Development of the Mechanism of Assessing Cyber Risks in the Internet of Things Projects

Sergei Grishunin[1(✉)], Svetlana Suloeva[1(✉)], Tatiana Nekrasova[1(✉)],
and Alexandra Egorova[2(✉)]

[1] St. Petersburg State Polytechnic University, St. Petersburg, Russia
sergei.v.grishunin@gmail.com, emm@spbstu.ru,
dean@fem.spbstu.ru
[2] Moscow State University, Moscow, Russia
alxegorova@gmail.com

Abstract. We developed the mechanism of assessing cyber risks for Internet of Things (IoT) projects. The relevance of this topic is explained by growing sophistication of cyber-attacks, the speed of new threats emergence and increasing damage from the attacks. The paper addresses decreasing efficiencies of existing mechanisms of cyber risk assessment and fills the research gaps in this area. Results include development of the mechanism's concept, its block diagram, the specification and description of its comprising tools and the case study. Unlike peers, the mechanism provided holistic approach to cyber risk assessment; integrated and coordinated all related activities and tools. It simulated the confidence interval of project return on investments (ROI) and showing the chances to go above risk appetite. It makes cyber risk assessment dynamic, iterative, responsive to changes in cyber environment. These advantages let us conclude that the mechanism should have a significant scientific and practical use.

Keywords: Internet of Things · Cyber risks · Cybersecurity · Risk controlling

1 Introduction

The Internet of Things (IoT) provides a wide avenue for innovations from the industrial use to healthcare and consumer. However, IoT can create significant risks for developers and users. The number and frequency of IoT attacks has been increasing while the direct and indirect damages have been rising. A single infected device can open the entire company ecosystem for attack, with potential disruptions ranging from individual privacy breaches to massive breakdown of public systems and threat to human life.

In such an environment, the procedures of cyber risk assessment must be integrated and coordinated in the single mechanism, which relies on combination of methods and tools and provide the range of likely monetary losses from the cybercrime during a given period. Such mechanism should ensure timely identification and assessment of threats, anticipation of likely new threats as well as the development and implementation of risk mitigation decisions. However, our research shows that many existing

O. Galinina et al. (Eds.): NEW2AN 2019/ruSMART 2019, LNCS 11660, pp. 481–494, 2019.
https://doi.org/10.1007/978-3-030-30859-9_41

mechanisms such as operationally critical threat-asset-vulnerability evaluation (OCTAVE) or cyber value at risk (CyVAR) only partially serve these purposes.

We closed the gaps in the research and developed the mechanism of cyber risk assessment in IoT projects. The novelty of the paper is driven by the advantages of the mechanism over its peers. Unlike peers, which estimate a single point estimate of risk impact, the mechanism simulates the confidential interval for project's ROI and shows the chances to go beyond risk appetite. It includes tools and methods that allow estimating risk frequencies with few data points. The mechanism provides the holistic approach for cyber risk assessment, integrates and co-ordinates all the activities of cyber risk assessment. It makes cyber risk assessment dynamic, iterative, responsive to changes in cyber environment.

In Sects. 2 and 3 we present the outlook for IoT and explain advantages of risk controlling application in cyber risk management. Section four presents the literature review in the area and identifies the research gaps. In Sects. 5 and 6 the mechanism of cyber risk assessment is developed and a case study is provided. In Sect. 7 the advantages of the mechanism are discussed and conclusions are formulated.

2 Internet of Things: Outlook and Challenges

The Internet of Things (IoT) is a suite of technologies and applications that equip devices and locations to generate data and information and to connect those devices and locations for instant data analysis and, ideally, "smart" action [2]. IoT implies physical objects being able to utilize the Internet to communicate data about their conditions, position or other attributes. In IoT, information and communication industries have merged together and formed info-communication space [3].

The number of IoT-connected devices will grow at compound annual rate of 15% to reach 31 billion units by 2020 with the estimated market value of $1.1 trillion [2]. It is fueled by (1) declining prices for bandwidth, data storage and computing; and (2) growing usage of augmented intelligence; and penetration of industrial robots. Industrial IoT units (such as devices for the conditions-based monitoring and predictive maintenance of capital assets) will capture of around 50% of global IoT spending [2]. The consumer, health or public services devices will take a share of 25% each [2].

Along with these opportunities, this industry is characterized by significant challenges that could stop investing in the sector. They include (1) lack of infrastructure to manage devices; (2) threat of users' non-acceptance of devices; (3) poor vendor execution, (4) operational problems; or (5) lack of regulation [2]. The most dangerous threats is the growing number of cyber-attacks on IoT units; the cyber-crime alone costs nations more than $1 billion globally [5–7]. Examples include (1) the distributed denial of services (DDOS) attacks; (2) data and identity theft; (3) reconnaissance attacks; (4) man in the middle penetration: (5) Trojans and viruses; and others [1]. Growing complexity, interconnection and pervasiveness of IoT expose these devices to new type of hazards that existing risk management methods are neither designed to anticipate nor predict [5, 8]. These challenges are forcing IoT developers, vendors and users to reconsider the approaches to cyber risk management [8] and switch to newest systems such as the project risk controlling [9, 11].

3 Risk Controlling in IoT Development Projects

Risk controlling (RC) is a goals-oriented set of methods, processes and tools for risk management in IoT development projects, the integral part of investment controlling [9, 11, 19]. RC provides the architecture (infrastructure and processes) of risk management while the project managers applying this infrastructure to particular risks make risk-informed decisions. The functions of RC are listed in [19]. Advantages of RC over the commonly applied integrated risk management are (1) fostering risk governance; (2) integration of risk management into the decision-making at all stages of the project; (3) co-ordination of all risk management activities; and (4) application of tools with low risk tolerance and increased focus on quantitative assessment of risks [9, 19].

In cyber security, RC is aimed to reduce the risk that the users of IoT solution fail to achieve the target return on investments (ROI) due to losses from the cybercrime [11]. The more complex the IoT project is the higher the gap can be between the realized and the target ROI (Fig. 1).

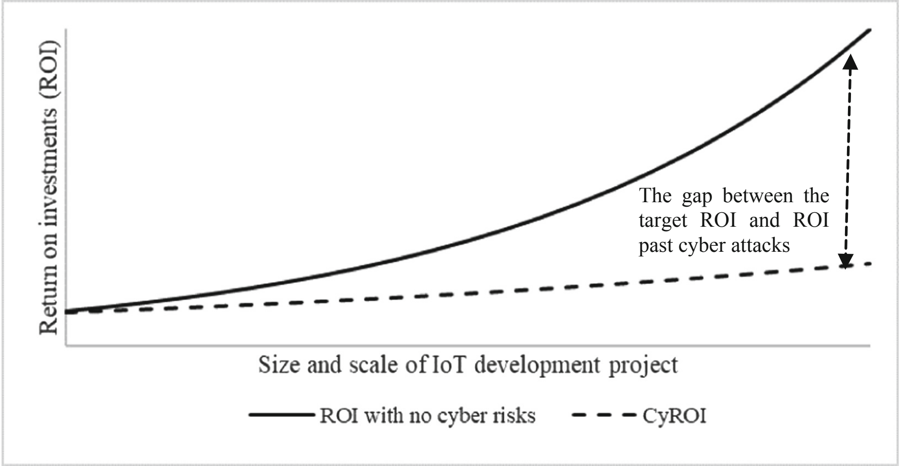

Fig. 1. Impact of cyber-attacks on IoT project ROI

This is underpinned by the increasing with the scale the attractiveness of the device to the attackers and the growing sophistication of the attacks resulting as increase in cost of controls and remediation. [10] To reflect the cyber exposures we developed the cyber ROI (CyROI) metric that measured the effectiveness of investments into IoT given cybercrime and related controls. For one-year horizon:

$$CyROI = \frac{(B - CL \times ME - C_{cs}) - (I_{IoT} + I_s)}{I_{IoT} + I_s} \tag{1}$$

Where, B – customer's benefits from application of IoT device; CL – losses from the cybercrime; ME – mitigation ratio, given the cybersecurity solution; I_{IoT} –

customer's investments into IoT device; I_s – customer's investments into development of cybersecurity solution; C_{cs} – maintenance costs of cybersecurity solution.

Consequently, for lengthy development projects with duration of more than one year, calculation of CyROI involves discounting for project's weighted average cost of capital (WACC):

$$CyROI = \frac{\sum_{t=1}^{T} \frac{\left(B_t - CL_t \times ME - C_{cs,t}\right)}{(1 + WACC)^t} - \left(I_{IoT} + I_s\right)}{I_{IoT} + I_s} \quad (2)$$

Where, t –the period of analysis; T – total number of periods.

To reduce this gap, IoT developers need to optimize the relationship among the benefits from adoption of technology; (2) residual losses from cyberattacks given control system; and (3) investments into control and remediation systems (cybersecurity solutions). Risk controlling system should (1) prevent and anticipate threats before they take hold; (2) monitor and neutralize risks already in play; and (3) restore normal operations as fast as possible if the risk event has occurred [10, 11, 13]. The critical question for the IoT developer is to assess accurately the potential impact of the threat on project ROI to decide on cost-effective measures and methods to minimize its consequences.

4 Cyber Risk Assessment: A Literature Review

The literature [1, 5–8] explored a great variety of risk assessment frameworks that we divided into the: (1) the qualitative mechanisms; (2) maturity models; (3) standards of risk management or (4) quantitative models. We applied SWOT (strength, weaknesses, opportunities and threats) approach [5] to analyze these researches.

The main strength of qualitative models such as operationally critical threat-asset-vulnerability evaluation (OCTAVE) [14], threat assessment and remediation analysis (TARA) [15], or cyber failure mode and effects analysis [5, 6] are (1) the holistic approach; (2) the simplicity and low cost; and (3) applicability for assessing emerging risks with no or limited statistics. Due to these strengths, these methods are applicable to small and medium IoT projects. Their weaknesses include: (1) qualitative interpretation of risk probability and impact: (2) usage of single point estimates; (3) simplification of the correlations among risks and calculation of aggregate exposure; and (4) absence of linkage between the risk impact and project targets [18]. The resulting threats are risk-acceptance inconsistency, range compression or centering bias [16]. The opportunities for improvements include (1) extensions to quantitative risk assessment; or (2) adding fuzzy logic that improves the integration of the opinions given by experts [4, 17]. Still, these improvements are not sufficient to mitigate weaknesses.

The strengths of risk management maturity models (RMM) such as the capability maturity model integrated or Exostar [5] is providing assessment of maturity of IoT cyber risk management system and identification of the gaps. Their disadvantage is the focus on pointing out vulnerabilities without assessing the magnitude of exposures in these weak spots and the impact on project's targets. The opportunity for RMMs is to be integrated with other approaches.

The strengths of information security standards such as ISO 27001 or NIST [12, 20] are that they (1) are auditable and widely recognized international standards in cybersecurity; and (2) they provide the holistic framework for organizing cyber risk management [5, 12]. However, they do not provide detailed models and tools for risk assessment and the guidance how the models can be applied in risk-oriented decision-making.

Lastly, the stochastic quantitative models (SQM) such as cyber value at risk (CyVAR) use probability theory to estimate the confidence interval of likely losses from cybercrime during the given timeframe [5]. The strengths of SQM are that they provide the quantitative assessment of losses with simulation of a very large number of scenarios. The limitations of existing SQM approaches [1, 5] are that they (1) provide only risk assessment tool but not a holistic risk assessment mechanism; (2) rarely access the impact of losses on project's targets; (3) may result in threats of overlooking of the emerging risks due to lack of data [5]. The opportunity for SQMs is development into full-scale mechanisms of risk management and risk assessment.

To summarize, the existing risk assessment frameworks in cyber area are constrained by a number of critical limitations. We will close these gaps in the research by development of the risk assessment mechanism based on principles of risk controlling.

5 Development of the Mechanism of IoT Cyber Risk Assessment

The developed block diagram of the mechanism is presented at Fig. 2. The prerequisite for applying the mechanism is the cyber risk controlling system in the project company. Such system can be built on the base of ISO 27000 or NIST [5, 20]. In addition, a clear understanding of the company's business drivers, security considerations as well as legal, regulatory and contractual requirements specific to its use of a particular IoT technology is required.

5.1 Mechanism Inputs and Risks Identification Step

The first inputs of the mechanism are business characteristics of IoT device that are necessary for further criticality and vulnerability assessment and calculation of CyROI. The second input of the mechanism is the assessment of the criticality of IoT asset for the project company. We applied additive-multiplicative scoring model for this purpose [21]. The model profiles IoT asset by critical factors in the several dimensions. They have influence on company's key business processes and operations, outsiders (customers, suppliers) and personnel. The others include (1) ties and interdependence with other critical information assets; (2) direct and indirect cost of IoT failure (including reputation, regulatory impact and goodwill); (3) cost of information loss and its recovery; (4) time and cost of asset return to normal operations; and (5) investments into IoT rehabilitation. Behind these, confidentiality, integrity and availability must be also considered [12].

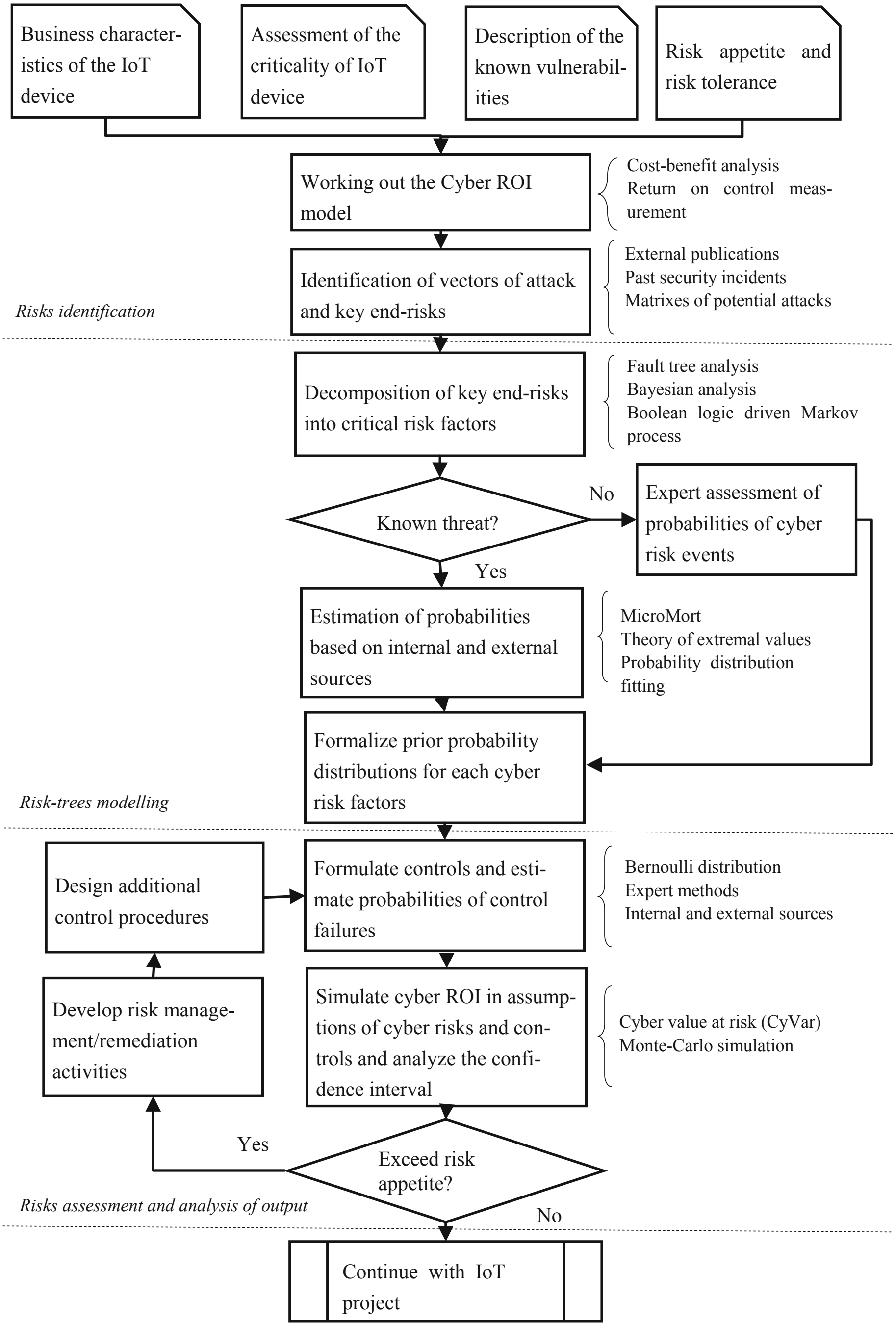
Business characteristics of the IoT device
Assessment of the criticality of IoT device
Description of the known vulnerabilities
Risk appetite and risk tolerance
Working out the Cyber ROI model
Cost-benefit analysis
Return on control measurement
Identification of vectors of attack and key end-risks
External publications
Past security incidents
Matrixes of potential attacks
Risks identification
Decomposition of key end-risks into critical risk factors
Fault tree analysis
Bayesian analysis
Boolean logic driven Markov process
Known threat?
No
Yes
Expert assessment of probabilities of cyber risk events
Estimation of probabilities based on internal and external sources
MicroMort
Theory of extremal values
Probability distribution fitting
Formalize prior probability distributions for each cyber risk factors
Risk-trees modelling
Design additional control procedures
Formulate controls and estimate probabilities of control failures
Bernoulli distribution
Expert methods
Internal and external sources
Develop risk management/remediation activities
Simulate cyber ROI in assumptions of cyber risks and controls and analyze the confidence interval
Cyber value at risk (CyVar)
Monte-Carlo simulation
Exceed risk appetite?
Yes
No
Risks assessment and analysis of output
Continue with IoT project

Fig. 2. The block diagram of the developed risk assessment mechanism

The second input is the results of IoT vulnerability assessment. It is done with application of RMM and vulnerability scanning software [5]. The former benchmarks the maturity of IoT cyber security model against the standards [12, 20], allowing identifying the weaknesses in the security system in general, and the specific areas for scanning and helps to decide on areas of improvement. The scanning software identifies the actual vulnerabilities in the weak spots and helps assessing their severity. The last inputs are the risk capacity (CyROI_T) and risk appetite (CyROI_R) thresholds. The former is the total cyber risk that the company can bear while risk capacity is the level of cyber risks that it can accept. There are characterized by the probabilities of achievements - γ or δ respectively. We set γ and δ at 90% and 95% respectively. After all inputs are collected, CyROI model is worked out with using the formulas (1, 2) and approach [4].

In the next step, the potential vectors of attack and end-risks are identified for each selected vulnerability. This analysis starts from identification of the generic vectors. The sources for this are (1) the publications of reputable organizations such as Verizon's Data Breach Investigation Report, Symantec or FireEye reports [21]; (2) the analysis of the internal or external databases of the past cyber incidents; or (3) expert knowledge. Then, the vectors are customized for the particular IoT and the matrices of potential attacks are formed [21]. The result is the set of end-risks $\{R_i\}_{i \in 1,N}$.

5.2 The Modelling of Risks Trees and Probabilities of Risk Factors

At this stage, each end-risk is decomposed into the key risk factors and for the latter the probability distributions are identified. This is done by the bowtie tree [19] (Fig. 3). The right side of the diagram is the CyROI model developed at the previous stage. The left side of the diagram is the causal network, where the ending node is the end-risk, the leave nodes represent the most credible risk factors (C_i) and conditions to achieve the malefactor's objectives, and the bottom nodes are the initial sets of the cyber-attack.

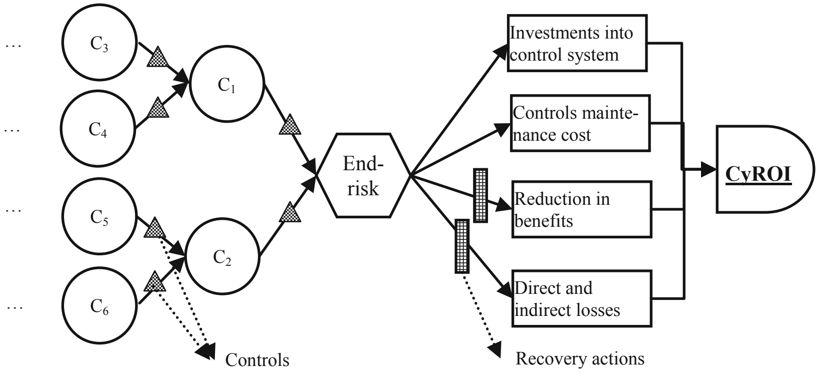
…
C3
C4
C5
C6
C1
C2
End-risk
Investments into control system
Controls maintenance cost
Reduction in benefits
Direct and indirect losses
CyROI
Controls
Recovery actions

Fig. 3. Example of bowtie diagram

To build the casual network the fault tree analysis (FTA) is applied [17]. This can be done with construction of Bayesian network.

$$P(C_1 \ldots C_M) = \prod_{j=1}^{M} P\left(C_j / pa\left(C_j\right)\right) \tag{3}$$

Where M – the number of risk factor; C_j – j-th risk factor, $P(C_1 \ldots C_M)$ – joint probability distribution of all risk factors and $P(C_j/pa(C_j))$ – conditional probability of j-th risk factor given ancestors of C_j; j- the number of risk factor. For bottom risk factors in the tree, the probability distribution function is determined. In rare cases, there are data of sufficient depth and length ($\geq$ 5 years) and there are expectations that the risks will repeat in the future. In this case, distribution fitting technique [5] is applied. The commonly applied distributions in this case are Poisson, Weibull, lognormal or distributions from theory of extreme values.

Often there are very limited internal information about past cyber events or there are some evidence from the reputable sources (such as Cybersecurity, Ventures, Kaspersky Lab, Verizon, Symantec or others), partners, customers or peers. In this case, the MicroMort approach is used [5] and beta probability distribution is applied [18].

$$\begin{gathered} P(X/\alpha, \beta) = \frac{x^{\alpha-1}(1-x)^{\beta-1}}{B(\alpha,\beta)} \\ B(\alpha, \beta) = \int_0^1 t^{\alpha-1}(1-t)^{\beta-1} dt \end{gathered} \tag{4}$$

Where: α – the number of evidences in which the cyber threat was detected in the period, β – the number of evidences in which cyber threat were not detected, P(X/α, β) the probability of cyber threat,

In “zero-day exploit” situation when the new vulnerability is discovered and no data are available, the probability distribution is determined by experts. In this case, the beta-PERT (program evaluation and review technique) distribution is applied:

$$\begin{gathered} P(X/a, b.c) = \frac{(x-a)^{\alpha-1}(c-x)^{\beta-1}}{B(\alpha,\beta)(c-a)^{\alpha+\beta-1}} \\ \alpha = \frac{4b+c-5a}{c-a} \\ \beta = \frac{5c-a-4b}{c-a} \end{gathered} \tag{5}$$

Where, a,b,c – minimum (a), most likely (b) and maximum (c) values that probabilities can take; P(X/a,b,c) – probability of the cyber threat. To calculate the chances (a,b,c) of the “child” risk factor in the tree given the expert assessments of the conditional chances of “ancestors” the log odds ratio (LOR) approach is applied [18].

At the next step, the existing and new cyber security critical controls are added to the tree and probability distributions of each control failure are worked out. The Bernoulli distribution [18] in case of proper statistics or triangle distribution with parameters assessed by experts (in absence of statistics) is the most common in this case. Finally, the correlations between end-risks should be established. These are calculated from the past statistics (if available) or evaluated by experts.

5.3 Risk Assessment and Analysis of Output

Once the previous steps are completed, the Monte Carlo simulation is run. It can be done in MS Excel with installed @risk modelling engine. The outcome of the simulation is (1) a range of possible values of CyROI given risks; and (2) CyROI descriptive statistics. The analysis of the outcome includes assessment of (1) expected variance of CyROI from planned ROI; (2) the most probable value of CyROI; (3) what end-risks and risk factors contributed the most to the deviation of outcome. If the lower bound of δ-confidence interval of CyROI is below $\text{CyROI}_{\text{R},}$ than the possible cyber losses are not acceptable for the company and the IoT project should be abandoned or sent back for rework and remediation of vulnerabilities. If the lower bound of γ-confidence interval of CyROI is above CyROI_{R} but below CyROI_{T} than the possible cyber losses are above the level the company is willing to tolerate. Additional control procedures should be introduced, the reliability of the existing control should be increased and remediation measures against vulnerabilities should be performed. After these measures are taken the Monte-Carlo simulation is run again to ensure that the range conditions are met. Analysis of the output helps to determine: (1) what reserves should be maintained in case of realization of adverse scenarios; (2) what are the key risk areas to concentrate attention; (3) what is the most optimistic and pessimistic scenarios of CyROI; and (4) what contingency plans need to be developed.

5.4 Advantages and Novelties of the Mechanism

The mechanism has important advantages over its peers such as RMM, OCTAVE or CyVAR (Table 1).

Table 1. Advantages of the mechanism over its peers

Peers	Developed mechanism
Qualitative assessment. Risk are single-points estimates with fix-value assumptions	Quantitative risk assessment. generates confidential interval of CyROI
Do not predict the chance of achievement of project's target ROI given cyber risks	Predicts the chance of achievement of project's target ROI given cyber risks
Weak analysis of the impact of each risk factor on potential variances of ROI	Shows the impact of each risk factor on potential variances of CyROI
Limited number of scenarios	Monte-Carlo simulation
Do not estimate the chances of going beyond the risk appetite	Estimates the chances of going beyond the risk appetite and risk tolerance
Difficulties in calculation of aggregated exposures	Calculates aggregated risk exposures given correlations among risks
Weak co-ordination and integration of risk assessment procedures	Integrates and co-ordinates all processes, activities and tools of cyber risk assessment
Do not model the probabilities of control failures	Model the probabilities of control failures
Require the data of sufficient depth and length to quantify the probabilities	Applies MicroMort approach allowing to quantify probabilities with few data points
Often do not provide the holistic approach of risk analysis	Provides the holistic approach of risk analysis

6 The Case Study Example for IoT Cyber Risk Assessment

The case study examines application of the mechanism in the IoT project company that develops preventive equipment maintenance system for the smartphone assembly plant. The project team concluded that the device will be exposed to DDOS attacks, remote malware code execution and related theft of intellectual property and hardware attacks (destruction of sensors). The resulting bowtie diagram is presented in Fig. 4.

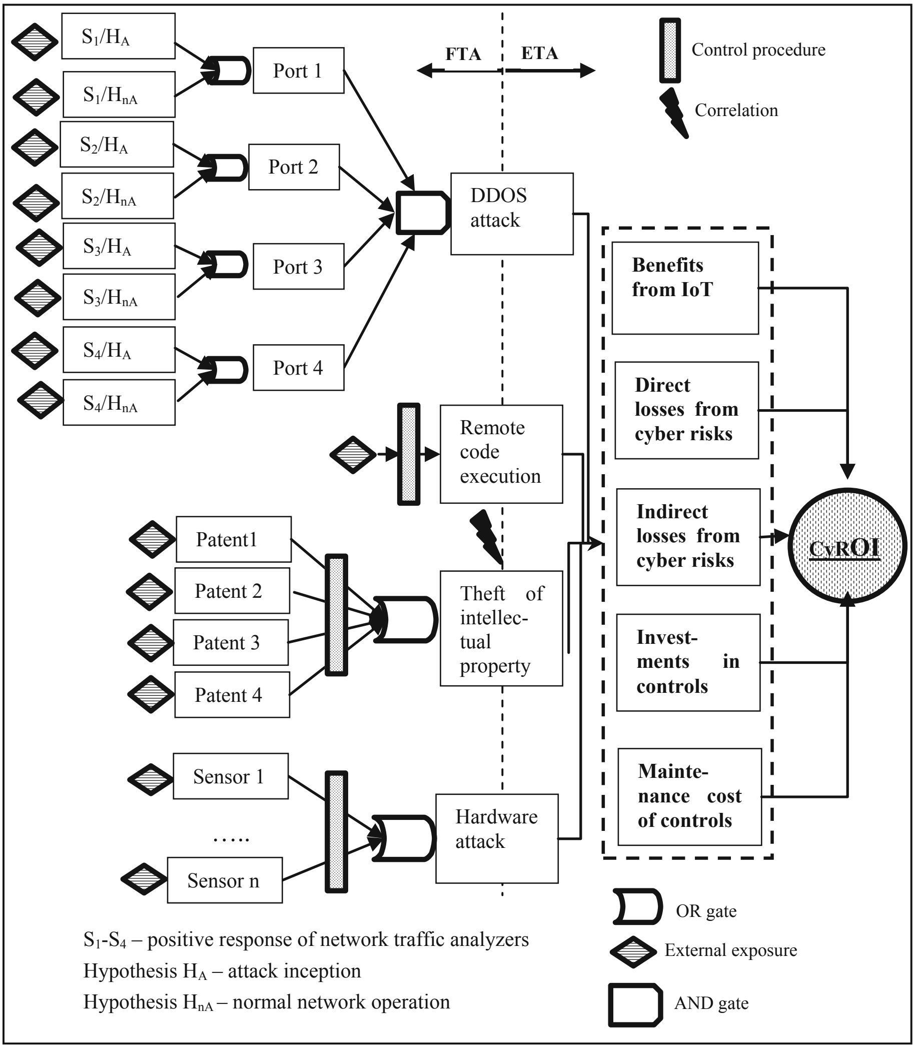

Fig. 4. Bowtie diagram of cyber risks analysis of a predictive maintenance system

To perform the calculations, the project team made following inputs to the mechanism (Table 2).

Table 2. Inputs for the risk assessment mechanism

End-risks	Modelling of probabilities			Modelling of impact
	Prior probabilities of risks	Posterior probabilities of risks	Probabilities of control failures	Probability of impact values
DDOS attack	Beta distribution with inputs from Gartner report	Bayesian network	Bayesian network	Triangle distributions with expert inputs
Remote code execution	Triangle distribution with expert inputs	–	Bernoulli distribution, inputs from internal statistics	Lognormal distribution, inputs from internal statistics
Theft of intellectual assets	Triangle distribution with expert inputs	Application of Boolean algebra	Bernoulli distribution, inputs from internal statistics	Triangle distribution with expert inputs
Hardware physical attack	PERT distribution	Log odds ratio	Bernoulli distribution, inputs from internal statistics	PERT distribution, inputs from internal statistics

The resulted risk CyROI probability analysis charts following the Monte-Carlo simulation are at Fig. 5.

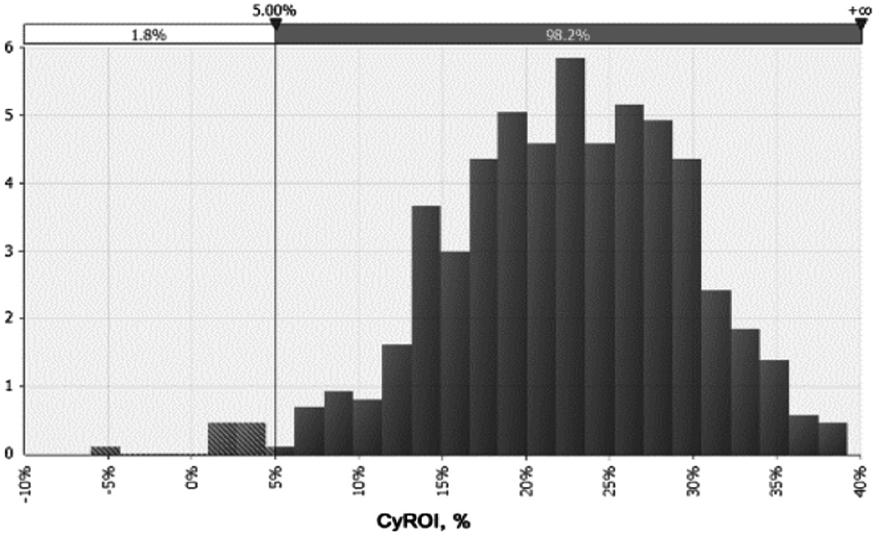

Fig. 5. CyROI probability analysis

Chart demonstrates that despite of potential cyber risk impact there is 98% probability that the value of CyROI will be above 5%. Thus, the developed system satisfies the customers' requirement of not to exceed risk appetite. Moreover, chart demonstrates that planned value of CyROI (10% and more) is not reached with 5% probability and exceeded with 95% probability.

CyROI sensitivity analysis shows the each end-risk influence on CyROI is at Fig. 6.

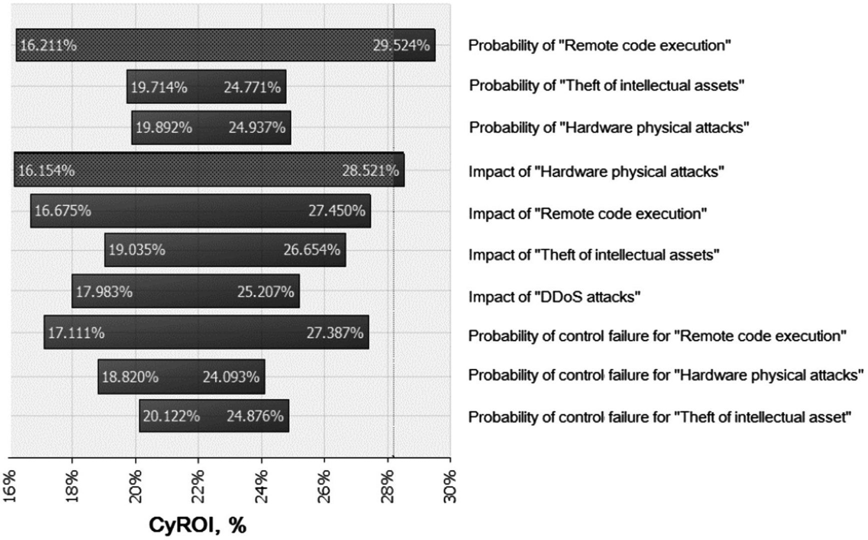

Fig. 6. CyROI sensitivity analysis

The sensitivity analysis helps the designers to develop efficient control and remediation measures. For example, the change in probability of realization risk "Remote code execution" has the most significant influence of CyROI and can cause its deviations from 16.2% to 29.2%. Thus, the control procedures for this event must be focused on the reduction of probability of attack. Conversely, the highest potential losses are from realization of risk "Hardware physical attack". The designers though must create the measures reducing the consequences of the attack, e.g. better protection of sensors.

7 Conclusion and Directions for Future Research

We developed the mechanism for assessing cyber risks for Internet of Things (IoT) projects to address decreasing efficiencies of existing frameworks in this area. The mechanism has advantages over peers. It provides holistic framework to cyber risk assessment; integrates and coordinates all related activities. It contains efficient tools and methods that quantify cyber risks, analyze their impact on project's target, build the distribution of project ROI and analyze the chances of going beyond risk appetite. These advantages make cyber risk assessment dynamic, iterative, responsive to changes in cyber environment and emerging of new threats. The directions of future research will be further elaboration of mechanism's tools such as (1) fitting appropriate probability distributions for different types of cyber risks by the available data; (2) enhancing models for identification attack vectors and evaluation of vulnerabilities; and (3) developing the advanced models of expert opinion calibration and probabilities assessment.

References

1. Abomhara, M., Koien, G.: Cyber security and internet of things: vulnerabilities, threats, intruders and attacks. J. Cyber Secur. **4**, 65–68 (2015)
2. Deloitte Inside. The Internet of Things. A technical primer (2018). https://www2.deloitte.com/insights/us/en/focus/Internet of Things/technical-primer.html. Accessed 2 Mar 2019
3. Glukhov, V., Balashova, E.: Economics and Management in Info-Communication: Tutorial. Piter SPb, St. Petersburg (2012)
4. Grichounine, S.: Developing the mechanism of qualitative risk assessment in strategic controlling. SPbSPU J. Econ. **10**(2), 64–74 (2017)
5. Radanliev, P., et al.: Future developments in cyber risk assessment for the Internet of things. Comput. Ind. **102**, 14–22 (2018)
6. Ralston, P.A.S., Graham, J.H., Hieb, J.L.: Cyber security risk assessment for SCADA and DCS networks. ISA Trans. **46**, 583–594 (2007)
7. Cherdantseva, Y., Burnap, P., et al.: A review of cyber security risk assessment methods for SCADA systems. Comput. Secur. **56**, 1–27 (2016)
8. Nurse, S., Greese, S., De Roure, D.C.: Security risk assessment in internet of things systems. IT Prof. **19**(5), 20–26 (2017)
9. Grishunin, S., Mukhanova, N., Suloeva, S.: Development of concept of risk controlling for industrial enterprise. Organ. Prod. **26**(1), 45–46 (2018)
10. Antonucci, D.: The cyber risk handbook: creating and measuring effective cyber-security capabilities. Wiley, Hoboken (2017)
11. Filko, S., Filko, I.: Risk Controlling of Information Security. Accounting, Analysis and Audit: Theoretical and Practical Problems. SSAU 16, pp. 123–127 (2016)
12. ISO/IEC 27005:2013.: Information technology - security techniques - information security risk management. International Organization for Standardization (2005)
13. Abie, H., Balashingham, I: Risk-based adaptive security for smart IoT in e-health. In: Proceedings of the 7th Conference on Body Area Networks, Oslo, pp. 269–275 (2002)
14. Caralli, R., Stevens, J., Young, L., Wilson, W.: Introducing OCTAVE: Improving the Information Security Risk Assessment Process. Hansom AFB, MA (2007)
15. Wynn, J., et al.: Threat assessment and remediation analysis methodology, Bedford (2011)
16. Thomas, P., Bickel, J., Bratvold, R.: The risk of using risk matrices. SPE Econ. Manag. **6**, 56–66 (2013)
17. Gusmao, A., Poleto, T., Silva, M., Silva, L.: Cybersecurity risk analysis model using fault tree analysis and fuzzy decision theory. Int. J. Inf. Manag. **43**(6), 248–260 (2018)
18. Hubbard, D., Seiersen, R.: How to measure Anything in Cybersecurity Risk. Wiley, Hoboken (2016)

19. Grishunin, S., Suloeva, S., NekrasovaT, T.: Development of the mechanism of risk-adjusted scheduling and cost budgeting of R&D projects in telecommunications. In: Galinina, O., Andreev, S., Balandin, S., Koucheryavy, Y. (eds.) NEW2AN 2018, ruSMART 2018. LNCS, vol. 11118, pp. 456–470. Springer, Cham (2018). https://doi.org/10.1007/978-3-030-01168-0_41
20. Framework for improving critical infrastructure cybersecurity. National Institute of Standards and Technology (2018)
21. Kotenko, I., Chechulin, A.: A cyber attack modeling and impact assessment framework. In: 5th Conference on Cyber Conflict Proceedings, pp. 1–24. IEEE, Tallinn (2013)