Determining Key Risks for Modern Distributed Information Systems

Dmytro Palko, Hrygorii Hnatienko, Tetiana Babenko, Andrii Bigdan

Taras Shevchenko National University of Kyiv, Ukraine

IntSol-2021

International Scientific Symposium «Intelligent Solutions»

Introduction

- Information security management occupies an increasingly important place in the operation of almost any organization that uses modern technologies for collecting, storing and processing information.

- This process is based on periodic analysis of information risks, which allows to identify security threats, vulnerabilities of the information system, implement appropriate measures to neutralize them and, as a result, constantly monitor the state of information security in the organization, given previous experience, new threats and vulnerabilities.

Problem Formulation

- The modeling and forecasting information security risks task has been and remains a significant and priority. This issue is especially relevant in the context of the widespread of complex multi-component information systems that have a distributed nature and contain a large number of nodes.

- Managing the cybersecurity risk assessment in distributed systems involves solving a set of problems related to functional distribution and hierarchy, a high degree of resources parallelization, and a near-complete lack of centralized management.

Problem Formulation

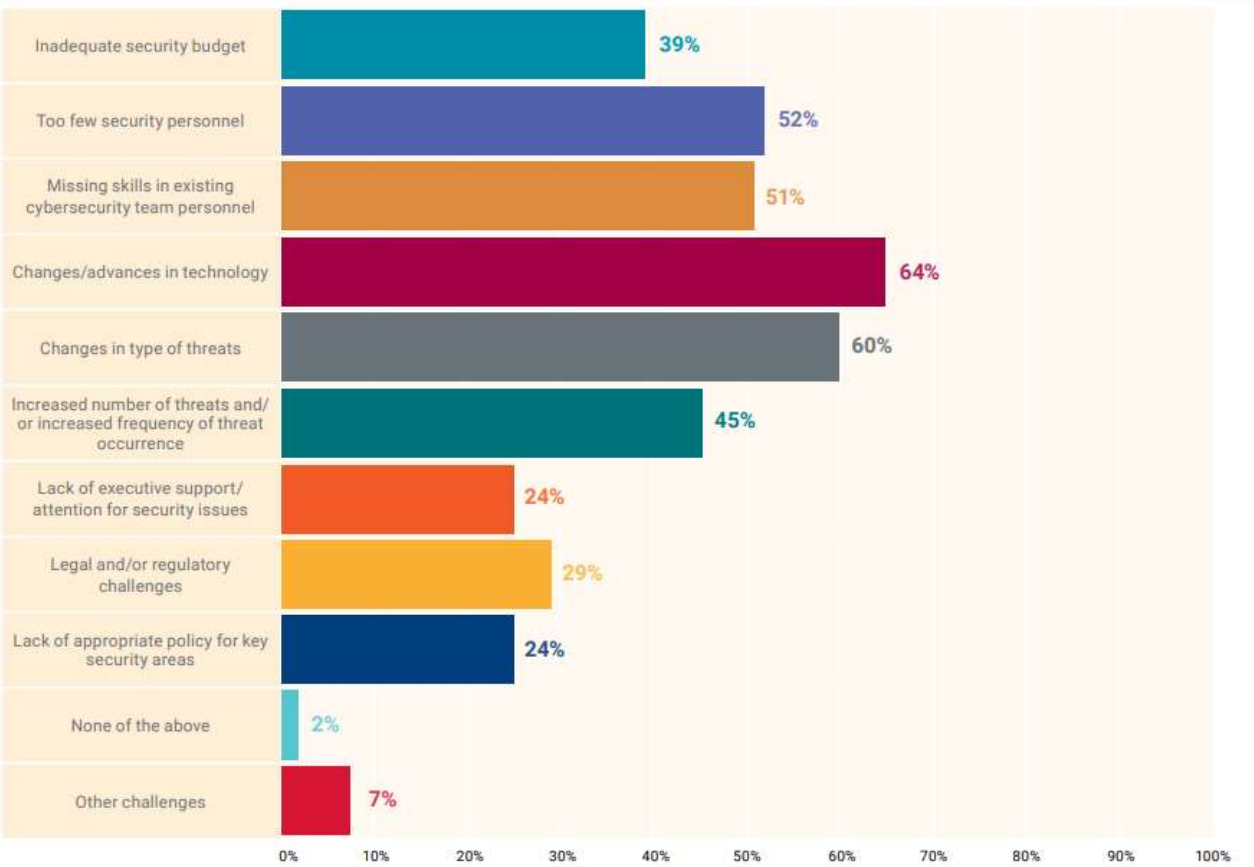

Fig. 1. Cybersecurity challenges today (According to ISACA's annual STATE OF ENTERPRISE RISK MANAGEMENT 2020 survey).

Problem Formulation

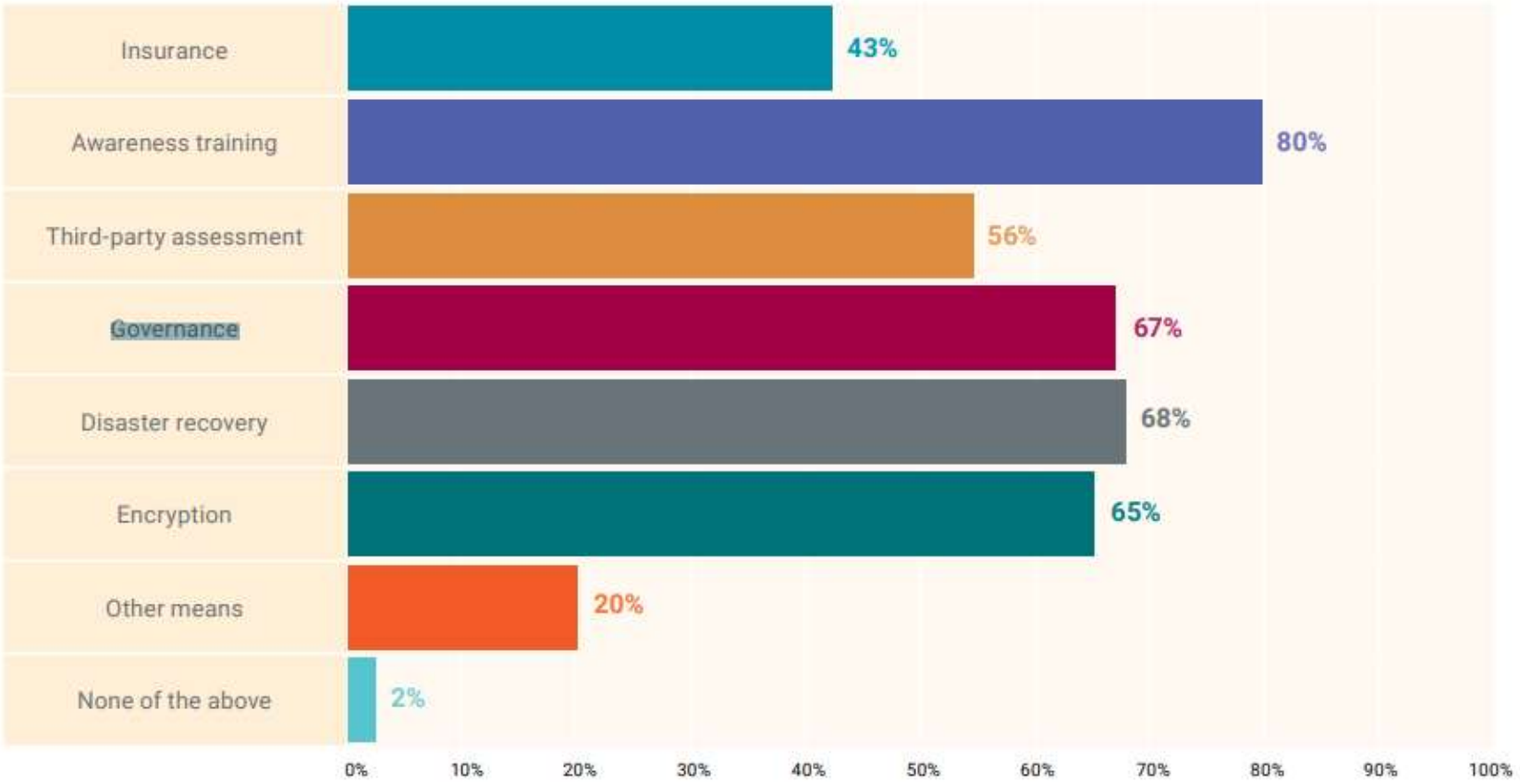

Fig. 2. Top mitigation controls (According to ISACA's annual STATE OF ENTERPRISE RISK MANAGEMENT 2020 survey).

The Research Methodology

The Data Collection Process

The data for analysis was compiled based on the results of interviews and questionnaires of information security specialists with different training levels and different focuses in their activities within this knowledge area.

Table 1
The Survey Participants Classification

№	Categories	Number of respondents	Percentage (%)
1.	Gender		
1.1.	Female	6	26.08
1.2.	Male	17	73.91
	Total	**23**	**100.00**
2.	Position		
2.1.	Information Security Engineer	6	26.08
2.2.	Information Security Auditor	2	8.69
2.3.	Penetration Tester	5	21.73
2.4.	Malware Analysts	2	8.69
2.5.	Infrastructure Engineer[2]	5	21.73
2.6.	Project manager	3	13.04
	Total	**23**	**100.00**

The Research Methodology

Questionnaire Development

- pilot survey (test the research instruments and adjust the questions)
- main questionnaire (mass survey of the target group using the final version of the questionnaires)

Research Criteria and Analysis of the Test Sample

Table 2

Risk Factors and Security Controls Measures Scale

Scale	Risk factors	Security controls
1.	Unimportant	Never
2.	Slightly Important	Seldom
3.	Important	Sometimes
4.	Very Important	Often
5.	Critical	Always

Key Risk Factors

Table 3

Top Security Risks Factors of Modern Distributed Information Systems Based on Researchers

Category		№	Risk factors
Technological factors	Logical (software)	Factor_1	Insecure applications use
		Factor_2	Inadequate patch management
		Factor_3	API vulnerabilities and breaches
		Factor_4	Technical flaws and errors during system design
		Factor_5	Insufficient logging and monitoring
		Factor_6	Broken authentication and session management
		Factor_7	Unapproved third-party software use
		Factor_8	Use of unlicensed software solutions with undeclared capabilities
		Factor_9	0-day vulnerabilities and errors associated with the development of information technology
		Factor_10	Broken access control[3]
	Physical (hardware)	Factor_11	Using outdated hardware and components with known vulnerabilities
		Factor_12	Servers and network appliances security misconfiguration
		Factor_13	Low reliability of the set of hardware and software components, lack of a recovery plan, and periodic backups
		Factor_14	Weak endpoints and network perimeter protection
		Factor_15	Unmanaged IoT and mobile devices
		Factor_16	The imperfection of the organizational structure of the IS, the need for frequent reconfiguration of the IS or its individual parts
		Factor_17	The possibility of information leakage and sensitive data exposure using technical channels
		Factor_18	Insufficient physical access control
		Factor_19	Unauthorized use of the organization's assets
		Factor_20	Lack of protection mechanisms against external network attacks
Organizational factors		Factor_21	Lack of a cybersecurity policy
		Factor_22	Non-compliance with the requirements of standards at the stage of design of the system
		Factor_23	Non-compliance with information security requirements during system exploitation
		Factor_24	Lack of control over information security incidents
		Factor_25	Lack of top management commitment support and involvement
		Factor_26	Lack of security audits
		Factor_27	Lack of antivirus protection policy
		Factor_28	Weak potential to apply existing protection technologies
		Factor_29	Inconsistencies between the infrastructure and the adopted security measures
		Factor_30	The inability to provide the proper level of support and comprehensive development of security systems
Human factors		Factor_31	Actions of unreliable employees
		Factor_32	Unintentional mistakes of service personnel
		Factor_33	Privilege abuse
		Factor_34	The essential list of persons with access to protected information
		Factor_35	Lack of personnel awareness (especially about phishing/social engineering)
		Factor_36	Lack of information security training
		Factor_37	A severe shortage of cybersecurity professionals
		Factor_38	Insufficient passwords hygiene
		Factor_39	Personnel access to potentially dangerous objects in the external network
		Factor_40	Data loss or theft controls lack

Key Security Controls and Risk Management Measures

Table 6
Key Security Controls of Modern Distributed Information Systems

№	Security control	Description
Control_1	Information security policies	controls responsible for implementing and verifying compliance with information security policies
Control_2	Organization of information security	controls responsible for the organizational component of information security measures and the distribution of responsibilities; creation of a management system for initiating and monitoring the implementation and operation of information security in the organization
Control_3	Personnel and human resources security	controls designed to regulate the work of personnel and contractors, identifying their responsibilities for information security both at the stage of the working process and upon dismissal
Control_4	Asset management	controls related to the inventory of company assets, classification of processed information, and media management
Control_5	Logical access control	controls responsible for restricting access to information and information processing facilities, access control policy, rights management for authorized users to systems and applications
Control_6	Cryptography	controls responsible for the proper and effective use of cryptography and public key infrastructure (PKI) to protect the confidentiality, reliability, and integrity of information
Control_7	Physical and environmental security	controls related to the management and prevention of unauthorized physical access, loss, damage, theft or compromise of assets and interruption of the organization's activities, as well as the definition of safe zones, entry controls, equipment security, "clear desk" and "clear screen" policies
Control_8	Operational security	a set of controls for ensuring the correct and secure work of processing information means that combines such activity as change management, backup, monitoring, logging and activity logs management, tracking the installed software and detecting malicious software, monitoring and eliminating identified vulnerabilities
Control_9	Communications security	controls related to network security, network services, information transmission, and messaging
Control_10	System acquisition, development, and maintenance	controls that define security requirements and protection mechanisms in development and support processes
Control_11	Supplier relationships	controls regarding relationships with third parties and contractors, protecting the organization's valuable assets that are available to them and ensuring an agreed level of information security and service delivery under agreements with suppliers
Control_12	Information security incident management	controls related to incident management, events, and information security vulnerabilities, reporting on identified violations, defining responsibilities, response procedures, and collecting evidence
Control_13	Information security aspects of business continuity management	controls that are necessary to ensure business continuity planning, verification and ongoing audit procedures, the availability of resources and information processing facilities, the use of resiliency and reliability principles to ensure security
Control_14	Compliance	controls that require compliance with legal and contractual requirements to avoid breaches of statutory, regulatory, or contractual obligations related to information security, procedures for protecting intellectual property, personal data, and assessing information security at all stages of the life cycle

The Importance of Risk Factors in Lifecycle of Modern DIS

Table 7
Mean Score for Each Risk Factor in Lifecycle of Modern Distributed Information Systems

Category		№	N	Mean	Std. Deviation	% percent
Technological factors	Logical (software)	Factor_1	23	3.043478	0.824525	60.8695
		Factor_2	23	2.826087	0.886883	56.5217
		Factor_3	23	3.695652	0.764840	73.9130
		Factor_4	23	3.739130	0.540824	74.7826
		Factor_5	23	2.782609	0.795243	55.6521
		Factor_6	23	4.217391	0.735868	84.3478
		Factor_7	23	2.695652	0.764840	53.9130
		Factor_8	23	3.869565	0.694416	77.3913
		Factor_9	23	3.826087	0.777652	76.5217
		Factor_10	23	4.173913	0.650327	83.4782
		Total	**23**	**3.4869564**	**0.7435418**	**69.7391**
	Physical (hardware)	Factor_11	23	4.130435	0.625543	82.6087
		Factor_12	23	4.086957	0.668312	81.7391
		Factor_13	23	3.434783	0.895752	68.6956
		Factor_14	23	3.913043	0.792754	78.2608
		Factor_15	23	2.869565	0.868873	57.3913
		Factor_16	23	1.913043	0.733178	38.2608
		Factor_17	23	3.434783	0.843482	68.6956
		Factor_18	23	3.086957	0.733178	61.7391
		Factor_19	23	2.869565	0.757049	57.3913
		Factor_20	23	4.304348	0.634950	86.0869
		Total	**23**	**3.4043479**	**0.7553071**	**68.0869**
Organizational factors		Factor_21	23	4.391304	0.656376	87.8260
		Factor_22	23	2.434783	0.787752	48.6956
		Factor_23	23	2.608696	0.782718	52.1739
		Factor_24	23	2.521739	0.845822	50.4347
		Factor_25	23	2.739130	0.810016	54.7826
		Factor_26	23	2.391304	0.838783	47.8260
		Factor_27	23	3.956522	0.824525	79.1304
		Factor_28	23	2.913043	0.596432	58.2608
		Factor_29	23	2.782609	0.795243	55.6521
		Factor_30	23	3.043478	0.638055	60.8695
		Total	**23**	**2.9782608**	**0.7575722**	**59.5652**
Human factors		Factor_31	23	2.782609	0.599736	55.6521
		Factor_32	23	2.304348	0.764840	46.0869
		Factor_33	23	4.000000	0.738549	80
		Factor_34	23	2.869565	0.548083	57.3913
		Factor_35	23	3.391304	0.782718	67.8260
		Factor_36	23	3.000000	0.603023	60
		Factor_37	23	3.347826	0.884652	66.9565
		Factor_38	23	3.260870	0.688700	65.2174
		Factor_39	23	2.086957	0.668312	41.7391
		Factor_40	23	3.782609	0.599736	75.6521
		Total	**23**	**3.0826088**	**0.6878349**	**61.6521**

Top-10 Risk Factors

Table 8
Top 10 Risk Factors for Distributed Information Systems

№	N	Mean	Std. Deviation	% percent
Factor_21	23	4.391304	0.656376	87.8260
Factor_20	23	4.304348	0.634950	86.0869
Factor_6	23	4.217391	0.735868	84.3478
Factor_10	23	4.173913	0.650327	83.4782
Factor_11	23	4.130435	0.625543	82.6087
Factor_12	23	4.086957	0.668312	81.7391
Factor_33	23	4.000000	0.738549	80
Factor_27	23	3.956522	0.824525	79.1304
Factor_14	23	3.913043	0.792754	78.2608
Factor_8	23	3.869565	0.694416	77.3913

Nearly all respondents ranked factors related to lack of cybersecurity policy, lack of protection mechanisms against network attacks, violations of authentication and session management, violations of access control, and use of components with known vulnerabilities as the most important. These factors should be identified in the process of assessing and managing information security risks and monitored in the future.

Frequency of Controls Occurrence

The generalization of the survey responses, according to the main groups of information security controls of modern distributed information systems in terms of frequency and effectiveness of their use, showed that most of the respondents identified controls responsible for the proper and effective use of cryptography and public key infrastructure, logical and physical access control, operational security and compliance with information security policies as important and most common in practice.

Table 9
The Mean Score for Each Control Factor

№	N	Mean	Std. Deviation	% percent
Control_1	23	4.260870	0.619192	85.2174
Control_2	23	3.391304	0.940944	67.82608
Control_3	23	2.347826	1.070628	46.95652
Control_4	23	3.782609	0.735868	75.65218
Control_5	23	4.304348	0.634950	86.08696
Control_6	23	4.478261	0.593109	89.56522
Control_7	23	4.478261	0.665348	89.56522
Control_8	23	4.260870	0.619192	85.2174
Control_9	23	4.130435	0.625543	82.6087
Control_10	23	3.000000	1.044466	60
Control_11	23	2.086957	0.900154	41.73914
Control_12	23	2.130435	0.757049	42.6087
Control_13	23	2.478261	0.845822	49.56522
Control_14	23	2.782609	0.951388	55.65218

Risk Factors Correlation

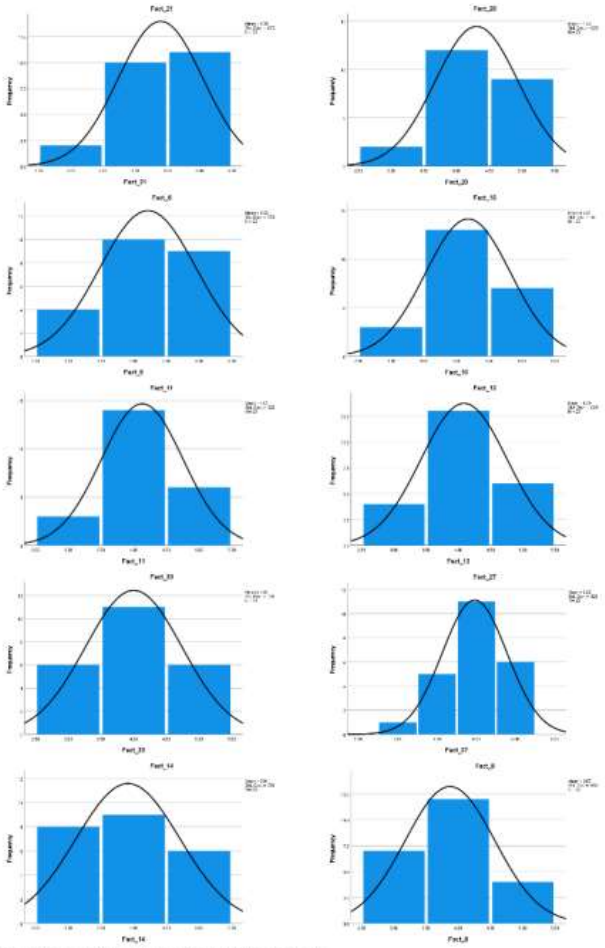

Figure 4: Frequency histograms for key risk factors

Since the volume of the studied sample is small (n<30), all factors are quantitative and the distribution of their values is not normal, it is decided to choose the rank correlation coefficient r-Spearman.

	Kolmogorov-Smirnov[a]			Shapiro-Wilk		
	Statistic	df	Sig.	Statistic	df	Sig.
Fact_21	.301	23	<.001	.760	23	<.001
Fact_20	.293	23	<.001	.771	23	<.001
Fact_6	.248	23	<.001	.798	23	<.001
Fact_10	.301	23	<.001	.788	23	<.001
Fact_11	.322	23	<.001	.778	23	<.001
Fact_12	.291	23	<.001	.798	23	<.001
Fact_33	.239	23	.001	.815	23	<.001
Fact_27	.260	23	<.001	.857	23	.004
Fact_14	.223	23	.004	.807	23	<.001
Fact_8	.270	23	<.001	.804	23	<.001

a. Lilliefors Significance Correction

Figure 5: Test of Normality for Key Risk Factors

Risk Factors Correlation

The interpretation of the correlation coefficient is based on the level of the bond strength:
- r > 0.01 ≤ 0.29 – weak positive connection,
- r > 0.30 ≤ 0.69 – moderate positive connection,
- r > 0.70 ≤ 1.00 – strong positive connection,
- r >-0.01 ≤-0.29 – weak negative connection,
- r >-0.30 ≤-0.69 – moderate negative connection,
- r >-0.70 ≤-1.00 – strong negative connection.

The interpretation of the significance level (p-level):
- if the p-level≤0.05, the relationship between variables is statistically significant;
- if the p-level> 0.05, the relationship between variables is statistically insignificant.

The p-level of correlation is differentiated into three levels:
- p ≤ 0.05 > 0.01 – low statistical significance (*),
- p ≤ 0.01> 0.001 – the average strength of statistical significance (**),
- p ≤ 0.001 – high statistical significance (***).

Table 10
Testing the Hypothesis about the Relationship between Variables Using Spearman's Correlation Coefficient

		Fact_21	Fact_20	Fact_6	Fact_10	Fact_11	Fact_12	Fact_33	Fact_27	Fact_14	Fact_8
Fact_21	Correlation_Coefficient	1.000	.065	-0.95	-.056	-.055	.205	.000	.118	.340	-.251
	Sig. (2-tailed)		.770	.665	.801	.803	.344	1.00	.592	.112	.248
	N	23	23	23	23	23	23	23	23	23	23
Fact_20	Correlation_Coefficient	.065	1.000	.119	.244	.134	.110	.107	-.164	.066	-.528**
	Sig. (2-tailed)	.770		.588	.262	.544	.616	.628	.453	.765	.010
	N	23	23	23	23	23	23	23	23	23	23
Fact_6	Correlation_Coefficient	-.095	.119	1.000	.005	.262	.071	-.069	.123	-.019	-.132
	Sig. (2-tailed)	.665	.588		.983	.227	.749	.755	.577	.932	.548
	N	23	23	23	23	23	23	23	23	23	23
Fact_10	Correlation_Coefficient	.056	.244	.005	1.00	.423*	-.234	.388	-.094	-.309	-.157
	Sig. (2-tailed)	.801	.262	.983		.044	.283	.067	.668	.152	.476
	N	23	23	23	23	23	23	23	23	23	23
Fact_11	Correlation_Coefficient	-.055	.134	.262	.423*	1.000	-.145	.193	.089	.040	-.038
	Sig. (2-tailed)	.803	.544	.227	.044		.510	.377			
	N	23	23	23	23	23	23	23	23	23	23
Fact_12	Correlation_Coefficient	.207	.110	.071	-.234	-.145*	1.000	.086	.183	.354	-.361
	Sig. (2-tailed)	.344	.616	.749	.283	.510		.695	.404	.098	.091
	N	23	23	23	23	23	23	23	23	23	23
Fact_33	Correlation_Coefficient	.000	.107	-.069	.388	.193	.086	1.000	-.200	-.401	.270
	Sig. (2-tailed)	1.000	.628	.755	.067	.377	.695		.360	.058	.214
	N	23	23	23	23	23	23	23	23	23	23
Fact_27	Correlation_Coefficient	.118	-.164	.123	-.094	.089	.183	-.200	1.000	.177	-.026
	Sig. (2-tailed)	.592	.453	.577	.668	.685	.404	.360		.418	.906
	N	23	23	23	23	23	23	23	23	23	23
Fact_14	Correlation_Coefficient	.340	.066	-.019	-.309	.040	.354	-.401	.177	1.000	-.415*
	Sig. (2-tailed)	.112	.765	.932	.152	.856	.098	.058	-.418		.049
	N	23	23	23	23	23	23	23	23	23	23
Fact_8	Correlation_Coefficient	-.251	-.528**	-.132	-.157	-.038	-.361	.270	-.026	-.415*	1.000
	Sig. (2-tailed)	.248	.010	.548	.476	.863	.091	.214	.906	.049	
	N	23	23	23	23	23	23	23	23	23	23

Conclusions

- The results of the study show that all risk factors in the life cycle of a modern distributed system are very important and require detailed analysis and consideration when building a profile of potential threats and assessing information security risks. The importance rating of the risk factors categories by nature can be given as follows (in order of importance): technological factors (logical and physical), human factors, organizational factors.

- The results of the study can be used by managers and information security engineers to assess the importance and probability of potential risks and further prevent and minimize their consequences, as well as build tools for identifying and analyzing the risks of distributed systems based on qualitative, quantitative and intelligent methods.

Thank you for attention !

d.palko@protonmail.com
http://fit.univ.kiev.ua/