GE-International Journal of Management Research
ISSN (O): (2321-1709), ISSN (P): (2394-4226)
Vol. 12, Issue 09, Sep 2024 Impact Factor: 8.466
© Association of Academic Researchers and Faculties (AARF)
www.aarf.asia,**Email** : editoraarf@gmail.com

Internet of Things (IoT) in Entrepreneurship : The Biggest Challenges

Devarshi Chatterjee
Student, Indian Institute of Management Ahmedabad, India
Vastrapur, Ahmedabad, 380015, India
deva.chat123@gmail.com;
and
Prof (Dr) Devapriya Chatterjee
Ex-Director (MBA), Shankara Group of Institutions Jaipur,
Management Consultant and Chartered Engineer (India)
BB-73, Salt Lake City, Kolkata-700064, India
chatterjee.devapriya@gmail.com,

Abstract

In several organizations, the main element for the augmentation of competitiveness is Internet of Things (IoT). Inspite of the growth of importance of the security of Internet of Things (IoT), and the steady increase in the number of cyber-attacks on the devices of Internet of Things (IoT), the research is still incomplete on the significance of the measures of security of Internet of Things (IoT) on the challenges of security. The study makes a review of the security of Internet of Things (IoT) in the organizations of the present era, manufacturing the products of Internet of Things (IoT), and commencing the modifications towards the digitalization of the processes of manufacturing, as well as the products. The scrutiny of the requirements in the security of Internet of Things (IoT), was based on the reports of the prevailing security of Internet of Things (IoT), and a detailed review that was made, for the strengthening of the security, and the charting of the required resolutions to the active challenges. The charting enables every stakeholder to understand the initiatives being made for the security of Internet of Things (IoT) in the requirements and issues of their businesses. It was concluded on the basis of the studies, that the organizations, in general, recognize that encryption is the basic measure of security, but fail to comprehend the advanced processes of the protection of devices and data, along with the surface of the threat. The research brings to light that most of the organizations lack the expertise in the security of Internet of Things (IoT), and are more inclined to outsourcing the operations of security to third party providers. There is transformation in the global market in the way that massive digitalization is under way, and that block-chain, big data as well as Internet of Things (IoT) are the testimonies of the transformation of the global activities and business from the physical environment to the digital environment, that augment the competition in business, and enhance the growth of business. This allows the citizens to control all connected products.

Keywords :competitiveness, cyber-attacks, digitalization, encryption and transformation

Objectives of Study

The major objectives of the study include :

a) Make a scrutiny of the present state of the security of Internet of Things (IoT) in the organizations by the analyses of the available documentation, as well as the resources, of Internet of Things (IoT)

b) Make the analyses as well as the identification of the demands of the organizations, at the time of the deployment and planning of the security of Internet of things (IoT), for their processes and products.

c) Make a gap analysis of the work on the security of Internet of Things (IoT), while considering that Internet of Things (IoT) would have a significant impact on the business model or the business strategy of the organization.

Methodology

It has to be considered that the level of security of the new digital technologies, including Internet of Things (IoT) is inadequate, and requires improvement. The organizations are focusing on innovative and cutting-edge technologies, that tend to be efficient, fast moving and competitive. Depending on the business, the organizations adopt the most suitable technology. Though the vast majority of organizations use cloud computing, it is still observed that a considerable number is already using or planning to use the Internet of Things (IoT). These innovative technologies, however, are a source of cyber risk to the processes as well as products, sensitive data and connection. These risks cause the organizations to be more vulnerable to digital intrusions, due to the enhanced number of points of entry. If the security of Internet of Things (IoT) is improperly implemented, it would result in a loss of reputation for the company, due to the compromise of business processes, by ways of leakage of data. It has further been observed, that Internet of Things (IoT) might also cause more sophisticated attacks on the systems of the users, and also deliver malware, that could be utilized by hackers, to use the network of Internet of Things (IoT) for launching digital attacks in the networks of the computers of businesses, as well as smart cities and houses. The researchers have always reported the bursts of innovative instances of fraudulence, known as sextortion scam, due to the panic raised over the reliability of smart cameras. This scam has the record of compromising the home cameras, thus establishing that every digital process could be hacked.

Studies also revealed that low-powered protection of the products of Internet of Things (IoT), gives the advantage to the hackers towards the creation of botnets of Internet of Things (IoT). These attacks are most unsophisticated, and permit botnets to deal with devices with the help of outdated vulnerabilities, and take control of the same.The most popular strategies for dealing with the devices comprise of the malware families of Nyadrop and Mirai. The researchers investigated the darknet for identifying the vulnerabilities of Internet of Things (IoT), that are most popular with the hackers. The hackers engage in business, by selling the new vulnerabilities, for modified firmware and routers for electricity. The darknet also enables the hackers to make purchases and sell botnets, that are based on the devices of Internet of Things (IoT), for organizing attacks of Distributed Denial of Service (DDoS). These attacks have urged the organizations to move for the systematic protection of the processes and devices of Internet of Things (IoT), but the same still lacks the commitment. Organizations mention that the lack of skillset of the employees is the major reason for entering into partnerships with the service providers of Internet of Things (IoT) as well as cloud service providers. The partnerships boost the arrangement of Internet of Things (IoT). However, the businesses acknowledge the limitations of the venture of partnership. They cease to have control over the data garnered by the services and products of Internet of Things (IoT), when the same are shifted from one partner to another, that leaves the data exposed. The study brings forward the challenges of unavailability of skillset and expertise, inadequate support of top management, as well as low consciousness of the security level of the processes and products of Internet of things (IoT).

Findings

The findings of the research could be divided in two segments. One segment would deal with the confrontations with the security of Internet of Things (IoT), and the other segment would deal with the steps for strengthening the security of Internet of Things (IoT).

1. Confrontations with the security of Internet of Things (IoT)

a) Alien Risk Surfaces

The businesses make common mistakes that the data from the system of Internet of Things (IoT) is safe, when not used for finance purposes. The businesses comprehend that the sensor measurement sent at intervals is not of importance to the cyber-attackers, as the information transmitted is not of critical nature. There is lack of information regarding the nature of risks towards the products of Internet of Things (IoT), and so a threat model could not be ascertained.

b) Inadequate Organizational Skillset

Since the technology of the services of Internet of Things (IoT) is comparatively new, the businesses require additional skillsets, and the identification of an expert, having knowledge in this unknown zone, proves to be of challenge. Competencies and responsibilities are segmented within organizations, and the responsibilities regarding Internet of Things (IoT) remain unclear.

c) Unclear Standards and Guidance

The businesses have complained about the unclear set of accepted standards, and the failure to identify authentic checklists and guidelines. The security-based organizations do not have a coherent structure, and fail to recommend specific standards that could be compatible to all the domains. The variety of standards makes the protection of the systems of Internet of Things (IoT) difficult.

d) Lack of Alertness and Perception

There is complete lack of awareness about the security of Internet of Things (IoT) among most of the users. Both businesses and customers need additional education in the matter of security, that would imbibe a principal understanding, of the steps to be taken for the mitigation of risks of hacking.

e) Undefinable Benchmarks for the Security of Internet of Things (IoT)

Though the organizations, in general, understand the importance of the protection required for the data and devices, that are transferred by Internet of Things (IoT), very few of the businesses make a design approach for the security. This is mainly due to the lack of understanding of the features of the systems of Internet of Things (IoT).

f) Issue with Third Parties

The businesses are aware that the transfer of data is a long process from the end of the producer to the end customers, that include service providers of Internet of Things (IoT), cloud providers and providers of communication.The businesses consider the risk involving third-parties as a severe menace to the confidential and sensitive information.

g) Ignorance of Top Management

Top management is generally ignorant of the security issues of Internet of Things (IoT), unless the system is dealing with sensitive and personal matters. The top management normally allocates only a meagre amount in the budget for the security of the devices of Internet of Things (IoT). There is however an augmentation in sales, consequential to the implementation of the measures of security on Internet of Things (IoT).

2. Steps for Strengthening the Security of Internet of Things (IoT)

a) Uniformity and Regulations

Standards and dedicated compliance help in the storage and handling of sensitive data of Internet of Things (IoT), that ensures the trust to the thirds parties who handle the data, and also protects the data. There needs to be large fines and standard operating procedures for the security of Internet of Things (IoT) that raises the responsibilities, and resolves the issues of undefined metrics challenges, as well as non-trusted third parties.

b) Security Operations by Third Parties

The organizations feel insecure due to the unavailability of adequate in-company skillsets, and so they tend to engage third parties for the operations of security, that would augment the level of service, as well as products, without incurring any expenditure for technology, or hiring an expert. This form of outsourcing tends to be the most popular among organizations for catering to the measures of security.

c) Promotion of Consciousness

All the surveys of research and market focus on the promotion of consciousness among businesses and customers, that could augment the awareness of the privacy of data and digital security. This improves the standards of security of the products of Internet of Things (IoT), and promotes a high level of competent workforce.

d) Deployment of In-Company Workforce

It is essential to have an in-company team, deployed for the security of Internet of Things (IoT), that could augment the in-time process of recovery, enhance digital resilience, make quicker detection of incidence, that would make the business better-managed and well-organized.

e) Funding

An enhancement in the funding of the security of Internet of Things (IoT) results in huge advantages, regarding the operational efficiency, building a relationship of trust with customers, as well as cause a rise of protection.

f) Deployment in the Ecosystem of Internet of Things (IoT)

It is observed that all organizations are not standalone, but comprise of a complicated business ecosystem with services, software as well as hardware. Any possible breach in the company would affect all the levels of security, as well as the manufacturers of software and hardware. Third parties could be engaged in a responsible role for providing protection against digital attacks, as well as providing cyber security training to employees. So it is essential to chart the responsibility of the employees in the ecosystem, specifying responsibilities and duties.

g) Execution of the Security Measures of Internet of Things (IoT)

There are two choices of executing the security measures, either at the design stage for in-coming customers, or after the product is launched in the market. The first choice is more secure and effective. The selection is driven by the requirements of the customers. It generally commences with modelling of threat, and assessment of risk and then ends with an optimal solution, that includes planning and mitigation of threat.

h) Business Strategy and Cyber Security

For the inclusion of the development of Internet of Things (IoT) in business strategy, the business needs to consider the associated risks and the necessary security, as part of the cyber security policy, that is incorporated in the corporate strategy.

Implementation and Recommendation

The measures for the strengthening and bracing of the security of Internet of Things (IoT), and the risks involved in the execution are discussed.

a) Third Party Outsourcing

It is understood by the organizations that third-party outsourcing is one of the cost-effective means for acquiring highly skilled security, as there is general opinion that it is not worth investing in the in-company skillset. There are mostly two types of security that are requested from the outsourcing suppliers. These comprise of outsourcing for specific services, and outsourcing for the entire project. A survey of the resources indicated that most of the organizations are acquainted with the risks involved in Internet of Things (IoT), but the security measures adopted are inadequate. The gap analyses indicate that there is lack of expertise varying from basic concept to highly skilled experts, who specialize in converting the measures of security to major operation processes.It was concluded that third party outsourcing is the result of lack of experienced personnel and time, and not just lack of expertise in the security of Internet of Things (IoT).

b) The Regulations of Legacy and Standardization

We are aware that solution to several troubles in business and consumers of services of Internet of Things (IoT) is certification. But the most intriguing fact is that there is no unified standard. The investigation of the attacks on the devices of Internet of Things (IoT), and the frequent susceptibilities that lead to the successful cyber attacks compel the organizations to seek guides for security for protecting the infrastructures and devices. A method of improving cyber security of Internet of Things (IoT) is the capacity to provide the updates of products, such that old versions of software are recognized as high security risks. To reduce vulnerability, it is necessary to use file security .txt with the public points of contacts for reporting of vulnerabilities. The heterogeneity of application domains, and end-users, warrant a level of multi-level standards, that vary in the degree of coverage.

c) Responsibility Allocation in Organization

There is common misunderstanding that cyber security is part of Information Technology. It is necessary that top management deploys the necessary capabilities, and take part in the brainstorming sessions of cyber attacks. It is observed that there is lack of knowledge among the employees in the field of security of the processes and products of Internet of Things (IoT).These employees need to be shifted more towards the leadership of top management as cyber security is nowadays the responsibility of all employees. This is inspite of the fact that the concerned employees may have no expertise in the field, and has little or no time for acquiring knowledge in the field of implementation of the measures of security of Internet of Things (IoT).

d) Making of Investment

Detailed surveys conducted on security have portrayed that organizations have slowly begun to make more investment for security, and are also allocating larger percentage from their budgets for programs of cyber-security. However, the trend of investment still indicates insufficient fund in comparison with the possible catastrophe of the cybercrime. Nearly ninety percent of the organizations are now of the opinion that investment for the new technologies are essential and crucial, including Internet of Things (IoT). However, the organizations have now expressed their readiness for increasing their budget for the security of Internet of Things (IoT). These organizations mainly include industrial goods, technology and automotive industry.

e) Internet of Things (IoT) Security Measures Implementation

It has come to light from surveys that though the organizations are highly interested in the security measures of Internet of Things (IoT), they are not making prompt decisions regarding the implementation. This is again because organizations are also adopting other technologies, like Artificial Intelligence, block-chain and cloud computing, though the security risks associated with these are higher. Internet of Things (IoT) being a new trend, the organizations had to bear huge misuse and series of cyber attacks on the devices, that compelled them to compile the measures of security even after the commencement of the running of the process. A few organizations are still clicking to the basic measures as passwords and encryption, and do not make further progress, as these lack the guidance and awareness. The most significant measures of security of Internet of Things (IoT), focus on secure communication, secure storage, authentication, as well as secure handling, that recognize the protection of data in process, in transit and at rest, along with the classification of the communicating devices.

f) Deployment within IoT Encryption

The typical survey reports in this field indicate that there is no clarity regarding the assignment and deployment of responsibilities, regarding the operations of the systems of Internet of Things (IoT) in the organization. If the responsibility for the security of Internet of Things (IoT), lies with the cloud, then the cloud service provider is responsible for the security of Internet of Things (IoT) in the cloud. For the other stages of operation, the responsibility is split between service providers and manufacturers of the products of Internet of Things (IoT), along with the application developers, third party specialists and security suppliers. The allocation between suppliers and the splitting of responsibilities would enable the handling of serious attacks, as well as leakage of information. In the event of litigation, it would be easier to prove to the stakeholders, that every possible action was taken to protect the business, and the possible reasons for the inability to prevent the incident.

g) Awareness Enhancement

The dynamic risks associated with the systems of security of Internet of Things (IoT) in organizations, are the lack of qualification in the growing, executing as well as troubleshooting the system of security of Internet of Things (IoT). There is essential need for employees, business leaders, as well as customers to undergo training in the security of Internet of Things (IoT). There would be a high level of proficiency, as well as consciousness and motivation to augment the market share, as there would be a demand from the consumers, for the purchase of products with augmented cyber-security. The result of the training would be to enable the understanding of the importance of the protection of information of the business environment, along with the understanding of the priorities as well as the leadership initiatives of the top management.

h) Cyber-Security Business Strategy and Security of Internet of Things (IoT)

The implementation of the security of processes and products of Internet of Things (IoT) is considered as a part of the business strategy of cyber-security, in the organizations. This helps in the strengthening of the security of the Internet of Things (IoT). It is necessary for the organizations to change the approach to security as the present strategies, like anti-virus solutions and intrusion detecting systems, are insufficient. The most common aspect is that the businesses think that it is unnecessary to insert security in the budget, as the business is not large enough, and that their Internet of Things (IoT) would never be a target of cyber-attacks. The other aspect is that there is no importance of cyber-security, from the point of view of finance, as there is increase of cost for the processes and products of Internet of Things (IoT).

Conclusion

The main objective of the research was to recognize the challenges associated with the security of Internet of Things (IoT) in business and identify measures, for overpowering the challenges. The suggested charting of the significance of each of the measures of the security would enable the organizations to alter their attitude towards the security of Internet of Things (IoT), enhancing the safety of the devices, along with the data of the customers as well as processes, with an overall advantage in the competitiveness of businesses. The major findings of the study always indicate the significance of the execution of the security as a salient part of the strategy of business. The plausible reasons for the organizations facing difficulties in creating an enhanced posture of security for Internet of Things (IoT), include lack of cooperation between other functional departments, lack of understanding of the protection from cyber attacks against Internet of things (IoT), view of the management that it is not a prime concern, not viewing the cyber attacks on the products of Internet of Things (IoT) as a notable risk, and lack of internal skillsets. The organizations believe that processes of operation are of greater significance than considering the security of Internet of Things (IoT). The observations have further revealed that very few organizations keep a track of the risks of the processes and products of their Internet of Things (IoT). This is disastrous in the sense, that these products reach the customers, and start operations of tracking, without any cyber security check. For enhancement of cyber resilience, the organizations need to modernize the strategies for cyber security and also incorporate the security of Internet of Things (IoT). The execution of the security of Internet of Things (IoT) in the strategies of business not only augment the levels of awareness, but also make the delivery of technical, commercial as well as organizational qualifications for the commercial and strategic usage of the security of Internet of Things (IoT), regarding it as a dynamic criterion for competition. The regulatory control as well as standardization of the security of Internet of Things (IoT), would make this security discernible and comprehensible, that would make it an inspiration for further advancement. The organizations have a general understanding regarding processes of ensuring safety, generation of cyber risks, as well as the security of Internet of Things (IoT). But they lack the ability to provide the value chain, necessary for the Internet of Things (IoT). As the organizations lack the expertise to provide the appropriate security needed for their Internet of Things (IoT), they believe in third party providers of security for Internet of Things (IoT), and also depend on the checklists and guidance provided by them.

Limitation

It was observed that the implementation of the security measures, as transfer of data or appropriate encryption, prove to be great challenges, and these are absolutely essential for the enhancement of the profitability of the organizations. The measures of security are of low level. This is again because the top management has constraints to make higher investment for advanced mechanisms of security. The organizations do not have the mechanism for a precise estimation of actual costs for protection from cyber attacks of the processes as well as the products of Internet of Things (IoT), and do not take financial risks. The research further observed that though Internet of Things (IoT) is recognized by the organizations as a critical necessity, in this age of augmented digitalization, the implementation of security for the processes and the products of Internet of Things (IoT) is not assigned as a task of prime concern. It is therefore necessary for the organizations to update the procedures of planning, such that steps are taken for the education of top management in the understanding of the security and the threats involved in the processes of Internet of Things (IoT), for the change of strategy, towards the incorporation of the security of Internet of Things (IoT), in the prime concerns of the organization.

Acknowledgement

The authors express their deep gratitude and indebtedness to the anonymous reviewers, who have shown the right direction in the research, and have always provided an excellent guidance.

References

1. C. MacGilliviray, D. Reinsel, "Worldwide Global DataSphere IoT Device and Data Forecast, 2019-2023", May 2019, IDC, #US45066919
2. D. Demeter, M. Preuss, Y. Shemelev, "IoT : a Malware Story," Kaspersky Malware Report, Oct. 15, 2019. [online]. Available : https://securelist.com/iot-a-malware-story/94451/
3. E. Foudil, Y. Shafranovich, "A File Format to Aid in Security Vulnerability Disclosure." IETF Draft, 2020
4. Exclusive Research Report : 2019 Global State of Cybersecurity in Small and Medium-Sized Businesses. Keeper & Ponemon, 2019. [online]. Available : https://start.keeper.io/2019-ponemom-report\
5. H. C. Y. Chan, "Internet of Things Business Models," *J. Service Science and Management*, vol. 8, pp. 552-568, 2015
6. I. Kuzminykh, "Development of Traffic Light Control Algorithm in Smart Municipal Network", in *Proc. TCSET,* Lviv, Ukraine, 2016, pp. 896-898
7. I. Kuzminykh, A. Carlsson, "Analysts of Assets for Threat Risk Model in Avatar-Oriented IoT Architecture," in *NEW2AN/ruSMART '18 LNCS,* vol 11118, Springer, Cham, 2018
8. I. Kuzminykh, M. Yevdokymenko, V. Sokolov, "Encryption Algorithms in IoT Security : Security vs Lifetime," unpublished
9. IoT Security Compliance Framework. Release 2.1. IoT Security Foundation, May 2020
10. IoT Signals, Microsoft Report, Jul. 25, 2019 [online] Available : https://azure.microsoft.com/en-us/resources/iot-signals/
11. J. M. Such, P. Siholas, A. Rashid, J. Vidler and T. Seabrook, "Basic Cyber Hygiene : Does it work?," in Computer, vol.52, no. 4, pp. 21-31, April 2019, doi : 10.1109/MC.2018.2888766
12. K. Fazzini, "A Popular New Sextortion Scam Tricks Victims into Thinking They Are Being Recorded on Their Nest Cameras," CNBC,Jan. 19, 2020. [online]. Available : https://www.cnbc.com/2020/01/19/sextortion-scams-tricks-victims-into-thinking-nest-cameras-record-them.html
13. K. Wnuk, B. Teja, "The Impact of Internet of Things on Software Business Models," in *Software Business, ICSOB, LNBIP,* vol. 240, Springer, Cham, 2016, pp. 94-108

14. N. Dragoni, A. Giaretta, M. Mazzara. "The internet of hackable things," in *SEDA '16. Adv in Intell Sys and Comp*, vol. 717, Springer, Cham, 2016

15. NIST Special Publication 800-53. Security and Privacy Controls for Federal Information Systems and Organizations. JT FORCE, 2013

16. P. Midleton, R. Contu, B. Pace, S. Alaybeyi, "Forecast IoT Security, Worldwide, 2018", Gartner Research, Feb. 28, 2018

17. State of Cyber-security Report 2020. Accenture. [online]. Available : https://www.accenture.com/_acnmedia/PDF-116/Accenture-Cybersecrity-Report-2020.pdf

18. S. Furnell, M. Gennatou, P. S. Dowland, "Promoting Security Awareness and Training within Small Organizations," in *Proc. 1st Australian Inf Sec Management Workshop,* Geelong, Australia, 2000

19. The State of IoT Security. Gemalto Research Report. [online]. Available : https://www2.gemalto.com/iot/iot-security.html

20. Z. Bi, L. D. Xu and C. Wang, "Internet of Things for Enterprise Systems of Modern Manufacturing," *IEEE Trans. on Industrial inf*, vol. 10, no. 2, pp. 1537-1546, May 2014