INFORMATION SECURITY INSTITUTE

A NEW SECURITY PARADIGM

FOR FINANCIAL INSTITUTIONS

RESOLUTION

LIST OF PARTICIPANTS WE ARE HONORED TO INVITE AS SPEAKERS:

Professor Harvey Wolf Kushner

Chairman of the Criminal Justice Department and a Professor of Criminal Justice at LIU Post, Brookville, New York. Internationally recognized expert on terrorism. Kushner has authored numerous columns, editorials, and six books, five of which focus on the pervasive problems inherent in international and transnational terrorism. His best-seller Encyclopedia of Terrorism has won numerous awards.

Dr. Oleg Maltsev

Author, criminologist, security expert, psychologist, photographer, and investigative journalist. He is a member of the presidium and academic researcher at the European Academy of Sciences in Ukraine (EUASU) and a member of the Ukrainian Academy of Sciences. He is an author of numerous books in areas such as applied history, sociology, depth psychology, philosophy, criminalistics, and criminology. He is an editor of several interdisciplinary peer-reviewed journals.

Professor Kathleen M. Carley

Professor in the School of Computer Science in the Carnegie Mellon Institute for Software Research at Carnegie Mellon University and also holds appointments in the Tepper School of Business, the Heinz College, the Department of Engineering and Public Policy, and the Department of Social and Decision Sciences. Director, CASOS Center at Carnegie Mellon University. Co-Director, Social Cyber-Security Working Group

Massimo Ortolani

Economist and economic consultant. He has been working in the ENI group, Mediocredito centrale and Unicredit group, with assignments mostly focused on international activities, assessment of geopolitical country risk and evaluation of investment projects. He has also worked as consultant in Latin America for UNIDO, and in Kazakhstan within EU programs. During the last decade has been focusing its research studies on geoeconomic risks, also as a lecturer on Economic Intelligence at the Tor Vergata University and Link Campus University of Rome. He is the author of "Economic Intelligence and Geoeconomic Conflict", among many other works.

Oliver Pahnecke

PhD candidate at Middlesex University. He obtained his LLM in International Business Law at Central European University, Budapest, and works as a fair trial expert for international organisations. He works as a rule of law expert for international missions and as a consultant for technical co-operation and finance.

Andrew Hoskins

EUASU Academician, Interdisciplinary Professor of Global Security in the College of Social Sciences, University of Glasgow UK. His latest book (with Matthew Ford) is Radical War: Data, Attention & Control in the Twenty-First Century (Hurst/OUP). He is founding Co-Editor-in-Chief of the Cambridge Journal of Memory, Mind & Media (2021-), founding Editor-in-Chief of the Sage Journal of Memory Studies (2008-), and founding Co-Editor-in-Chief of the Journal of Digital War (2020-).

Prof. Vitalii Lunov

Associate Professor in Bogomolets National Medical University. Presidium member and academician of European Academy of Sciences of Ukraine, Member of the American Psychological Association, the American Academy of Clinical Psychology, World Federation for Mental Health (USA), and the European Academy of Natural Sciences (Hannover, Germany).

Costantino Slobodyanuk

Presidium Member of EUASU. Associate fellow of the Ukrainian Academy of Sciences. Head of the Strategic council of the Information Security Institute. Head of Civil Society Organization Kavalyer. Editor-in-chief of the Newspaper Unsolved Crimes. He is engaged in the studies of online reputation management and security of enterprises.

Olga Panchenko

Corresponding Member of EUASU, attorney, and Director of Redut Law Company. n An associate fellow of the Ukraine Academy of Sciences. Chief editor of the Newsletter on the Results of Scholarly Work: in sociology, criminology, philosophy and political science. Journalist of the newspaper Unsolved Crimes. Presidium member of Odessa Scientific-Humanitarian Society and Historic-Literature Scientific Society.

Pavlo Pedina

EUASU expert, expert in finance, banking, insurance, and asset valuation. Financial consultant. Investment adviser for Slav Invest, financial director of MANORM Holding, and the head of the Paradox Credit Protection Society.

RESOLUTION

"A New Security Paradigm for Financial Institutions"

(27.03.2023)

This document is a summary, conclusions and highlights of the international meeting that took place online on March 27, 2023 on the platform of the Information Security Institute (ISI). The event addressed some of the most pressing issues that relate to security and key vulnerabilities in the financial sector, such as:

1. How cybersecurity should be approached, given the fact that despite multi-million-dollar infusions, this toolkit hasn't solved key issues in the industry?

2. How can social cybersecurity (as a new interdisciplinary research area) help solve the core problem in the financial sector?

3. What could be the model for a new security paradigm in the financial sector? What requirements must be imposed on the new paradigm so that it is error free on the construction stage?

4. What would be a relevant professional development program for CISOs (chief information security officer) of financial institutions?

5. What industries, other than financial, urgently need a similar approach to solve their technological problems?

Today we are at a distinctive point in history, when representatives of the largest consulting companies (McKinsey & Co), the "Big Four" audit companies (Deloitte, PwC, KPMG, EY) and a number of specialized structures (Merrill Lynch, Information Security Media Group, Proofpoint, Cyber Security Hub) are forced to acknowledge that it is crucial to develop a new security paradigm and find ways to decrease the impact of human factor for the effectiveness of business structures. In the subsequent section of the resolution, we will analyze the comprehensive statistical data pertaining to the aforementioned structures.

The International scientific and practical roundtable "A New Security Paradigm for Financial Institutions" has established the essential prerequisites for fostering a productive expert dialogue aimed at addressing the prevailing challenges in the security industry. Furthermore, the timing of the roundtable coincided with two remarkable events in the financial sector. The unforeseen financial collapses of the American Silicon Valley Bank and Swiss Credit Suisse served as an additional indicator of the turbulent state in which the international financial market currently finds itself. Once again, it has become evident to everyone that in today's landscape, no entities are immune, and the human factor can still exert a catastrophic influence on the destiny of diverse business establishments. A succession of errors

committed by personnel at the strategic and tactical management levels can potentially lead towards ruin not only medium and small-scale participants but also formidable giants within the banking sector like Silicon Valley Bank and Credit Suisse. –

The roundtable yielded several key conclusions

Conclusion #1: The integration of programs aimed at mitigating the influence of human factors must be prioritized within the framework of the new security paradigm.

For an extended period, Western security experts have widely embraced the notion of "technology's supremacy over human factors" as an unquestionable principle.

Reality in the field of security demonstrates that without addressing the human factor, technological solutions alone are insufficient to ensure the security of financial institutions. During the roundtable, experts not only reached a consensus regarding the paramount significance of developing a program to minimize the human factor, but also engaged in deliberations on the foundational model for constructing such a program. Notably, **Dr. Oleg Maltsev**, during his presentation, introduced a model comprising three essential elements that must coexist within any organization or business structure to establish a highly efficient security system. These elements are as follows:

Scientific Monitoring: It is imperative to establish continuous monitoring and analysis of the potential criminal environment, ensuring a comprehensive understanding of evolving threats.

Dedicated Training Center: The creation of a separate training center is vital, where experienced managers, independent of public programs, can impart knowledge and skills to employees, fostering a culture of expertise and preparedness.

Regular and Competent Training: The provision of regular and competent training plays a pivotal role. **By prioritizing the competence of individuals, organizations can effectively safeguard against both external and internal threats.** These elements form the foundation for building a robust security system that can proficiently mitigate risks and protect against various security challenges.

Conclusion #2: The new security paradigm necessitates a balanced approach.

Both cybersecurity measures and a system to minimize human errors are central elements. These two components are complementary and should not be treated as mutually exclusive. Any attempt to disrupt this balance would result in a false sense of security, leading to severe repercussions and potential financial collapses.

In his report, **Prof. Massimo Ortolani** from Italy highlighted the following: «*In the fresh investigation survey made by the Italian Association of cyber security companies "CLUSIT REPORT 2023" we can see the following conclusions: it's quite important to find balance between the utmost importance of the human factor and counter cyber-crime efforts that will still have to rely on the use of technology-driven toolkits and of compliance applications*».

Conclusion #3: It is crucial to expedite the development of a practical program aimed at mitigating the influence of the human factor.

The proposed program to minimize the impact of the human factor should adopt a multidisciplinary approach. **Dr. Oleg Maltsev** emphasized in his report that the "*modern security paradigm transcends specialization due to the unpredictable nature of our rapidly transforming world. A security specialist is akin to an intricate and valuable key designed for a complex lock. The career trajectory of such a specialist involves acquiring skills, advanced training, transitioning to the role of a teacher/expert, and ultimately evolving into a scientist. No other security system is effective in today's context.*"

During the roundtable, **Prof. Andrew Hoskins** emphasized the additional threat posed by databrokers, highlighting the need to consider their impact in the development of the program. It is not only a matter of ensuring secure storage and confidentiality of information but also addressing the various methods through which databrokers from the dark industry can influence employees of business structures.

Furthermore, experts reached a consensus that such a program is crucial not only for the banking sector but also for several other market sectors. **Oliver Pahnecke** specifically noted that industries such as the medical industry, education, Big Data Companies, the energy industry, insurance companies, credit unions, and start-ups are particularly sensitive to the human factor. As the program evolves, the list of industries requiring attention is likely to expand.

Conclusion #4: The experts derived three essential requirements to be considered during the development phase of the program.

1.Rejection of mass-market tools: The program should avoid relying on generic or standardized solutions and instead focus on tailored approaches that address the specific needs and challenges of each organization.

2.Strict respect for the balance of interests: The program should prioritize maintaining an equilibrium between the interests of employees and employers.

3.Multifunctionality: The program should not only identify vulnerabilities and concealed threats but also identify areas of potential growth within the company by identifying reliable and promising employees.

The first requirement is directly related to the fact that any mass-market tools in terms of security have the potential of a critical threat. Such mass-market tools, in particular, create favorable conditions for infiltration of unscrupulous employees and representatives of criminal subcultures into the business. As **Professor Harvey Wolf Kushner** noted, *"The security field has changed a lot recently. I know that many collapses in companies are caused by the human factor and the lack of necessary training of employees. That's why the new program needs special tools that are not available to everyone, this is not a mass-market. And I would like to participate in the creation of a system where selection plays the main role. Such a system is needed now for the financial sector, for banks, for the insurance industry, etc. And the most important thing - the emphasis in the system should be on the elimination of the human factor".*

The first requirement directly stems from the understanding that mass-market security tools can pose a significant threat. These tools create an environment conducive to the infiltration of unscrupulous employees and individuals from criminal subcultures into businesses. As **Prof. Harvey Wolf Kushner** pointed out *"there have been notable changes in the security field. Many company collapses can be attributed to the human factor and the lack of adequate employee training. That's why, the new program necessitates specialized tools that are not accessible to everyone, eschewing a mass-market approach. I would like to participate in the creation of a system where personnel selection plays the main role. Such a system is crucial for the financial sector, including banks, insurance companies, etc. And the most important thing, the emphasis in the system should be on the elimination of the human factor".*

The second requirement was formulated by attorney **Olga Panchenko**: *"To reduce the impact of the human factor, it is essential to establish clear guidelines rather than mere recommendations. Concerns may arise regarding the potential violation of human rights and the possibility of discrimination. When it comes to individual responsibility, an individual's activity does not lead to consequences for the collective. But when it is a group tendency, everything changes, i.e., advisory instructions are no longer enough, guiding instructions are needed. The proposed paradigm incorporates these guiding instructions while ensuring a balance between the rights of employees and employers, thereby eliminating any form of discrimination."*

The third requirement pertains to the elimination of bias in the implementation phase of the program within business structures. As highlighted by **Oliver Pahnecke**, the program should serve as a crucial tool not only for owners and top managers to identify existing, hidden, or potential threats related to the human factor, but also as a valuable support system for competent employees. This program should facilitate their upward career progression by leveraging its benefits. It is crucial for the program to be completely neutral in nature, with its primary objective being the reduction of the human factor's impact on the short- and long-term success of business structures.

Conclusion #5: The Human Factor should be viewed exclusively as a system.

During the roundtable, criminologist **Costantino Slobodyanyuk** proposed a four-element human factor system comprising Employee Selection, Insider threats, Behavioral stress, and Human errors. Experts not only endorsed this approach but also reached a consensus that simplifying this holistic system by focusing solely on individual elements would create a false sense of security and potentially result in financial collapse.

Prof. Vitalii Lunov emphasized that the new program would need to incorporate various psychodiagnostic tools, such as psychometric assessments, projective techniques, and skill tests. He highlighted that when considering Employee Selection and Behavioral stress, there exists a correlation *"the greater the hierarchical position of an employee within the company, the greater the need for employing projective techniques to gather objective information for decision-making and implementing necessary adjustments. The employee's level within the hierarchy determines their responsibilities, access to confidential information, and the level of pressure they experience. Hence, it is imperative to utilize both projective psychodiagnostic techniques and skill tests to construct accurate predictive models of employee behavior."*

Statistics and Public Consensus

The acknowledgment of the human factor as a critical issue in the security sphere has been established through a series of reports initiated by government agencies, cybersecurity organizations, financial institutions, CISOs, and analytical and expert companies. The convergence of public consensus on this matter highlights the urgent need for addressing this key problem.

In the current historical context, we find ourselves at a pivotal moment where prominent consulting firms like McKinsey & Co, Big Four audit companies including Deloitte, PWC, KPMG, EY, and specialized entities such as Merrill Lynch, Information Security Media Group, Proofpoint, and Cyber Security Hub, are forced to recognize the necessity of implementing a comprehensive solution to mitigate the human factor. The preparation for the roundtable involved an extensive review of more than 50 reports from diverse organizations. **Financial expert Pavel Pedina** presented the compilation of statistics and analytics during the roundtable:

- 95% of cybersecurity breaches are traced to human error *(**WEF** report "The Global Risks Report 2022");*

- 82% of all breaches involved the human element *(**Proofpoint** "Cybersecurity: The 2022 Board Perspective" report);*

- insider threat incidents have risen 44% over the past two years *(**Ponemon Institute's** "2022 Cost of Insider Threats" report);*

- $4.24 million is average cost of data breaches *(**Ponemon Institute** "2022 Cost of Insider Threats" report);*

- According to a study by **IBM**, 95% of cyber security breaches result from human error;

- *"Human error is the leading cause of financial crime."* This is the main conclusion of the Financial Conduct Authority (FCA) published in the Financial Crimes Handbook;

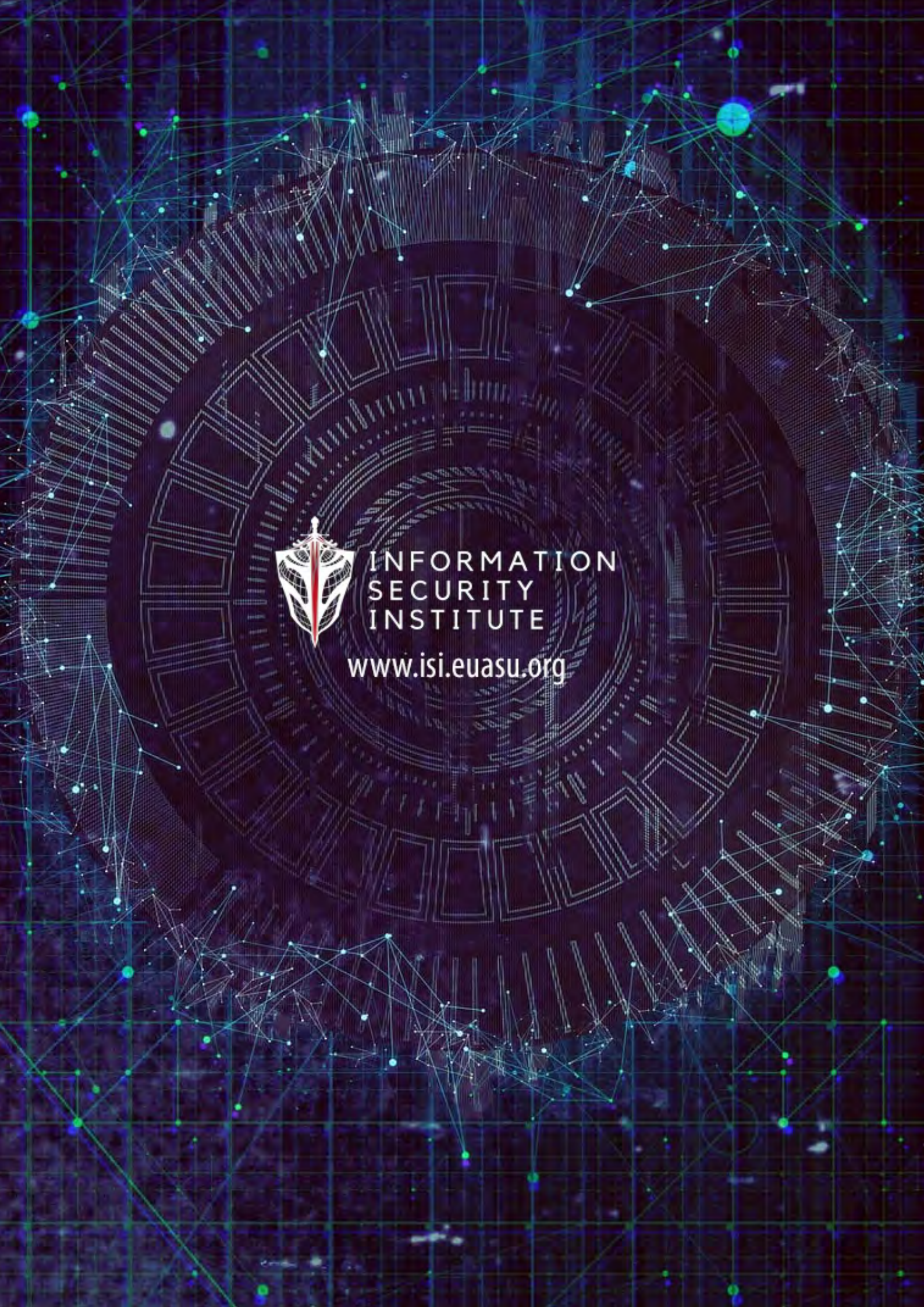
- **McKinsey&Co**: *The rise in cybercriminals targeting employees and insiders, utilizing social engineering tactics to manipulate them into revealing sensitive information or accessing systems, poses a substantial cybersecurity risk for organizations. Employee behavior and insider threats stand out as prominent vulnerabilities that demand serious attention.* (Source: Protecting your critical digital assets: Not all systems and data are created equal (McKinsey&Co)

- **KPMG**: *Financial crimes are often committed with the active participation or complicity of bank employees or by exploiting flaws in internal controls. 88% of financial crimes reported to KPMG involved employee involvement or collusion.* (Source: "Clarity on Financial Crime in Banking" (KPMG)

- **PwC**: "PwC's Global Economic Crime and Fraud Survey 2021. Turning Risk into Resilience" notes that nearly half of all economic crimes are committed by internal actors;

- **Deloitte**: "Financial Crime Risk Management" article notes that insider threats pose a significant risk to organizations.

In light of the above, we are proud to declare that the Information Security Institute (ISI) will undertake the development of a program to reduce the impact of the human factor in the coming months. The expert group leading this initiative will comprise specialists from diverse fields including security, psychology, criminology, criminal justice, information security, mentality and culture, economics and finance, as well as human rights. **Dr. Oleg Maltsev**, the Scientific Director of ISI, will lead the expert group.


INFORMATION
SECURITY
INSTITUTE
www.isi.euasu.org