10 % Ransomware and 12 % are other types of cyber-attacks.

CYBER-ATTACK AND ENTREPRENEURSHIP

Start-ups are often prime targets for cybercriminals due to their smaller teams and limited security resources, making them more vulnerable than larger enterprises. It has observed that approximate 43% of cyber-attacks are targeted on small business while as just 14% entrepreneurs of them have sufficient mechanism and defended the cyber-attacks. However, a start-up's size can also be an advantage—it allows for a more agile and security-conscious culture to be built from the start. From day one, every start up should prioritize training employees in essential security practices to build a strong foundation for cybersecurity.

While securing endpoints is essential, it's only part of the equation. With businesses increasingly shifting to the cloud and hybrid work becoming a permanent norm, cybercriminals are relentlessly targeting unsecured identities. Alarmingly, 93% of organizations have faced two or more identity-related breaches in the past year. This underscores the urgent need for strong identity solutions like Identity and Access Management (IAM). IAM ensures that access is granted to right person, for right time, and with right devices, reinforcing overall cybersecurity.Cybercriminals continuously refine their attack strategies based on your business's security measures. Weak cybersecurity practices can leave the businesses and entrepreneurs to get exposed to these evolving threats. In the event of a cyber-attack, your business stands to lose in terms of: Loss of Revenue, Ransomware, Loss of Customer Trust, and Damage to business/entrepreneurs, Reputation and Legal Implications. It has observed that, due to various types of cyber-attacks entrepreneurs are facing the various consequences for their business and start-ups namely system downtime and loss of productivity , revenue loss, loss of customer trust , important and critical data loss , loss of future business opportunities ,penalties in terms of legal matters , loss of equipment's and devices , various penalties , lawsuits filed against the organization or entrepreneurs and mainly loss of business reputation which plays adverse impact on business and its future growth .

RESULT AND DISCUSSION

The present study has carried out empirical research based on survey of 30 entrepreneurs. The data is analysed using Statistical Package for the Social Sciences statistical tool. The findings from the study are as:

- **Enterpreuners Aswareness about cyber security:** It has observed that most of the entrepreneurs are ware about the cyber-attacks. The research has resulted that there is need of data protection of entrepreneur's businesses as well as data security also. The most of the entrepreneurs have not implemented cyber security policies where as there is need of establishing and implementing the cyber security policies. Also, it has observed that most of the employees in small businesses are not ware about cyber security.Hence it has concluded that, entrepreneurs must be aware about the cybercrimes, cyber-attacks, need and significance of data security and data protection as well as proper cyber security policy must be implemented by the entrepreneurs. Also, entrepreneurs must make their employees aware about the cyber security and cyber-attacks.
- **Password Mangment**: The study depicts the password management security taken care by an entrepreneur, it has observed that 33 % frequently uses strong passwords, 40 % rarely uses strong passwords while as 10 % uses strong passwords to some extend and 10 % never uses strong passwords for their businesses. 40 % entrepreneurs enforce regular password changes, 23 % rarely, 17 % to some extend and 20 % never enforce for the same. The study also carried out in the line of password management tool; it has resulted that, 37 % has tool, 27 are rarely uses, 17 % uses to some extent and 20 % never uses password management tool. It has concluded that there is need of using strong passwords, enforcing the employees to change their passwords regular as well as entrepreneurs should use the password management tools for their day-to-day activities and tasks.
- **Access Controls:** The access controls used by am entrepreneurs illustrates that, 70 % are utters that there is need to have access controls while as 30 % says no need of the same. 43 % regularly reviews about the access logs while as 57 % not. 37 % entrepreneurs has configured firewall while as 63 % does not have.Hence it has been concluded that there need to have access controls and regular reviews of access controls as well as business must have well configured Wi-Fi facility so that it will not result on cyber-attacks. As well as data security, safety and privacy will be protected
- **Training and security measures** need to be taken care by an entrepreneurs. It has observed that 43% entrepreneurs organizes data privacy and security training to their employees while 33 % rarely and 23 % never do the same. 47 % entrepreneurs conduct regular audit as compared to 17 % does it rarely and 37 % never conduct the audits.
- **Secure access controls** such as biometric , key access card are available with 50 % entrepreneurs while as 27 % rarely uses an 23 % does not uses the access controls in their business and organization . 70 % are uses security cameras while as 30 % does not have security cameras. The study also reveals that, 63 % entrepreneurs takes cares of restriction of visitors in their organization where the data and security is considered while as 23 % rarely think about it and 13 % never takes care of visitors access to the organization.

Hence it has concluded that entrepreneurs needs to take care of employees training , regular data security audits, access controls and physical security , security cameras as well as visitors access to the sensitive data and sever rooms as well as in the organizations

HYPOTHESIS TESTING

H_1: The cybersecurity measures adopted by entrepreneurs vary significantly.

The researcher has carried out chi-square test to test the various cyber security measures carried out an entrepreneur. The result of the same are as

Table 1 :- Chi sqare test for cyber security measuers adopted by enterprenuers

Cyber Security measures adopted by entrepreneurs	strong access control	firewall configured	Cyber-attack/ Cyber threats awareness	Need of Data security and data protection	Cyber security policy is implemented	Row total

YES	21 (16.40)[1.29] (13.60)[1.56]]	11 (16.40)[1.78]	18(16.40)[0.16]	23(16.40)[2.66]	9(16.40)[3.34]	82
NO	9(13.60([1.56]	19(13.60)[2.4]	12(13.60)[0.19]	7(13.60)[3.20]	21(13.60)[4.03]	62
						150(Gran d Total)

The value of chi-square is 20.3372 and p-value is 0.000428 here $p<0.05$ and the result is significant.

As $P<0.05$ null hypothesis is rejected and alternate is accepted Therefore is has resulted that, the cybersecurity measures adopted by entrepreneurs vary significantly.

Cybersecurity Model for Entrepreneurs

Information security is an ever-evolving discipline that integrates diverse technologies, frameworks, and best practices. The choice of cybersecurity frameworks and solutions varies greatly among organizations, influenced by factors such as industry, scale, and operational scope.[12,14] The present study has suggested cyber security model for entrepreneurs in the following figure 2 which will be useful for small, medium as well as large business and entrepreneurs to run their business in the safe cyber world or cyber space

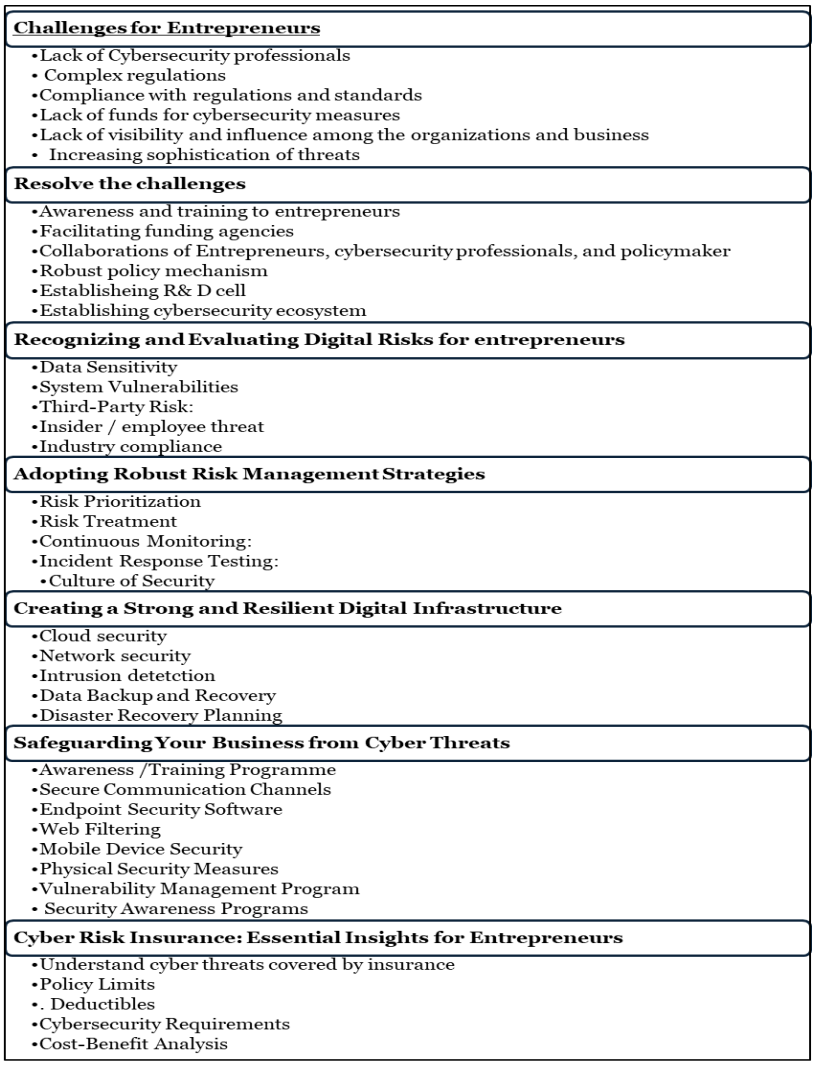

Figure 2: Cyber security model for Entrepreneurs

Cybersecurity for Entrepreneurs

Entrepreneurs faces various cyber security challenges such as limited resources, emerging threat, innovations in new technologies, human error, regular risk assessment and addressing it , Firewall setup and security , training employees, using cybersecurity framework , cloud security , AI and security , mobile device security , end point security , compliance of data protections and regulations, adopting cyber insurance and fostering cyber security culture in the organization, encouraging open communication about cyber threats and cyber-attacks .

Entrepreneurs, especially those running start-ups and small businesses, are prime targets for cyber threats. For entrepreneurs, their businesses from cyber threats. By following key cybersecurity best practices, they can safeguard sensitive data and strengthen your start-up's security. Proactively adopting these measures will help mitigate risks, defend against cyber-attacks, and enhance your overall cybersecurity resilience. An entrepreneurs can opt cyber security tips suggested in the presently study such as network security , employee training , information protection , firewall security , make action plan , frequent backups , access control and authentication rights. So that they will be safe in the cyber world for day to day tasks.

Cyber Insurance for Entrepreneurs

In the digital era, entrepreneurs are facing cyber-attacks and it has impacted on financial and organizations reputations adversely. The study also covers there is need of cyber insurance for entrepreneurs as a part of cyber. The various types of Coverage in Cyber Insurance includes data breach, network security, privacy to protect personal data , business interruption , cyber extortion , media liability , legal and regulatory charges , data loss and restoration data security and network security as well as crisis management. Cyber insurance is not just a protective measure but a strategic investment that underscores a business's commitment to safeguarding its digital assets and customer trust. Cyber insurance is an indispensable tool that provides peace of mind and ensures long-term sustainability for entrepreneurs.

FOSTERING A CYBERSECURITY CULTURE FOR ENTREPRENEURS

Cybersecurity culture for entrepreneurs and organization plays significant role to have cyber safe environment. There is need to foster the cyber security culture, be updated with the emerging cyber security trends and measures , as well as to understand the legal implications of cyber security breaches represented in the above figure 3. Fostering a cybersecurity culture is essential for entrepreneurs as it helps protect business assets, build customer trust, and ensure long-term success. As well as entrepreneurs can strengthen their business resilience, protect their stakeholders, and drive sustainable growth.

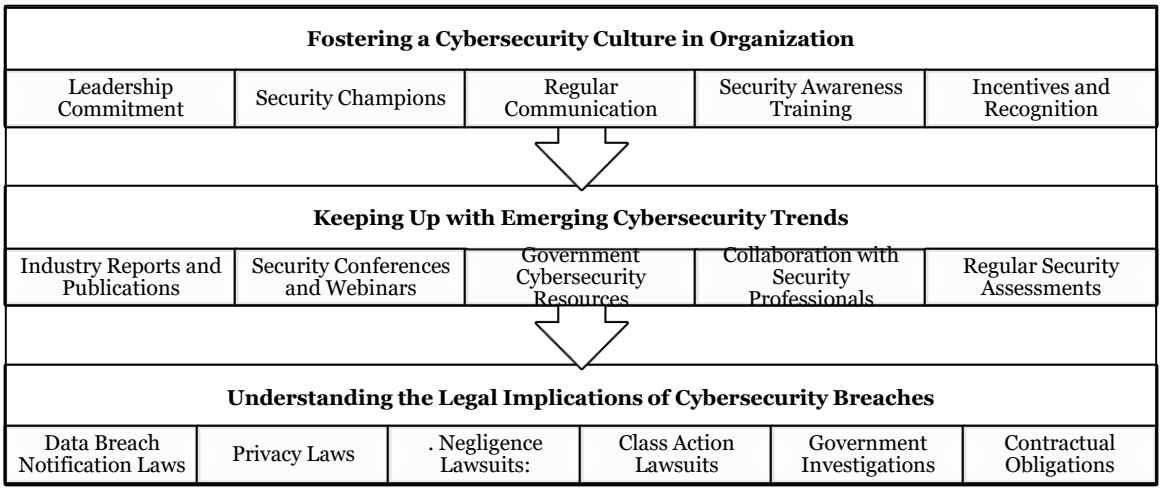

Figure 3: Cybersecurity culture for entrepreneurs

Suggestions:

- There is need of frequent security assessments which will be beneficial for addressing the potential vulnerabilities within your IT infrastructure and organization setup.

- Adopt a multi-layered security approach that combines advanced technological solutions with comprehensive employee training and awareness initiatives.
- Create a detailed incident response plan to ensure efficient handling and recovery in the event of a cyberattack.
- Entrepreneurs must stay informed about emerging cybersecurity trends and potential cyber threats, implementing proactive measures to safeguard their businesses.
- Work with legal experts to understand your data security responsibilities and reduce legal risks associated with cyber incidents.
- By proactively addressing cybersecurity concerns, entrepreneurs can focus on growing their businesses and achieving lasting success in the digital landscape.
- Entrepreneurs must adopt the cyber insurance which helps businesses to navigate the complex landscape of cyber threats and ensure long-term resilience.

CONCLUSION

The future of cybersecurity is ever-evolving and unpredictable. Individuals who can foresee trends, develop new skills, and adopt emerging technologies will be uniquely equipped to drive and shape the industry's direction.Cybersecurity threats are a persistent and ever-changing challenge for businesses in the digital era. Entrepreneurs need a thorough understanding of cybersecurity best practices and risk management techniques to effectively safeguard their businesses. Creating a strong digital infrastructure and promoting a culture of security awareness are essential for reducing cyber risks. Cyber risk insurance can serve as an effective tool to mitigate the financial consequences of cyber-attacks. Ongoing learning, adaptability, and collaboration with cybersecurity experts and entrepreneurs need to take care of innovative tools and techniques, measures to take care of to defend cyber-attacks and be safe in the Cyber space and sustain in the internet world

REFRENCES

[1] https://onlinelibrary.wiley.com/pb-assets/assets/19364490/SI%20CFP-1694804644.pdf
[2] https://snatika.com/single-blog/entrepreneurial-opportunities-in-cybersecurity--data-science--and-it-industry
[3] Nick Rahimi N., Murad S., Lee S. (2024). Entrepreneurship Opportunities in Cybersecurity https://www.researchgate.net/publication/382378756_Entrepreneurship_Opportunities_in_Cybersecurity
[4] Wasyihun Sema Admass, Yirga Yayeh Munaye, Abebe Abeshu Diro,(2024) . Cyber security: State of the art, challenges and future directions, Cyber Security and Applications, 2, ISSN 2772-9184, https://doi.org/10.1016/j.csa.2023.100031
[5] https://cybervie.com/other/the-future-of-cybersecurity-challenges-and-opportunities/
[6] https://www.villageglobal.vc/insights/5-entrepreneurial-opportunities-in-cyber-security-today
[7] Jagpreet Kaur, K .R. Ramkumar (2022). The recent trends in cyber security: A review. Journal of King Saud University – Computer and Information Sciences 34 (2022), 5766–5781
[8] https://www.fcc.gov/communications-business-opportunities/cybersecurity-small-businesses
[9] https://www.connectwise.com/blog/cybersecurity/11-best-cybersecurity-frameworks
[10] https://www.linkedin.com/pulse/cybersecurity-101-entrepreneurs-powerdmarcom-hqyoc?utm_source=share&utm_medium=member_android&utm_campaign=share_via
[11] Brahme, A., & Joshi, S.B. (2013). A review of cybercrime: An ever growing threat and its influence on society & IT sector.
[12] Brahme, A. M. (2012). Internet Fraud as One of the Cyber Threat and its Impact in India. International Journal of Computer Science and Information Security, 10(11), 38.
[13] Brahme A. (2013) .A REVIEW OF CYBERBULLYING AND CYBER THREATS IN EDUCATION. International Journal of Computer Engineering and Technology (IJCET) -4(3), Pages: 324-330. https://iaeme.com/MasterAdmin/Journal_uploads/IJCET/VOLUME_4_ISSUE_3/IJCET_04_03_029.pdf
[14] Brahme, A., & Mundhe, S.D. (2014). A Comparative Study of Social Networking Sites and Ever-increasing Cyberbullying with Respect to Indian Youth and Teenagers.

[15] Pavithran A. Why Cybersecurity is the Cornerstone of success for Business of All Sizes. https://www.entrepreneur.com/leadership/why-cybersecurity-is-the-cornerstone-of-success-for/483763
[16] Afolabi, John. (2024). Cybersecurity Challenges and Solutions for Small Businesses.
[17] https://www.stationx.net/cyber-attacks-on-small-businesses-statistics/
[18] Saha, B. and Anwar, Z. (2024) A Review of Cybersecurity Challenges in Small Business: The Imperative for a Future Governance Framework. Journal of Information Security, 15, 24-39. doi: 10.4236/jis.2024.151003.
[19] Khamrai Mr. Vineet Khamrai.(2024). Cybersecurity And Risk Management For Entrepreneurs In The Digital Era. 12(4) https://www.ijcrt.org/papers/IJCRTAG02024.pdf
[20] Patil A. (2024) . Research Paper on Cyber Security Challenges and Threats, 4(1). https://ijarsct.co.in/Paper15082.pdf
[21] https://www.verizon.com/about/news/verizon-2021-data-breach-investigations-report
[22] https://www.connectwise.com/blog/cybersecurity/11-best-cybersecurity-frameworkshttps://www.fcc.gov/communications-business-opportunities/cybersecurity-small-businesses
[23] https://www.fcc.gov/communications-business-opportunities/cybersecurity-small-businesses
[24] 10 Biggest Cybersecurity Challenges Industry is Facing in 2023 (thesagenext.com)
[25] Albalawi, Azzam & Almaiah, Mohammed. (2022). Assessing And Reviewing Of Cyber-Security Threats, Attacks, Mitigation Techniques In Iot Environment. Journal of Theoretical and Applied Information Technology. 100.
[26] https://www.geeksforgeeks.org/10-cybersecurity-tips-for-entrepreneur/
[27] https://www.startupcityindia.com/for-entrepreneur/cybersecurity-for-entrepreneurs-safeguarding-your-business-from-evolving-threats
[28] Chandna, V. and Tiwari, P. (2023), "Cybersecurity and the new firm: surviving online threats", Journal of Business Strategy, Vol. 44 No. 1, pp. 3-12. https://doi.org/10.1108/JBS-08-2021-0146
[29] Dasawat, S.S., & Sharma, S. (2023). Cyber Security Integration with Smart New Age Sustainable Startup Business, Risk Management, Automation and Scaling System for Entrepreneurs: An Artificial Intelligence Approach. 2023 7th International Conference on Intelligent Computing and Control Systems (ICICCS), 1357-1363.
[30] Alraja, M. N., Butt, U. J., & Abbod, M. (2023). Information security policies compliance in a global setting: An employee's perspective. Computers & Security, 129. 100 https://doi.org/10.1016/j.cose.2023.103208
[31] https://version1.equitymatch.co/newsbrief/implementing-foundational-cybersecurity-measures/
[32] https://www.ceotodaymagazine.com/2024/12/cybersecurity-challenges-for-modern-entrepreneurs-what-you-need-to-know/
[33] https://www.arenesslaw.com/navigating-cybersecurity-challenges-for-startups/
[34] https://www.pwc.com/gx/en/services/entrepreneurial-private-business/five-cyber-security-issues.html
[35] Brahme A.(2024) , Forecasting usage of social networking sites for sustainable education and its influence on students and academician. Sustainable Smart Technology Businesses in Global Economies, 252-262. ISBN 9781041017721