2022-03-16

The Challenges with Internet of Things Security for Business

Kuzminykh, I

10.1007/978-3-030-97777-1_5
Springer International Publishing

The Challenges with Internet of Things Security for Business

Ievgeniia Kuzminykh[1][0000-0001-6917-4234], Bogdan Ghita[2][0000-0002-1788-547X], and Jose M. Such[1]

[1] King's College London, Strand, London, WC2R 2LS, UK
ievgeniia.kuzminykh@kcl.ac.uk
[2] University of Plymouth, Drake Circus, Plymouth, PL4 8AA UK
bogdan.ghita@plymouth.ac.uk

Abstract. Many companies consider IoT as a core element for increasing competitiveness. Despite the growing number of cyberattacks on IoT devices and the importance of IoT security, no study has yet primarily focused on the relationship between the potential impact of IoT security measures and the security challenges when implementing them. This paper presents a review of the current state of the art in IoT security for companies that produce IoT products and started transitioning towards the digitalization of their products and processes. The analysis of challenges in IoT security was conducted while mapping the relevant solutions for strengthening security to the already existing challenges. Based on the analysis, we conclude that almost all companies have an understanding of basic security measures such as encryption, but do not understand threat surface and not aware of advanced methods of protecting data and devices. The analysis shows that most companies do not have internal experts in IoT security and prefer to outsource operations to security providers.

Keywords: Business Strategy, IoT Certification, IoT Security, Regulations.

1 Introduction

The global market and society are currently undergoing the process of digitalization of the objects. Internet of things, digital twins, big data, blockchain are all evidence of a global trend of moving valuables and activities from the physical world to the digital world that drive growth of the business and raise the competitiveness. IoT came to simplify and optimize business processes, improve society lives, allow people to control connected products, save money and time, while maintaining our security and privacy. Are companies ready for the secure transmission, processing, and storage of IoT services data which are increasingly becoming part of their products and processes?

According to the Cisco Annual Internet report, we will have 29.3 billion networked devices by 2023 including smart TV, smartphones and M2M applications, such as smart meters, healthcare monitoring, transportation, and package or asset tracking [1].

The report Worldwide Global Data Sphere IoT Device and Data Forecast, 2019-2023, provides a forecast of 41.6 billion connected IoT devices, or "things", generating 79.4 zettabytes (ZB) of data in 2025 [2].

But the level of security of new online technologies, including IoT, remains quite low. According to Gartner report in 2018 [3] most of the companies considered IoT security IoT security not as part of the business strategy but as line-of-business unit. Therefore, the poor "security by design", and little control over the technology within connected devices were the consequences of the strategy and led to the growing number of cyberattacks on the IoT. In the period from 2015 to 2018 about 20% of the organizations were exposed to the attacks on IoT system, as reported by Gartner survey.

The number of cyberattacks on IoT devices is growing rapidly, as more and more customers, companies, municipal services start to use "smart" devices, such as routers, DVR cameras, smart traffic lights, asset trackers, smart meters, connecting to the Internet but not everyone is concerned about security [4]. By themselves, these devices may not be of interest to the cybercriminals. However, hackers crack them to use as robots to create botnets - networks of infected smart devices to conduct DDoS attacks - or as a proxy server for other types of malicious actions. Hackers simply need to discover the place where devices are connected not properly to be able to get into the system. And often, nine times out of ten they are successful. Most owners of hacked devices do not even suspect how their IoT devices are used. Cybercriminals see more and more financial opportunities to use such devices.

Regardless the number of attacks on IoT the Gartner report predicted that even in 2020 the security of the Internet of things would not be a priority for business [3]. In addition, the implementation of best security practices and tools in IoT planning would be ignored. Due to these two constraints, the companies can lose their reputation.

In this paper, we will take a look on the current state of the IoT security of the companies by analyzing the resources and available documentation on security in IoT. The purpose of the study is to identify and make analysis of the challenges that enterprises are faced when they plan and deploy IoT security at their products and processes. Moreover, several solutions to reduce risks related to IoT security have been analyzed as well and been mapped against identified issues.

Despite the growing importance of IoT, no study has yet primarily focused on the impact of IoT security on the business strategy or business models. For example, Z. Bi et al in [5] investigated the impact of IoT on manufacturing and enterprises, K. Wnuk and B.Teja in [6] analyzed the impact of IoT on software business and requirements engineering, H. C. Y. Chan in [7] made analysis of value chain elements and stakeholders for IoT business model and validated proposed business models through the case studies of some companies. But none of these works had considered IoT security factor when developing or analyzing the impact of IoT on the business strategy or business model of enterprise. Our study is intended to fill this gap.

The organization of the paper is as follows: Section 2 presents most important challenges raised with IoT security for businesses. In Section 3, the possible solutions to strengthen the IoT security are described, and analyzed in Section 4. Finally, Section 5 presents the conclusions.

2 Challenges in IoT Security

The following list outlines the challenges that enterprises are faced during planning and deploying IoT security. Totally, the discovered challenges can be divided in two categories: internal and external. Each category has number of challenges related to certain source that summarised on the Fig.1. Regardless the end user concerns about security of IoT services and products are high, the SMEs do not consider it as a challenge for business.

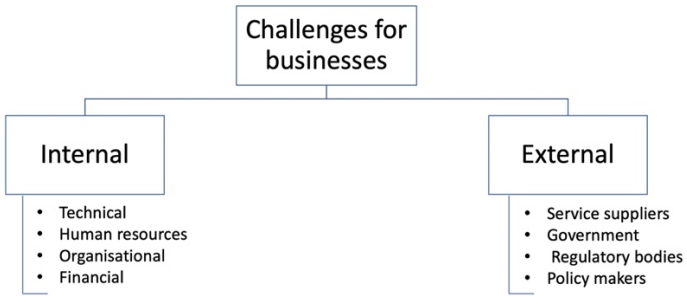

Fig. 1. The sources of challenges with IoT security for businesses.

Non-Trusted Third Parties. According to the report of Gemalto report about state of IoT security [8] most companies see the challenges with trying to secure their IoT products and services in ensuring data privacy and amount of data being collected. This user data can be shared between or even sold to various companies, violating the rights for privacy and security. Since data have a long way from its producer to the end consumer, including cloud, communication, and IoT service providers, most of the companies consider third-party risk as a serious threat to sensitive and confidential information. This stated in the report of Ponemon about State of Cybersecurity in Small and Medium Sized Businesses [9] with numbers of 57% who consider that third parties expose their companies to risk regarding a data privacy, and 58% who are not confident that their primary third party would notify them if it had a data breach.

Lack of Awareness. Regardless the fact that more than half (54%) of consumers own an IoT device (on average, two devices per person), only 14% consider themselves knowledgeable about the security of these devices [8]. This knowledge includes awareness about security measures, and principal understanding of what measure mitigate or eliminates what risk. Such statistics show that both consumers and enterprises need additional education in this area.

Unknown Threat Surface. The biggest mistake of the businesses that data from IoT system is often not considered critical until it is used for billing and accounting. In their opinion, the device sending sensor measurement periodically does not carry critical information and is not of interest to hackers. The report [10] showed that number of companies that have no confidence in identifying assets for threat model [11–13], as well as in understanding and assessing cyber risks, raised from 9% in 2018 to 18% in 2019 which is caused by the emergence of new technologies like IoT, blockchain, big data,

etc., that brought the complexity of an organization's technology footprint, including threat and cyber risk assessment.

Lack of Support from Top Management. Regarding the level of investment in security, the survey [10] showed that IoT device manufacturers and service providers spend only 11% of their total IoT budget on securing IoT devices. Regardless the 92% of companies have seen an increase in sales or use of the product following the implementation of IoT security measures, the company leaders are not encouraged by the widespread use of IoT security, they are more interested in getting their products to market quickly, rather than taking the necessary steps to build security.

Top managers pay attention to security in cases when IoT system is dealing with personal sensitive information, as customers' medical, financial, or tax records, otherwise the security is out of priority of management. Security financial investment, especially advanced, is painful for top management, therefore, the level of security measures remains low in IoT and leads to so many successful attacks.

Lack of In-House Expertise. Since IoT services is a new technology, for most of the companies is unknown territory that requires additional competence, and a finding an expert that skilled enough in IoT solutions can be challenging. For example, security professionals need practical knowledge of embedded devices, sensors, and computer-computer data communications, they should have experience in integrating heterogeneous protocols for data transfer, communications and network design both within the local Internet of things infrastructure and in cloud environments.

According to IoT Signals report from Microsoft [14] about half of the companies (47%) do not have enough workers skilled in IoT, and 44% are not having enough finances to invest in IoT security training for employees. Lack of external regulation on how to secure IoT devices and services, lack of internal knowledge of how to provide security measures were pointed as challenging in dealing with IoT. Moreover, inside organizations it is not clear who is responsible for IoT security and who does what: responsibilities and competencies are fragmented within the companies that causes uncertainty among companies and customers.

Undefined Metrics for IoT Security. The studies showed that companies really recognize the importance of protecting the IoT devices and data that they generate or transmit, and 50% of companies provide security based on a design approach. Two-thirds (67%) of organizations report using encryption as the main method of protecting IoT assets with 62% data encryption immediately upon reaching the IoT device, and 59% upon exiting the device [8]. But at the same time the organizations state that it is hard to define the right level of security, determine when that's fine enough. Basic encryption is good, but this is an artifact measure inherent to IT security in general, however, more specific measures to ensure the security of IoT are not popular due to lack of understanding of IoT system features, as limited memory and computational resources of IoT devices [15], special communication and information exchange protocols, supply chain complexity and increased connectivity of IoT ecosystems, as well as not understanding the essence of these measures.

Lack of Standards. The security of the Internet of things suffers from a lack of generally accepted standards. All businesses revealed the lack of standards, guidelines and/or checklists on how to ensure the security of IoT [8–10]. Adding new devices or their

components to the IoT ecosystem given that there are no standards, increase the risk of penetrating into critical systems (e.g. industrial, municipal, energy, etc.) by intruders with the subsequent termination of operations.

Although, there are many best practices and recommendations for IoT security from the security-focused organizations, there is no single coherent structure. Large vendors, world leader companies have their own specific standards, while each IoT domain has its own incompatible standards from industry leaders in certain domain. The variety of these standards makes it difficult not only to protect systems, but also to ensure interoperability between them.

3 Measures to Strengthen IoT Security

The following list outlines the measures for the companies that reduce risks related to IoT security.

Investment. Increasing investment into IoT security carries almost unlimited potential benefits in rise of protection, operational efficiency and in creating trustful relationships with customers. As survey [16] showed that the performing of better investment in the security allows for the business to stop more attacks, find and fix breaches faster and have less breach impact.

IoT Security as Part of Cybersecurity Business Strategy. The changing of business strategy forward new technologies trends related to digital transformation allows to achieve greater efficiency while also better protecting the business. However, in the process of including IoT development to the business strategy the organizations should not forget about the risks associated with IoT. Internet of things security, as part of cybersecurity policy, must be woven into corporate strategy, product design, budgets, and permeated with everyday business activities. Companies are required to change the approach to information security and the nature of their IT budgets, move their security mindset from technology-based defenses to new models for the implementation of information security, to proactive steps that include technology, process, and education.

IoT Security as Part of Cybersecurity Business Strategy. Most of the companies (99%) feel insufficient expertise to ensure the security of their products and processes, so they attract external consultants [17]. Using external suppliers and consultants in security operations can significantly increase the level of service and products without investment in technology or expert hiring.

An outsourcing continues to be popular solution in providing security measures for the companies: they prefer to outsource the security operations related to IoT, even if they have expertise, to do some operations as risk assessment, monitoring the traffic for malicious activities, incident response service. The outsourcing is more common trend among small and medium businesses, that was observed in previous years [18].

Allocating Responsibility within IoT Ecosystem. Nowadays, all businesses are not standalone production but complicated enterprise ecosystem with set of hardware, software and services. The potential breaches occurred in the company will affect not only company itself but hardware/software manufactures and all level of society. Cybersecurity could be one of these managed services that helps the company to tackle the IoT

security risks. Third-party supplier can play a responsible role on helping the companies to protect against cyberattacks and providing security training for employees. Therefore, it is important to map the responsibility within all interacting elements in company's IoT ecosystem to specify and divide duties and responsibilities.

Allocating Responsibility within Company. Having cybersecurity team inside company with allocated task related to IoT security can improve cyber resilience, provide faster incident detection, shorter response time and in-time recovery process. Well organized, supported and managed by company leaders IoT security will help to deal with the pervasive risks of the IoT technology for business.

Implementing IoT Security Measures. After series of the attack and misusing of IoT devices the companies are forced to add security measures to their products or include into already running processes. The implementing of best practices and security measures as stated by ENISA in [19] can help ensure overall security of IoT system and devices, prevent or properly respond to potential cyberattacks. There two approaches of implementing security measures to the product: at the design stage for new customers, and after the product is on the market. The first approach is the most effective and secure.

Both approaches can be accompanied by a systematic implementation or driven by customer requirements. During systematic implementation of IoT security the process is starting with threat modelling, risk assessment, and required security measures towards components of product and ending with mitigation, planning, and the optimal solution for each customer. But many companies admit that selection of IoT security measures is primary driven by customer requirements, and that some customers are not security-driven at all, they just need to have their data collected by IoT.

Standardization and Legacy Regulation. The legal standards and regulatory frameworks aimed at IoT service providers and manufacturers, with large fines and working instructions, can raise responsibilities of the business for IoT security, as well as, both non-trusted third parties and not defined IoT security metrics challenges can be resolved with it. The set of dedicated compliance and standards how to handle and store sensitive IoT data can help with ensuring protection of user data and lead to more trust towards third parties who have access to the data.

Standardization and legacy regulation will be a driving factor in the development of cybersecurity hygiene and culture, raising awareness and responsibility. Mandatory set of measures and requirements for the security level in different IoT domains will increase customer confidence towards manufacturers of IoT products and services. Moreover, companies will no longer be unaware of what a sufficient level of security is, and there will be no need in search of an individual solution for each client that will allow save time and resources. The certification procedure for IoT devices should not be bureaucratic and provide the buyer with a guarantee that it has a certain degree of protection against hacker attacks.

Raising awareness about security of companies is one of the measures to improve IoT product security standards. Many authors and reports [9, 20] emphasize higher general awareness among customers and business can drive a market growth, increase the understanding of cybersecurity and data privacy. A high level of competences will create a more skilled workforce that can serve as a differentiator by itself.

4 Analysis of IoT Security Measures

In this section the result of the analysis of measures for strengthening IoT security and risks associated with their implementation will be presented.

Investment. A number of security reports from Ponemon, Accenture, Deloitte, Hiscox, PwC [9, 16, 17, 21, 22] have already noticed that in the past 5 years the companies have begun to pay more attention to security, have larger percentage of investments in security. The reports of 2018 and 2020 [21, 23] showed that companies spend 10-12.5% of budget on cybersecurity programs.

Although 83% of organisations agree that new technologies are necessary and crucial, investment is lagging. Only two out of five companies invest in new technologies, including IoT. However, companies are ready in the near future to increase investment in security of Internet of things: about half of the companies expressed a desire to do this, of which the most interested in investing were areas such as the automotive industry, industrial goods and technology [22].

IoT Security as Part of Cybersecurity Business Strategy can help strengthen the security of IoT products and processes, but first, organizations need to change their approach to security because existing security strategies in the form of security appliance (FW, anti-virus solutions, intrusion detection systems) are becoming not enough. All organisations, including large businesses, continue to struggle with insufficient, outdated security strategies and plans that do not consider fully all risks and threats.

There is no research that can show business strategy of the companies towards the IoT security, but mindset regarding common security strategy in the company shows that there is three way of focus [24]:

- security operations operate under stealth and secrecy (60%)
- security efforts prioritize external threats (55%)
- security efforts mainly focus on prevention (55%)

In total, 42% of companies have no governance policies associated with IoT risks included to the business continuity plan [16].

The most *common reason* why these enterprises do not consider it necessary to include security into the business plan is because they consider themselves too small or insignificant to justify such measures. The opinion that prevails in this category of respondents is that their IoT system will not be affected by cyberattacks.

The *second popular reason* for business is that cybersecurity is not considered enough in priority. Companies prefer to place functionality of the products and processes related to IoT on the higher level than security.

Outsourcing Security Operations to Third-Party. The organizations believe that outsourcing is a cost-effective way to attract additional expert knowledge since it is quite difficult to convince management of in-house investments in such a narrow sector as IoT security.

The types of security services requested by companies from security suppliers can be divided into two types:

1) outsourcing that oriented on providing certain service, and
2) outsourcing that focused on the whole product.

Some companies purchase just additional pentesting of the product in addition to the pentesting conducted inside company, and some purchase all spectre of services during transmission, hosting and processing of data, including server security, authentication and authorization of users for granting access to data collected by IoT devices.

From the analysis of the reports we can conclude that the reasons for outsourcing are not only the lack of expertise in IoT security, but also the lack of time or human resources, therefore majority (93%) of companies indicated that they turn to suppliers in providing more than 10% of security operations, vulnerability management and incident monitoring. Only 8% of companies are highly confident in external suppliers and 55% stated that they are fairly confident [8]. Therefore, with such a low level of trust, it is better to have internal expert in-house with basic level of understanding the security measures, and proper evaluate what can be outsourced.

Generally, the involvement of professional service providers or security consultants should be considered as positive aspect that gives confidence in ensuring cyber and IoT security.

Allocating Responsibility Within IoT Ecosystem. The allocating IoT security operations to the external supplier demonstrates the trust relations inside value chain, and in many cases, relieves liability from the company itself. Another approach of managing security in company is to do it with its own efforts and do not delegate security operation to outsourcing parties. The allocating IoT security to the department or person in the company demonstrates a willingness to move towards including IoT security into the business strategy. In this case, all responsibility in providing protection and recovering measures lays on the company itself.

The Gemalto report [8] shows that there is no clear understanding who is responsible for what operation in IoT system deployed in the company. If with responsibility for stored in the cloud IoT data all is clear, and cloud service provider is responsible for security, then the responsibility for other stages of operation of the IoT system are split between manufacturers of IoT products, IoT service providers, API developers and third-party security suppliers and specialists.

Allocating Responsibility Within Company. For a long time, cybersecurity has been the responsibility of IT departments. The most common misconception among business leaders is that they believe that Information Security is part of IT. But security is a separate area that requires time.

In many cases the task of dealing with IOT security is done by the person who just interested in this field. This person has *no expertise* in security or has little, but spend his/her time on getting knowledge and implementing security measures. This approach is more appropriate to medium and small companies mostly due to lack of the resources.

Regardless the high concern about cybersecurity of IoT (80% think that a security incident related to unsecured IoT product could be catastrophic [9]), the top management rarely participates in cybersecurity discussions regarding, for example, building security into product designs. Earlier research showed that only 22% of companies have business leaders are accountable for cybersecurity [16], and only 21% monitor the risk of their IoT products [9]. But even these numbers need to be shifted more towards responsibility of top management because nowadays the cybersecurity is becoming a common task for all company employees.

Implementing of IoT Security Measures. Regardless the most companies (80%) are interested in IoT security [9], they are not in a rush with implementing security measures. According to [8] almost one-quarter of companies is aware of cybersecurity risks, but some companies do not have IoT security measures in place at all. This is because with the adopting of new technologies (IoT, AI, block chain, cloud computing), the main preference for half of companies (50%) was the pushing ahead a digital transformation, despite the potential security risks associated with them [8].

After series of the attacks against IoT devices, companies are forced to add security measures into their marketed products. Some companies have hung with a basic security measures as encryption and passwords and do not progress more due to the lack of awareness and guidance of how to do it. But it is required to keep balance between cryptography algorithm and level of security. Some of the algorithms are high energy consuming that can reduce the lifetime of IoT devices that powered by battery [25].

Half of the companies implements their security measures based on the current cybersecurity needs and customer demands, and do not consider future pervasive risks and needs [16]. The more aware customers about security risks and threats, the bigger the demand for IoT security measures. Therefore, it is very important to help consumers really understand what is happening with their data and teach them how it is possible to protect it.

Some companies have more than basic level with a systematic approach based on one of the cyber security frameworks, e.g. ISO 27001 [26], IoT Security Foundation [27], NIS directives [28], NIST SP 800-53 [29], IEC 62443 [30] UL 2900 series [31], and Cyber Essentials in UK [32].

The most important security measures in IoT should be focused on authentication, secure communication, handling, storage, which are aimed to protecting data in transit, protecting data in process, and protecting data at rest [33]. All companies should strive for providing all set of the data-centric security measures. This is not only correct, but also important if organizations have serious intension towards protecting their assets and the data of customers [11, 12, 19].

Standardization and Legacy Regulation. While certification promises a solution to many problems for business and for consumers of IoT services, a unified standard still does not exist. However, the large amount of IoT vulnerabilities forced the organizations focused on providing guides for security to make a number of recommendations on protecting IoT devices and IoT infrastructures.

Among bodies involved in the producing of recommendation for security of IoT devices, such as OWASP, ENISA, IoT Security Foundation, NCSC. The recommendations partially duplicate each other, are *advisory in nature*, therefore, cannot be considered as legacy regulations, and most companies simply ignore them.

Due to the fact that passwords are the most common weakness, the principal recommendation in all guidelines relates to the strengthening and control of the use and procedure of generating passwords. All passwords of user IoT devices should be unique and without the ability to reset them to factory settings.

Another measure of enhancing of IoT security stated in many guidelines is the ability to provide product updates, either remotely or in place. Usage of old versions of software are identified as high security risk in many regulations on ensuring IoT security.

Given the heterogeneity of applications by end-user (private person, company, state) and application domain (health, automotive, HVAC), the system of standards will be multi-level, varying in degree of coverage and detail [34].

While mitigating the risk associated with the low trust to suppliers the appearing of new standards and regulation can pose another challenge related to compliance with various standards, legal and regulatory structures.

Raising Awareness. The IoT security training for employees, customers and business leaders is required to build effective cybersecurity culture. It could be done through the educational institutions, roundtables, workshops, security consultancy firms, etc. [35].

IoT security training has not yet been widely disseminated in most organizations. The percentage of organizations that conduct educational training for employees and third parties about the risks in IoT remains small - only 24% of companies currently provide such information and education [9]. However, it is promising that three out of ten business leaders plan to invest more in IoT security training in the future [23].

Finally, the effectiveness of each security measure and its impact towards the identified challenge is presented in Table 1.

Table 1. Impact of the Measures on the Issues with IoT Security.

	Third parties	Lack of awareness	Threat surface	No support from management	No in-house expertise	Undefined metrics	Missing standard
Investment	Medium	High		Medium	High	Low	
IoT security strategy		Medium	High	High		Medium	Low
Outsourcing			Medium				
Ecosystem leadership	High			High	Low		
Company leadership	Medium			High	Medium		
IoT security measures			High			Low	Medium
Standardization						High	High
Raising awareness		High	High		High		Medium

Regardless its popularity the outsourcing is not effective strategy of the company in solving the issues related to IoT security. This measure leaves the company blind in relation to the threat surface, possible security solutions, does not increase knowledge within the company. The most effective method for solving a series of the most cutting-edge problems is an investment but not all companies are willing to spend more on security and on staff education.

Raising awareness is one more effective way to solve the set of the issues related to personal expertise inside company. During training the employees can expand their knowledge about IoT technology, attack surface, protection security measures, and, also, help the client to select IoT solution.

Using this matrix, the companies will be able to navigate in the selection of security measures and choose the most effective way to solve their specific issues.

5 Conclusions

The paper was aimed at identifying challenges with IoT security for business and finding possible measures to overcome these challenges. The proposed mapping of the

impact of each of the security measure will help companies change their mindset towards IoT security, increase the protection of devices, processes and customers data, and thus, business competitiveness.

Our findings continue to highlight the importance of implementing the IoT security as part of the business strategy. Among the reasons why companies have difficulties with creating a stronger IoT security posture are 1) lack of in-house expertise, 2) not understanding how to protect against IoT cyberattacks, 3) not a priority issue, 4) lack of collaboration with other functions, 5) management does not see cyberattacks on IoT products as a significant risk. First two are primary reasons for not implementing the IoT security, others are main reasons for companies to consider IoT security as afterwards because operational processes considered as more important.

Only two of ten companies monitor the risk of their IoT products and processes. This is catastrophic because these products go to the market, start operate in the customer houses or monitor engines without any cyber security check. Another challenge is related to implementing security measures, they are either basic in form of encryption and secure data transmission or have necessary for customer level.

Standardization and regulatory control of IoT security will make security of IoT tangible and understandable for business and, therefore, uses IoT security as a driving force for growth.

Finally, while more organizations are concerned about IoT security, the analysis showed that implementation of IoT security is not a priority task. Increasing understanding of IoT security risks and threats among top management and business leaders may facilitate the change of strategy towards inclusion of IoT security in the company's priority tasks. The companies must update the way they plan and execute IoT security.

References

1. Cisco Public: Cisco Annual Internet Report. (2018).
2. MacGillivsry, C., Reinsel, D.: Worldwide Global DataSphere IoT Device and Data Forecast, 2019–2023. 13 (2019).
3. Contu, R., Middleton, P., Alaybeyi, S., Pace, B.: Forecast : IoT Security , Worldwide , 2018. 26 (2018).
4. Kuzminvkh, I.: Development of traffic light control algorithm in smart municipal network. Mod. Probl. Radio Eng. Telecommun. Comput. Sci. Proc. 13th Int. Conf. TCSET 2016. 896–898 (2016). https://doi.org/10.1109/TCSET.2016.7452218.
5. Chengen, W., Li Da, X., Zhuming, B.: Internet of Things for Enterprise Systems of Modern Manufacturing. IEEE Trans. Ind. Informatics. (2014).
6. Wnuk, K., Murari, B.T.: The impact of internet of things on software business models. Lect. Notes Bus. Inf. Process. 240, 94–108 (2016). https://doi.org/10.1007/978-3-319-40515-5_7.
7. Chan, H.C.Y.: Internet of things business models. Internet Things Data Anal. Handb. 735–757 (2017). https://doi.org/10.1002/9781119173601.ch45.
8. Gemalto: The State of Iot Security. (2018).
9. Ponemon Instsitute: Exclusive Research Report 2019 Global State of Cybersecurity in Small and Medium-Sized Businesses. (2019).
10. Marsh: 2019 Global Cyber Risk Perception Survey. Microsoft Insights. 1–36 (2019).

11. Kuzminykh, I.: Avatar Conception for Thing Representation in Internet of Things. Proc. 14th Swedish Natl. Comput. Netw. Work. (2018).
12. Kuzminykh, I., Carlsson, A.: Analysis of Assets for Threat Risk Model in Avatar-Oriented IoT Architecture. Lect. Notes Comput. Sci. 11118 LNCS, 52–63 (2018). https://doi.org/10.1007/978-3-030-01168-0_6.
13. Bakhshi, T., Ghita, B., Kuzminykh, I.: Securing IoT Firmware - Technologies and Research Challenges. ACM Surv. (2021).
14. Microsoft: IoT SIGNALS. 80 (2019).
15. Kuzminykh, I., Carlsson, A., Yevdokymenko, M., Sokolov, V.: Investigation of the IoT Device Lifetime with Secure Data Transmission. Lect. Notes Comput. Sci. 11660 LNCS, 16–27 (2019). https://doi.org/10.1007/978-3-030-30859-9_2.
16. Accenture: Building Pervasive Cyber Resilience Now. Securing the Future Enterprise Today – 2018, https://www.accenture.com/_acnmedia/pdf-81/accenture-build-pervasive-cyber-resilience-now-landscape.pdf.
17. Deloitte: 2019 Future of cyber survey | Deloitte | Risk. (2019).
18. Cyber Security Breaches Survey 2020. Comput. Fraud Secur. 2020, 4 (2020). https://doi.org/10.1016/s1361-3723(20)30037-3.
19. ENISA: Good Practices for Security of Internet of Things in the context of Smart Manufacturing. Eur. Union Agency Netw. Inf. Secur. 1–118 (2018).
20. Furnell, S., Gennatou, M., Dowland, P.S.: Promoting security awareness and training within small organisations. Proc. 1st Aust. Inf. Secur. Manag. Work. (2000).
21. Wharton, G.: The Hiscox Cyber Readiness Report 2019 | Hiscox UK. R. (2019).
22. Randeria, Z., Horne, R.: Global State of Information Security® Survey. PwC UK. (2018).
23. Accenture: State of Cybersecurity Report 2020. (2020).
24. Accenture: The Cyber Security Leap: From Laggard to Leader. (2015).
25. Kuzminykh, I., Yevdokymenko, M., Sokolov, V.: Encryption Algorithms in IoT: Security vs Lifetime. Lect. Notes Data Eng. Commun. Technol. (2021).
26. International Standard Organization: IEC/ISO 27001:2013 Information technology — Security techniques — Information security management systems. (2013).
27. Iot SF: IoT Security Compliance Framework Release 2.1. (2020).
28. Markopoulou, D., Papakonstantinou, V., De Hert, P.: The New EU Cybersecurity Framework: The NIS Directive, ENISA's Role and the General Data Protection Regulation. SSRN Electron. J. (2021). https://doi.org/10.2139/ssrn.3493561.
29. National Institute of Standards and Technology: NIST Special Publication 800-53: Security and Privacy Controls for Federal Information Systems and Organizations. (2013).
30. IEC: Industrial communication networks – Network and system security - IEC 62443.
31. UL Standards: ANSI/CAN/UL Standard for Software Cybersecurity for Network-Connectable Products, Part1: General Requirements - UL2900-1. (2017).
32. Such, J.M., Ciholas, P., Rashid, A., Vidler, J., Seabrook, T.: Basic Cyber Hygiene: Does It Work? Computer (Long. Beach. Calif). 52, 21–31 (2019). https://doi.org/10.1109/MC.2018.2888766.
33. Inside Secure: IOT SECURITY SOLUTIONS White paper.
34. Huawei: Iot_Security_White_Paper_2018_V2_En.Pdf. (2018).
35. Kuzminykh, I., Yevdokymenko, M., Yeremenko, O., Lemeshko, O.: Increasing Teacher Competence in Cybersecurity using the EU Security Frameworks. Manuscr. Submitt. Publ. (2021).