MOLDOVA CYBER WEEK 2020

MOLDOVA CYBER WEEK 2020
ONLINE CONFERENCE & WEBINARS
Building a strong cybersecurity infrastructure in the New Normal

November 25–27, 2020,
Chisinau, Moldova

UNDER THE PATRONAGE:

GOVERNMENT OF
REPUBLIC OF MOLDOVA

ORGANIZED BY:

Information Technology
and Cyber Security
Service

TECHNICAL UNIVERSITY
OF MOLDOVA

CO-ORGANIZERS:

STRATEGIC PARTNERS:

moldova IT PARK

Tekwill

USAID FROM THE AMERICAN PEOPLE

Sweden Sverige

MAIN PARTNERS:

CISCO

MUK Classics of distribution

PARTNERS:

XONTECH SYSTEMS

THALES

MICRO FOCUS

HUAWEI

it lab

elcore Elcore Distribution

GTB Technologies Data Security that Works™

kaspersky

rapidLINK The best connection ever

MOLDATSA

cooperare germană DEUTSCHE ZUSAMMENARBEIT

Implemented by giz Deutsche Gesellschaft für Internationale Zusammenarbeit (GIZ) GmbH

20 ANI DE COOPERARE ELVEȚIA-MOLDOVA

Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Swiss Agency for Development and Cooperation SDC
Agenția Elvețiană pentru Dezvoltare și Cooperare
Швейцарское управление по развитию и сотрудничеству

simpals

Table of Contents

Mr. Ion CHICU,
Prime Minister of the Republic of Moldova

The global COVID-19 coronavirus pandemic – an unprecedented crisis and one of the greatest tests we are all currently facing - has shaken the very foundations of the infrastructure preparedness. In a rapidly changing world and as the pandemic crisis has taught us, digital transformation is no longer an option. It is a necessity.

Information technology has become vital and an integral part of everyday life. The positive impact of technology on society has brought change and is continuously helping us to reach new heights that have never before been conceived. Along with a series of other benefits, information technology can empower work efficiency and advancement of national and international infrastructure goals in a transformative manner.

COVID-19 pandemic crisis has impacted our lives and changed many daily routines in a considerably short time, accelerating digital transformation and heavier reliance on digital services. While we had to adapt to a new reality, technology has proved to be a useful and necessary tool to help ensure that governments continue to provide essential public services during the COVID-19 crisis. The crisis has strengthened and reshaped our society's dependency on ICT and the Internet due to the more widely adopted remote working and distance learning practices. The importance of largely investing and developing an extensive digital infrastructure became thus imperative, ensuring equitable access to digital infrastructure, which has never been more important than now. The 'New Normal' has brought to light both the advantages of an innovative and robust public administration and the need for thorough understanding and reassessing the implications in cyber security.

The use of digital technologies has profoundly changed the definition of security architecture of our democracies. The cyberspace has become a separate battlefield with cyber-attacks becoming a powerful, low-cost option of warfare. Therefore, cyber security is essential and critical with governments across the world prioritizing the issue of cyberspace, focusing both on developing mechanisms of preventive action and capacity building, as

well as laying grounds for greater cooperation at the international level by addressing mutual concerns and identifying tools for enabling a safer cyber environment for all of us.

One of the lessons the pandemic has taught us is that we can never be fully prepared for such 'Black Swan' events as COVID-19 and that the profound knock-on effects for almost every aspect of our lives and economies are far-reaching. That is exactly why we have to be prepared to adapt and make sure we have a robust cyber environment. The dynamic and fast-moving nature of cyber security is increasing our proactiveness, vigilance and resilience at all levels. It is my strong belief that developing a secure, sustainable and resilient cyberspace requires a multi-stakeholder's approach, bringing together governments, ICT communities, industries, academia, which are essential to building effective resilience capabilities. Despite the current challenges, we can work together as to seize the opportunity.

We must become more agile in adjusting or developing national cybersecurity strategies, as well as legal and regulatory framework regarding cyberspace. More than ever, cyber security requires international cooperation and an increased trust, at all levels, between countries and industries. Collaboration at the policy, technical and law enforcement levels are vital to protect us and allow us to work together to find solutions, by also exchanging knowledge and information to address common challenges. Furthermore, we have to join our efforts to work toward unified awareness campaigns.

In this respect, the **8th edition of Moldova Cyber Week "Building a strong cybersecurity infrastructure in the New Normal",** that has embraced a fully digital format, provides a great opportunity and a platform for an open dialogue on perspectives of cybersecurity in a new reality. As the COVID-19 pandemic accelerates digital transformation, it is essential that we all take a cognizant look at our cybersecurity posture and implement concrete measures aimed at building a stronger level of digital trust and enabling a robust cybersecurity environment in a post-pandemic world as we all walk this path together.

Along this path, it is our common opportunity to grow together by learning from each other and by supporting a cybersecurity community without boundaries. COVID-19 pandemic has revealed the importance of international, cross-stakeholder coordination, building partnerships and developing common approaches to strengthening cyber resilience.

I am confident that Moldova Cyber Week 2020 will contribute to fostering the dialogue and cooperation, as well as raising the cybersecurity awareness in challenging times, but also sharing knowledge and information, exchanging ideas and good practices on ways to continuously improve digital trust across institutions, industries and individuals as cyber security in the 'New Normal' is our shared responsibility.

Mr. Serghei POPOVICI,
Director of the P.I. "Information Technology and Cyber Security Service"

Distinguished officials and dear participants,

I am honored to welcome you to the 8th edition of the "Moldova Cyber Week 2020" event — a high-ranking conference gathering that aims to strengthen collaborations between governments, the private sector, academia and various cyber stakeholders. The MCW 2020 aligns the capabilities and the expertise of participating organizations in various cyber security domains such as incident management, raising awareness of potential threats and presenting remedial solutions. COVID19 presents us with an unprecedented challenge in all areas of digital activity, but Covid-19 has also shown the importance of digital technologies and their capabilities at ensuring reliable supply of essential services, effective governance and power of efficient communications.

The Information Technology and Cyber Security Service is pleased to be one of the organizers of MCW2020 event and we are confident that MCW 2020 shall ascertain the need for a secure cyberspace infrastructure at enabling an environment for the use and implementation of innovative technologies.

MCW is a flagship annual information technology event for the Republic of Moldova in the cyberspace calendar. The event brings together the cyber knowledge experts, practitioners specialists in cybersecurity, policy makers, private and public personalities and external partners who have demonstrated unconditional support and solidarity for MCW 2020. I am convinced that by cooperating with institutional standard bodies and technology providers, the quality and security of IT applications and related products will increase through an efficient and effective process.

The 3-day event aims to bring together the national and international community into an open dialogue and discuss current cybersecurity issues such as: adapting the legislative framework to the new normal, cyber governance and risk management based on the

top threats of year 2020, the definition of critical infrastructure in the new normal, international cybersecurity cooperation, combating cyber fraud, etc. We want to draw upon your learning and knowledge sharing to improve the cyber ecosystem and to develop a national cyber security infrastructure and a culture of cyber security among our citizens. Given the diverse cyber capabilities of specialists in the regional and international context, we in Moldova rely on a coordinated approach.

The initiatives we take are to strengthen the Moldovan cybersecurity capacity at both policy and technical level. We ensure that Moldova is adequately cyber competent at implementing all the necessary measures and regulations designed to promote peace and security in an increasingly sophisticated and hyper-connected cyberspace.

I am confident that the speakers in this 08th edition of MCW 2020 will share their knowledge and experience and enable Moldova to better understand and channelize ideas to navigate more efficiently the challenges of the digital future. We in Moldova are standing firm and want to identify opportunities in emerging technologies and develop the infrastructure, capabilities and relationships at addressing tomorrow's cyber challenges.

Mr. Viorel BOSTAN,
PhD Dr. Hab Rector, Technical University of the Republic of Moldova

Distinguished officials and dear participants,

The impact of COVID-19 has led organizations and their staff to adopt and implement new technologies for continuity of work in a short time frame. As more and more organizations are implementing the online work culture, there is ever more dependence and reliance on computer systems, mobile devices and the internet. This has opened a Pandora's box of new cyber threats, online frauds, phishing and malware activities and loss of personal data.

As more and more of our citizens take - up the online route and undertake work, communicate, shop, share and receive information to mitigate the impact of social distancing, the more the malicious actors are exploiting these new found naive cyber citizens. Cyber security institutions and individuals are required to engage in full cooperation to detect, investigate and keep criminal cyber activity to the minimal.

The increased frequency of cyber-attacks as well as their level of sophistication are deeply disturbing and impacting the economy, finances, governance and our daily lives. Cybercrimes affect one and all, whether it's individuals, businesses, public sector or the non-profit sector. All of these are clear warnings that cybersecurity and cyber threats must be taken seriously and be treated with a high level of urgency and following a systemic approach. We all are required to join hands to safeguard illicit use of cyberspace and its related crimes and promote a sense of national cyber security through the strategic use of cyber security instruments and the collection, analysis and dissemination of cyber intelligence.

The situation requires effective countermeasures, and today I am really glad to see everyone who has joined us - in a completely online format of Moldova Cyber Week (MCW) 2020 event, decided and guided by the "new normal". These hard times have motivated

us to reinvent ourselves and find innovative solutions to face the 'new normal' challenges.

One of the essential and fundamental keys of successful cybersecurity ecosystem is collegial and joint effort between government, industry and universities. These are the reasons why Technical University of Moldova puts considerable efforts to develop its expertise, build successful partnerships with industry leaders, train competent professionals and contribute solidly to new technology developments in this critical field. In this context, it is an honor and responsibility to be the co-organizers of the main cybersecurity forum of Republic of Moldova, Moldova Cyber Week.

Conference Chair, Ms. Natalia SPINU,
Chief of Center for Response on Cybersecurity Incidents,
Information Technology and Cyber Security Service

Welcome to "Moldova Cyber Week 2020"

Over the last 7 years "Moldova Cyber Week" has welcomed more than 250 experts and 4000 participants. Continuing the tradition, this year our team under the 'New Normal' was faced with a dual challenge, the first to make the event online and second making the "Moldova Cyber Week" relevant following the impact of COVID19 on cyberspace. Our team diligently at making the 08th edition of MCW 2020 pertinent and powerful in the national and regional context and curated an event at strengthening the debate in and around cyber security infrastructure.

This year, Covid-19 revolutionized our way of life, societal interactions and came to define a new normal. The cyberspace also became more active with more number of users becoming online, work from home culture taking precedence and cybersecurity encountering new challenges in a fast paced changing cyber environment. We as a cyber security community have been confronted with a new set of challenges and the new normal has made it all the more important to work together in a conducive and constructive manner to tackle these challenges.

The 08th edition of the "Moldova Cyber Week 2020" meets these challenges by bringing together important cyber security stakeholders for the first time in an 100% online event with a clear focus and devotion to the cause of cyber security.

The period from March 2020 onwards has shown that nothing in this world can be taken for granted and the world of cyber security in particular is always evolving with new threats, need for more robust architecture and more investment in better and secure algorithms in cyberspace. The dynamics of the world evolve and mutate in cyberspace and the variables keep changing the equation, thus making cyberspace an ever evolving and challenging problem set. The new normal has made us focus more on creating a unified

co-curated digital development framework, which incubates opportunities and reduces threats and risks in providing the society and all its citizens to work in a secure cyber environment.

For this year's edition of "Moldova Cyber Week 2020" we focus our attention on the new normal. The new normal has redefined our way of working, changed our day-to-day activity set, and brought forth a new set of challenges in cyberspace. Cyberspace and cybersecurity in particular has been at the cornerstone of encountering new challenges with more and more people becoming online and the limits of our critical cyber infrastructures being questioned. COVID-19 has also offered us a new vector of opportunities to develop our cyber security and make it more agile, scalable and cyber malware proof and all that in a matter of five months. Today more than ever each of us need each other's expertise to keep our business afloat, to run our financial institutions and to keep living our lives by meeting the need for essential services in healthcare and education.

"Moldova Cyber Week 2020" embodies deep discussions, practical exercises and a platform to work together in building a strong and collaborative partnership between private and public sector enterprises, governmental institutions and academia in preserving our societal norms in cyberspace for each of our citizens.

I would like to express my sincere gratitude to all the co-organizers, partners and to each and every one who contributed and worked tirelessly in organizing this year's online conference and webinars. Your selfless support, devotion and unequal contribution to the field of cybersecurity is what makes "Moldova Cyber Week 2020" a platform for constructive debates, learnt lessons, insightful keynotes and practical knowledge and experience sharing.

I wish you an enjoyable conference and I strongly believe that our reunion will be useful and will have a positive impact both nationally and internationally, because together we are stronger. I hope that the experience of the 08th edition of "Moldova Cyber Week 2020" will enrich our understanding, knowledge and make us think critically towards a more secure and prepared cyber security architecture and most importantly make us believe in the power of standing together and to face the times that are yet to challenge our cyberspace.

HISTORY

2–3 October, 2013
The 1st edition
“Cyber Security in Moldova: Challenges, Trends and Responses”

15 October, 2014
The 2nd edition
“Cyber Security in Moldova: Challenges, Trends and Responses”

15 October, 2015
The 3rd edition
”The role of the Public-Private Partnership in the field of cybersecurity”

28–30 November, 2016
The 4th edition
“Cyber exercises for people with decision-making functions in the public and private sectors”

21–23 November, 2017
The 5th edition
“ITU Joint ALERT cyber drill for Europe and CIS Regions”

29 October–02 November, 2018
The 6th edition
“Building a Secured Digital Future through Partnership”

19–20 November, 2019
The 7th edition
“Regional Cyber Resilience Forum & Workshops”

Building a strong cybersecurity infrastructure in the New Normal

Launched in 2012, "Moldova Cyber Week" is a large national cyber security event held annually under the patronage of the Government of the Republic of Moldova. This year, the 8th edition of the event is organized by the P.I "Information Technology and Cyber Security Service", Technical University of Moldova, International Telecommunication Union and European Union.

Mission

"Moldova Cyber Week" mission is to create an open dialog between the countries from the region and the international community on issues and challenges impacting and structuring the policies and frameworks on Cybersecurity. The MCW is an inclusive forum, advancing debates, accentuating partnerships between private and public decision makers and creating a deep dialogue platform for inter-governmental and inter-agency policy makers, advisors and the society. The event presents an active participation platform, that integrates enlightening keynotes, in-depth panel discussions, networking opportunities, Q&A sessions and deep dives into actionable insights that strengthens cybersecurity strategies for the future.

Online Conference &Webinars 2020

The year 2020 and the impact of COVID-19 has made organizations adopt multiple technologies such as Cloud, Mobility, Internet of Things (IoT) and this has opened up a whole new avenue for cyber threats and crimes.

Year 2020 has demanded a comprehensive, integrated and critical approach at addressing the cyber security challenges and all that taking into account the remote environment of working. The "Moldova Cyber Week" shall objectively address these challenges in the realm of national and regional contexts and explore further the challenges posed by cyber security in the age of the 'New Normal'.

The MCW 2020 in the New Normal creates a secure space to listen, learn, debate, advise and infer the current global strategic puzzle of Cyber security. The event aims to deep dive into the security challenges presented by COVID19 and how the 'New Normal' in the fast growing digital landscape presents opportunities and new threats in cyberspace.

Agenda

1st Day	Wednesday, November 25
09:00–9:30	**Welcome address** **Cybersecurity Infrastructure in the New Normal**

Cyberattacks are now the fastest growing crime on a global scale. As COVID19's second wave takes shape and the second wave of shutdown is implemented in many of the European nation states - interpersonal interactions have given way to cyber interactions. Our home environments have been transformed to a more digital setting and the onslaught of cyber-crimes and vulnerabilities in the cyber landscape are increasing by the day. The panel presents the new Cybersecurity infrastructure challenges from an industry and the government perspective and brings together experts to discuss some of the fundamental cyber infrastructure changes that the "New Normal" has brought in.

Opening ceremony

H.E. Mr. **Ion CHICU**, Prime Minister of the Republic of Moldova
Mr. **Malcolm JOHNSON**, Deputy Secretary General at International Telecommunication Union
H.E. Mr. **Peter MICHALKO**, Ambassador of the European Union to the Republic of Moldova
H.E. Mr. **Dereck J. HOGAN**, U.S. Ambassador to the Republic of Moldova
Mr. **Serghei POPOVICI**, Director, Information Technology and Cyber Security Service, Republic of Moldova
Mr. **Viorel BOSTAN**, Dr. Hab, Rector, Technical University of Moldova, Republic of Moldova

Moderator: Ms. Natalia SPINU, Chief of Center for Response on Cybersecurity Incidents, ITSEC, Republic of Moldova

9:30–10:00	**KEYNOTE The Threat Landscape of 2020** Mr. **Martin LEE**, Technical Lead of Security Research Talos, Cisco's threat intelligence and research organisation

10:00–11:00 **Panel Discussion Panel Discussion**

Cyber Policy Governance and Risk Management

Organizations are increasingly concerned about threats to data confidentiality, integrity and availability. Compromised data is the biggest risk that organizations face, as data is information and data loss damages the trust and reputation of an organization and brings in big financial losses. Today's pragmatic approach by organizations to address cyber-attacks is good, but it remains to be seen whether such solutions address the problem of pre-emptive cyber threats before they cause too much damage. It remains to be established whether the quantitative estimate of the potential impact (i.e. the risk) is accurate, whether investments for the protection of important assets are appropriate, and whether overall governance of the decision about cyber risk management is optimal. The panel shall address some of the fundamental questions around Cyber governance and risk management.

Speakers:

Mr. **Jaroslaw PONDER**, Head of the International Telecommunication Union Office for Europe

Ms. **Eneken TIKK**, Executive Producer, Cyber Policy Institute, Finland

Mr. **Mihai (Ion) DANTIS**, Expert, European Union Project "Improving Cyber Resilience in the Eastern Partnership Countries (Armenia, Azerbaijan, Belarus, Georgia, Republic of Moldova, Ukraine)", Romania

Ms. **Franziska KLOPFER**, Project Coordinator, DCAF - Geneva Centre for Security Sector Governance, Switzerland

Mr. **Radu STANESCU**, Senior Information Security Consultant, European Parliament, CEO Sandline, Romania

Moderator: Mr. Iulian CHIFU, President, Center for Conflict Prevention and Early Warning, Romania

11:00–11:15 **KEYNOTE**

EU4Digital: Improving Cyber Resilience in the Eastern Partnership Countries

Mr. **Besnik LIMAJ**, Team Leader of the European Union Project "Improving Cyber Resilience in the Eastern Partnership Countries (Armenia, Azerbaijan, Belarus, Georgia, Republic of Moldova, Ukraine)"

11:15–11:45 **KEYNOTE**

Artificial Intelligence and cyber security

Mr. **Mika LAUHDE**, Huawei Global Vice-President for Cyber Security and Privacy

11:45–13:00 **Panel Presentation**

Emerging trends in Cybersecurity, Cybersecurity Challenges and Opportunities

In this panel, the international experts within private sector are invited to share their vision on future of cybersecurity, in order to increase the performance and automation of organizational processes, providing also examples and good practices for addressing cyber risks and threats. Trends and directions in the development of cyber security threats are increasingly difficult to identify, data protection methods and technologies in organizations must be continuously adapted to prevent cyber security risks, and manufacturers of cybersecurity technologies and solutions in the field are the most informed and prepared. for these challenges.

The continuous updating and investment of resources in the right direction of development to strengthen security measures annually saves millions of users, not to mention the colossal amounts of money saved.

Speakers:

Mr. **Volodymyr ILIBMAN**, "How to increase the efficiency and automation of cybersecurity in your organization", Security Account Manager, Cisco

Mr. **Olexandr POGREBNOY**, "Hidden Threats, the most unexpected reasons of information leakage", Solution Manager, GTB Technologies

Mr. **Dan DEMETER**, "APT Threat Landscape of 2020. What should we expect from the future?", Security Researcher, Kaspersky

Mr. **Sergey KUZNETSOV**, "Protecting data in the Digital World - Thales", Regional Director, Thales

Moderator: Mr. Dinu TURCANU, Vice-Rector, Technical University of Moldova, Republic of Moldova

13:00–13:30 **KEYNOTE**

Creating Effective Cyber Security Ecosystems

Mr. **Ramsés GALLEGO**, International Chief Technology Officer, Micro Focus

14:00–14:30 **KEYNOTE**

Cybersecurity in Air Traffic Management

Mr. **Veaceslav FRUNZE**, Acting Director at Moldavian Air Traffic Services Authority (MOLDATSA)

Mr. **Patrick MANA**, Cyber-Security Cell Manager - EATM-CERT Manager at EUROCONTROL

14:30-15:15 **Panel Presentation**

Redefining Cybersecurity of Critical Infrastructures

Critical infrastructure protection is a long-standing priority, but many organizations lag in their response to cyber threats. COVID-19 has broadened the definition of critical infrastructure while also providing a reminder to enterprises to question which systems are essential for their operations. Organizations managing critical infrastructure must develop a proactive cybersecurity posture, but COVID19-led disruptions have heightened this challenge. For example, disruption of supply chains could prove disastrous during an emergency and small and medium scale enterprises may have to shut shop. Thus, new dimensions are being added to the definition of Critical Infrastructure and the pandemic has shown that even personal protective equipment (PPE) could become a part of critical infrastructure during a pandemic. The panel discusses the 'Critical Infrastructure' and its new dimensions and its evolving definition and what it means in the 'New Normal".

Speakers:

Mr. **Roberto SETOLA**, PhD, Professor at the University Campus Bio-Medico of Rome, Director of the Complex Systems and Security Lab

Mr. **Stanislav FESENKO**, Head of System Solutions, Group-IB

Mr. **Alexandru BERTEA**, "Advanced Threat Intelligence in modern Security Operations Centers", Cybersecurity Product Manager, Stefanini Emea, Republic of Moldova

Moderator: Mr. Marwan Ben RACHED, Technical Officer, Cybersecurity Telecommunication Development Bureau, International Telecommunication Union

15:15–15:45 **KEYNOTE**

Strengthening National Cybersecurity

Mr. **Lavy SHTOKHAMER**, Executive Director at Israel National Cyber Directorate

15:45–16:30 **Panel Presentation**

Building a National Cybersecurity Capacity – Lessons from other Countries Regional and International Cybersecurity Cooperation

National capacity building for new and emerging technology is never easy. This is more difficult for a small nation state with limited resources. AI is a broad term with applications to all aspects of human life — economic, social and personal. Key considerations would range from setting a vision and strategy that addresses the economy, Jobs / Workforce, Commercialization, Industrial Automation, Government Systems, national security, law, society, governance and execution. These considerations have known and unknown consequences and internal and external dependencies. Thus, national capacity building is a continuous process especially in context to cybersecurity that is an ever evolving field. The panel presents lessons and learnings from respective countries in the regional and global context and addresses some of the regional and international cybersecurity cooperation impacting National Cybersecurity capacity building.

Speakers:

Ms. **Amy MAHN**, International Policy Specialist, National Institute of Standards and Technology, Applied Cybersecurity Division, U.S. Department of Commerce

Ms. **Brittany A. MANLEY**, "Cybersecurity capacity building and cooperation", Associate Cybersecurity Operations Researcher, CERT Division, at the Software Engineering Institute

Mr. **Adli WAHID**, Expert, the European Union Project "Improving Cyber Resilience in the Eastern Partnership Countries (Armenia, Azerbaijan, Belarus, Georgia, Republic of Moldova, Ukraine)
Mr. **Dan CIMPEAN**, General Director at National Directorate of Cyber Security, Romania
Moderator: Mr. Radu STANESCU, Senior Information Security Consultant, European Parliament, CEO Sandline, Bucharest, Romania

16:30–17:30 **Panel Presentation**

The New Reality Post-COVID-19. Cybercrime and Financial Fraud-Cybersecurity challenges

Cyber attacks in the form of financial losses, reputation damage, loss and compromised consumer data can subject businesses under strict regulations and costly settlements. With the advent of digitization and automation of financial systems, these crimes have become more electronically sophisticated and impersonal. COVID19 have given Cybercrime a new dimension as most businesses have had to go online in a short period of time without adequate security measures in place in order to survive and reach their customers. As stated in the WEF report in 2018 fraud and financial crime is a trillion-dollar industry. COVID19 has made it more lucrative for the cybercriminals and the problem has compounded, advocating for more robust financial instruments to challenge the financial fraud risks. The panel discusses the new reality Post-COVID19 and how financial instruments and institutions would be required to address cybercrime challenges during crises such as COVID19.

Speakers:

Ms. **Monica Violeta** ACHIM, PhD Dr. Hab, Faculty of Economics and Business Administration of the Babeș-Bolyai University and Mr. **Mircea SCHEAU**, PhD in Public Order and National Security, University of Craiova (UCV), "The new dimensions of economic and financial crime in the digital economy", Romania
Mr. **Giorgi JOKHADZE**, Project Manager Cybercrime Programme Office, Council of Europe

Mr. **Mircea SCHEAU**, "Cyber Security Reactivity in Crisis Times and Critical Infrastructures", Cybersecurity Program Manager, Integrated Intelligence, Defence and Security Solutions, Romania
Moderator: Ms. Marina BZOVII, Executive Director of the Moldovan Association of ICT Companies, Republic of Moldova

17:30–17:50 **Closing KEYNOTE**
Securing Tomorrow Today: Critical Investments that Require Time and Attention
Mr. **Keyaan J WILLIAMS**, Founder of Cyber Leadership and Strategy Solutions (CLASS - LLC)

17:50–18:00 **Closing Remarks**

Ms. **Natalia SPINU**, Chief of Center for Response on Cybersecurity Incidents, ITSEC, the Republic of Moldova

Webinars

2nd Day	Wednesday, November 26 | ONLINE

PARALLEL WEBINARS

9:30–9:40	**Welcome address**
9:30–11:00 **Parallel session**	**Protecting Critical Infrastructure with Cisco SecureX Part I** Trainer: Mr. **Pavel RODIONOV**, Security Architect, CISCO

Abstract: The Cisco SecureX platform is a built-in experience within our security portfolio that connects with your entire security infrastructure. It is integrated and open for simplicity, unified in one location for visibility, and maximizes operational efficiency with automated workflows. Cisco SecureX radically reduces threat dwell time and human-powered tasks to stay compliant and counter attacks.

11:15–12:45 **Parallel session**	**Protecting Critical Infrastructure with Cisco SecureX Part II** Trainer: Mr. **Pavel RODIONOV**, Security Architect, CISCO

Our speaker as a Security Architect at Cisco, will give you a practitioner's approach to protect critical infrastructure using the Cisco SecureX platform.

9:30–11:00 **Parallel session**	**Incident Response and Threat Hunting Training Part I** Trainer: Mr. **Adli WAHID**, Expert, the European Union Project "Improving Cyber Resilience in the Eastern Partnership Countries (Armenia, Azerbaijan, Belarus, Georgia, Republic of Moldova, Ukraine)

Abstract: Threat hunting and Incident response tactics and procedures have evolved rapidly over the past several years. Incident response and threat hunting teams are the keys to identifying and observing malware indicators and patterns of activity in order to generate accurate threat intelligence that can be used to detect current and future intrusions. This Training covers the fundamentals of threat hunting; how to build out a hunt program in your own environment; and how to identify, define, and execute a hunt mission.

11:15–12 :45 **Parallel session**	**Incident Response and Threat Hunting Training Part II** Trainer: Mr. **Adli WAHID**, Expert, the European Union Project "Improving Cyber Resilience in the Eastern Partnership Countries (Armenia, Azerbaijan, Belarus, Georgia, Republic of Moldova, Ukraine)

This training introduces essential concepts for network hunting and endpoints hunting and then allows participants to apply techniques to hunt abnormal patterns.

13:30–15:30 **Parallel session**	**Mastering Cyber Executive Leadership** Trainer: Mr. **Keyaan J WILLIAMS**, Founder and Managing Director of Cyber Leadership and Strategy Solutions

Abstract: This learning session will explore four critical areas required for effective leadership in cybersecurity:
(1) governance;
(2) strategic management;
(3) performance measurement;
(4) workforce development.

15:45–17:00 **Parallel session**	**Avoiding Senseless Security Metrics: A new prescription for seeing security information clearly** Trainer: Mr. **Keyaan J WILLIAMS**, Founder and Managing Director of Cyber Leadership and Strategy Solutions

Abstract: The struggle with metrics affects all business leaders who strive to measure and communicate the value of their programs and initiatives effectively. Security metrics are some of the most difficult measurements to communicate because non-technical business leaders and security executives require metrics interpretation that can be communicated to make critical decisions in simple language. This webinar shines a new light onto old security measurements to help our business counterparts see the information more clearly and imply.

13:30–15:30 **Parallel session**	**Advanced Incident Response and Digital Forensics** Trainer: Ms. **Evgeniia LAGUTINA**, ArcSight Presales Consultant, Micro Focus

Abstract: It takes intuition and specialized skills to find hidden evidence and hunt for elusive threats. This webinar encompasses abilities that DFIR community needs to succeed at their craft and confirms that cyber professionals can detect compromised systems, identify how and when a breach has occurred and understand what attackers took or changed, and successfully contain and remediate incidents. The webinar will help you to test and update your knowledge of detecting and fighting threats and how to keep your work role secured.

15:45–17:00 **Parallel session**	**CipherTrust Data Security Platform by Thales: CipherTrust Manager and Transparent Encryption functionality — live demonstration** Trainer: Mr. **Igor AFANASIEV**, Pre-Sales Consultant Russia & CIS, Cloud Protection & Licensing – Thales

Abstract: As data breaches continue at alarming rates, securing sensitive data is critical to all organizations. The CipherTrust Data Security Platform integrates data discovery, classi-fication, data protection and unprecedented granular access controls, all with centralized key management. CipherTrust Manager is an industry-leading enterprise key management solution that enables organizations to centrally manage encryption keys, provide granular access controls and configure security policies. CipherTrust Manager manages key lifecy-cle tasks including generation, rotation, destruction, import and export, provides role-based access control to keys and policies, supports robust auditing and reporting, and of-fers development-and management-friendly REST APIs. CipherTrust Transparent Encryption delivers data-at-rest encryption, privileged user ac-cess controls and detailed data access audit logging. Agents protect data in files, volumes and databases on Windows, AIX and Linux OS's across physical and virtual servers in cloud and big data environments.

3rd Day	Friday, November 27 | ONLINE

PARALLEL WEBINARS

09:30	**Welcome address**
9:30–12:00 **Parallel session**	**Industrial Control Systems (ICS) and SCADA Security** Trainer: Mr. **Dmytro CHERKASHYN**, Coordinator for the Institute for Security and Safety, International Telecommunication Union, Centers of Excellence for cybersecurity in Europe, Security Scientist at Security and Safety at the Brandenburg University of Applied Sciences

In recent years the number of cyber incidents involving a variety of digital industrial systems in the energy, oil, and gas sectors, transportation, production, government, and other critical sectors has dramatically raised. Digitalization and global interconnection make it difficult to operate security measures in an old fashioned manner.
This workshop will provide a comprehensive introduction to ICS cyber security and cover the following topics:

- Introduction to ICS and SCADA technology;
- What is the difference between classical IT and OT/ICS/SCADA in terms of cyber security;
- What to do, if an incident happened despite applied controls.

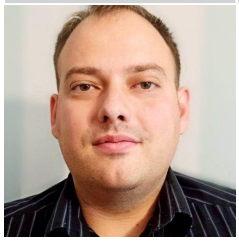
9:30–12:30 **Parallel session**	**Cyber Risk Management in the Information Age** Trainer: Mr. **Mihai DANTIS**, Expert, the European Union Project "Improving Cyber Resilience in the Eastern Partnership Countries (Armenia, Azerbaijan, Belarus, Georgia, Republic of Moldova, Ukraine) Mr. **Radu STANESCU,** Senior Information Security Consultant, European Parliament, CEO Sandline, Romania

It has become imperative for every organization to become aware of all risks inherent in the evolving cyber landscape. The webinar Cyber Risk Management in the Information Age equips you with a comprehensive understanding of how to identify and mitigate vulnerabilities within an organization's networks, systems, and data.

The webinar Cyber Risk Management in the Information Age presents a comprehensive understanding of:

- The local and European laws that require risk management and security measures in place;
- how to achieve Compliance;
- how to identify and mitigate vulnerabilities within an organization's networks, systems, and data;
- practical examples of how to critically analyze an organization's risk profile and gain the skills needed to lead your business / institution through the complexities of the cybersecurity landscape.

12:30–14:00 **Parallel session**	**Data leakage protection — best practices** Trainer: Mr. **Olexandr POGREBNOY**, Solution Manager, GTB Technologies



Barely a day goes by without a confidential data breach hitting the headlines. Data leakage, also known as low and slow data theft, is a huge problem for data security, and the damage caused to any organization, regardless of size or industry, can be serious. From declining revenue to a tarnished reputation or massive financial penalties to crippling lawsuits, this is a threat that any organization will want to protect themselves from.

14:00–15:30	**Up your Yara threat hunting skills – A short introduction on how to identify and classify malware using Yara** Trainer: Mr. **Dan DEMETER**, Security Researcher, Kaspersky, Romania

Have you ever wondered how Kaspersky discovered some of the world's most famous APT attacks? Now, the answer is within your reach. This training will lead you through one of the essential tools for the APT hunter: Yara detection engine. If you've wondered how to master Yara and how to achieve a new level of knowledge in APT detection, mitigation and response, it all breaks down to a couple of secret ingredients. One of them is our private stash of Yara rules for hunting advanced malware. During this training you will learn how to write the most effective Yara rules, how to test them and improve them to the point where they find threats.

International Telecommunication Union - ITU

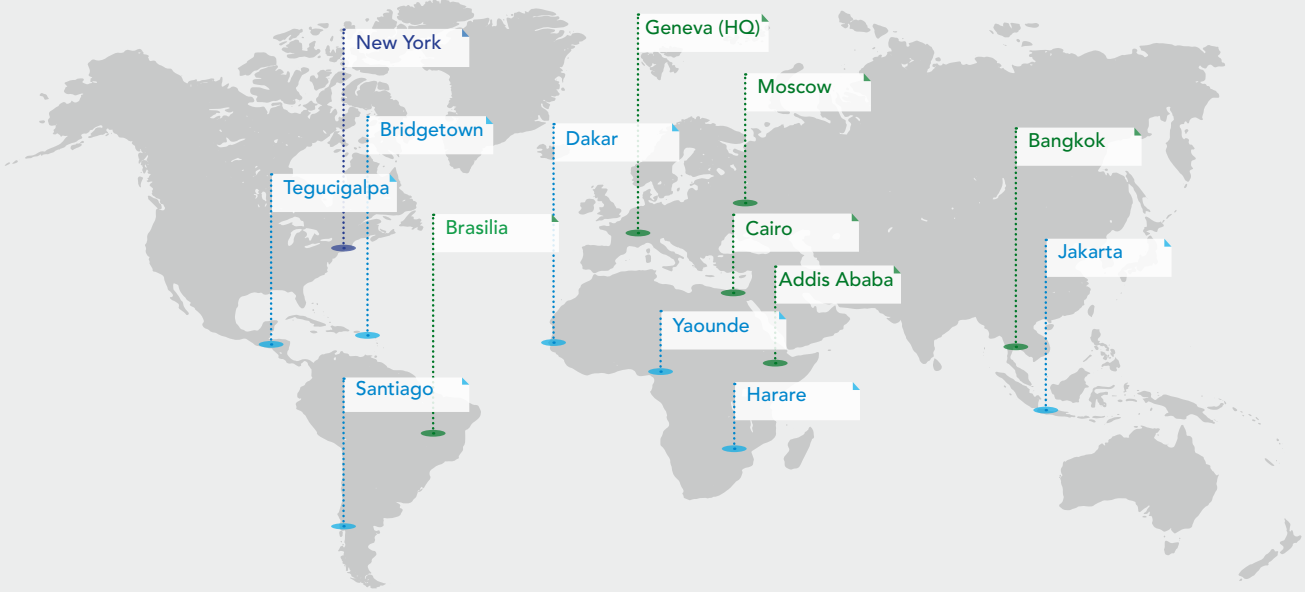
ITU is the United Nations specialized agency for information and communication technologies (ICTs) with a global membership of **193 Member States** as well as some **900 companies, universities, and international and regional organizations.**

GLOBAL PRESENCE

6 Regional Offices

7 Area Offices

Liaison Office with the UN



ITU Telecommunication Development Sector (ITU-D)

ITU has **three Sectors** which work through conferences and meetings.

- **ITU-R** — Radiocommunication Sector
- **ITU-T** — Telecommunication Standardization Sector
- **ITU-D** — Telecommunication Development Sector

Thematic priorities

As an ITU-D member you can also partner with us in activities of your interest that include:

CAPACITY DEVELOPMENT
Building a digitally competent society.

CYBERSECURITY
Creating a trusted cyberspace for all.

DIGITAL INCLUSION
Ensuring inclusive, equal access and use of ICTs for all.

DIGITAL INNOVATION ECOSYSTEMS
Accelerating innovation ecosystems for digital transformation.

DIGITAL SERVICES AND APPLICATIONS
Developing digital strategies and services to transform countries to a digital society for SDG.

EMERGENCY TELECOMMUNICATIONS
Building disaster-resilient ICT infrastructure for reduced loss of lives and damages.

ENVIRONMENT
Creating a circular economy for ICT equipment.

NETWORK AND DIGITAL INFRASTRUCTURE
Providing reliable Connectivity to everyone.

POLICY AND REGULATION
Supporting collaborative policy and regulatory frameworks for digital market development and user well-being.

STATISTICS
Helping countries with evidence-based ICT policy adoption for digitally inclusive societies.

Technical University of Moldova — the only institution of higher engineering education in the Republic of Moldova

Technical University of Moldova was established in 1964, with three engineering faculties. Today, the university comprises 9 faculties with a qualified teaching and engineering staff of over 733 scientific-didactic staff, including about 314 with scientific-didactic titles of academics, habilitated doctors, doctors of sciences, professors and associate professors, lecturers. Today, more than 9,500 students study at the university. The development of the processes of economic globalization and the formation of the United Europe requires the construction of a unique European university space in accordance with the Bologna Process. Aware of the important role of universities in achieving the objectives of the Bologna Process, which have led to essential changes in the mission and priorities of universities, the Technical University of Moldova aims to raise the value of national engineering education by: increasing the quality of education as a determinant of local human potential; the development of scientific-technical research as an indispensable component in engineering professional training; encouraging the mobility of students and teachers; favoring the access and integration of graduates on the local labor market, etc.

The fundamental mission of the Technical University of Moldova is to provide young people with quality studies, combining education, research and innovation that will contribute at building a sustainable society and economy based on knowledge and to shape the student's personality in the spirit of creativity and critical thinking. In order to meet the imperatives of the time, the Technical University of Moldova has structured the study process in three cycles, offering young people a wide variety of study programs in the technical field at cycle I - Bachelor, integrated studies at Architecture, cycle II — Master and cycle III — PhD.

The engineer is the main creative force of society able to make human life more comfortable, and currently, the Technical University of Moldova is the only institution of higher technical engineering in the Republic of Moldova, which trains specialists in the nine

faculties: “Energetics and Electrical Engineering”; “Mechanical and Industrial Engineering, and Transport”; “Computers, Informatics and Microelectronics”; “Engineering and Management in Electronics and Telecommunications” “Technology and Management in Food Industry”; “Light industry”; “Cadastre, Geodesy and Construction”; “Urbanism and Architecture”; “Economic Engineering and Business”.

The Technical University of Moldova is recognized on the stage of national scientific research, with remarkable results internationally. The TUM research centers successfully implement in practice the university’s research strategy within numerous grants and research programs won through competition.

International collaboration in the field of education and research is a priority of the university. TUM has collaboration agreements with about 75 universities in Belgium, Belarus, Bulgaria, Canada, Germany, France, the Netherlands, Romania, USA, Sweden, Ukraine, Spain, Russia, etc. Based on the bilateral agreements, the students from TUM carry out internships in technological practice in European countries, taking advantage of the opportunity to deepen their knowledge in the field of modern languages. The mobility of students and teachers is on the rise and is one of the basic priorities of university life. The Technical University of Moldova has an imposing technical-material base with 315 laboratories, 95 computer-aided design classes. Students are accommodated in 12 student dormitories with medical points, canteens, etc.

Our university is constantly evolving, imposing itself with new standards in education and research, which are gradually disseminated in the process of professional training of specialists.

TECHNICAL UNIVERSITY OF MOLDOVA

Chisinau, Republic of Moldova
168, Stefan cel Mare Bd., MD-2004
www.utm.md
/UTMoldova

Grasping Knowledge Embracing Research Augmenting Innovation

Meeting the imperatives of the time, the core mission of the **Technical University of Moldova** is to provide **quality education.**

TUM combines **practical training and mentorship** for the new generation of **engineers.**

Engineering contributes to building a **secure society** and sustainable economy able to make the human life more comfortable and safe.

Among other areas, TUM ensures professional training of specialists in the top fields of IT, **Cyber Security**, Nanotechnologies, **Digital Communications** and Software engineering.

Study programs in Romanian, **English**, French and Russian

EDUCATION IN CYBERSECURITY

Mr. Dinu ȚURCANU,
Vice-Rector for Informatization, Partnerships, Institutional Image and Communication, Technical University of Moldova

Ms. Rodica BULAI,
University lector, Faculty of Computers, Informatics and Microelectronics, Technical University of Moldova

Mr. Dumitru CIORBĂ,
Dean of Faculty of Computers, Informatics and Microelectronics, Technical University of Moldova

Abstract

The article addresses education as the smartest investment in cybersecurity. One of the most intriguing findings is that 95% of security incidents involve human errors. Most security attacks are concerned with human weakness to attract victims and persuade them to give involuntary access to personal and sensitive information. To eliminate errors caused by social engineering and negligence and to increase users' awareness of the threats, technologies and services should be combined with education. Education in the field of cybersecurity is a necessary consideration for both individuals and families, as well as for businesses, governments and educational institutions.

For families and parents, the online safety of children is of major importance. Equally essential is the protection of information that might affect your personal finances, and precious family assets, such as photos, videos etc. For educational institutions, it is important to understand the link between the online world and the "real" one. Teachers, staff, students, tutors, pupils, etc. should be trained in appropriate on-line behavior to reduce vulnerabilities and create a safer online environment. A better awareness through security education can help enterprises protect their intellectual property and ensure availability of services.

Governments hold an enormous amount of personal data and records of their citizens, as well as confidential government information, which most often serves as a target for

attack. Only through education and awareness, the confidence in public services can be gained. Cybersecurity depends on education.

1. Introduction

We are facing an eyebrow-raising talent shortfall in cybersecurity. The cybersecurity job market, according to a joint report by Frost &Sullivan and (ISC)2, will see a labor shortage exceeding 1,5 million unfilled positions by 2020 [1]. Given the rapid and continuous evolution of threats, it is critical that educational cybersecurity programs share best practices and curriculum updates.

But it is just as important for enterprises — from startup businesses to large corporations, and from small nonprofits to vast government agencies — to do their part. They have the means as well as the critical need to enhance their employees' cybersecurity knowledge.

Even those employees who did arrive with security knowledge have more to learn. The field of cybersecurity is constantly expanding, with more domains to secure and more ways to attack. Intrusions are harder to detect; attackers are stealthier and more evasive.

The best defense is to provide comprehensive education programs for all. You don't have to turn everyone into a cybersecurity expert. IBM, for example, requires all employees to complete digital training each year, which covers matters from secure handling of client data to appropriate sharing on social media sites. Employees can easily learn how to spot and avoid the most frequent types of threats, such as phishing attacks in emails.

Whether taught in a school, university setting or carried out in an enterprise, cybersecurity is a holistic problem and needs a holistic solution. Just as educational institutions start to develop interdisciplinary approaches (such as joint programs between computer science and business, medical, law, economics, public policy, criminology, and even journalism schools), organizations should ensure that their approach to security reaches the people responsible for infrastructure, human resources, data, applications, ethics assurance, management policy, and legal compliance.

There have been technological advancements within the last few years to help secure corporate networks against unintentional, or intentional, risky behavior by users. But while such technical controls and the establishment of sound policies are essential components of effective security, educating, in cybersecurity is one of the best investments a country can make — and a rational recognition that it will take all of us to create a more secure future [2].

2. The initial period — school — acquaintance with the aspects of cybersecurity and safe "surfing" in a virtual environment

The peculiarity of the socio-economic development of the Moldovan economy, and of the world economy as a whole, determines the presence of a significant number of risks, including informational ones, which pose a threat to the stable functioning of any enterprise and person.

These aspects require the formation of an "informational" culture, which should be cultivated in every person, starting from school. These will then develop in the course of evolution at the university and at the workplace. All these steps, in our view, must comply with certain requirements/standards, and with three pillars — three qualities:

a) to study — to explore — to know;
b) to teach — to accustom — to be able;
c) responsibility — consciousness — implication.

So, in school/ lyceum we consider it is necessary to develop and to implement in the following areas: the study of awareness of students about staying safe while surfing the Internet; the familiarization with the rules of safe work on the Internet; the formation of students' informational culture, the ability to independently find the necessary information using web-resources; the discipline training while working on the network.

The trainees should know: the list of the Internet information services; the rules of the safe work on the Internet; and the danger of a global computer network.

The trainees should be able to: responsibly treat the use of on-line technologies; work with web- browser; use information resources; search for information on the Internet.

A good start for the Republic of Moldova is that on June 14, 2018 the Memorandum of Understanding on the development of digital education in general education was signed, and as a result of this agreement the curriculum, the electronic support and the Guide for Students and Teachers of the 1st grade were developed; the virtual library, www.smarte-du.md, was consolidated; funds have been collected for the procurement of 1850 digital tablets in support of each Ist grade teacher across the country. In the 2018–2019 academic year, the "Digital Education" module will be studied by 34,642 students, being compulsory for the 1st grade pupils and optional for those of II–VI grades. In this respect, it is important that Digital Education also develops cybersecurity culture. Analyzing the primary, secondary and lyceum curricula for Informatics, compulsory or optional, we only met in the updated curriculum for the VIIth grade — HOW TO BEHAVE IN THE VIRTUAL SPACE. In

this regard, we consider that cybersecurity education modules must be included in every curriculum of Informatics for all the grades from the I[st] to the XII[th].

The International Center for Protection and Promotion of Women's Rights "La Strada" of the Republic of Moldova undertook a series of actions to create information services for both children and parents/teachers (portal www.siguronline.md). The portal provides young users with the opportunity to access useful information about how to protect themselves from abusive content and actions in the virtual environment, how to develop a responsible attitude to the posted content, and to report possible abuse, while retaining anonymity. The General Prosecutor Office has set up a hotline where virtual crimes can be reported. The Police General Inspectorate has been involved in a number of projects such as, *Together we make the Internet better! An informed child — A protected child* for the protection of children's rights and needs in the Republic of Moldova. We come to realize that we all have a common responsibility to make cyber space safer for everyone, especially for children, namely through information, education and awareness.

3. The transit period — the university — the study and development of the principles and standards to ensure and respect for cybersecurity

Methods and cybersecurity technologies — is the youngest area of IT in our country. The other areas — software, hardware, service — to the contrary, have roots in the "inherited" technologies that were formed several decades ago. Education of cybersecurity can be divided in two directions: the first is future civil servants, whose activities are not focused on the direct provision of cybersecurity, and the second is training future officials, whose activities are directly focused on the provision and supervision of cybersecurity. When forming the list of competencies, various formal sources of requirements that employers can present to cybersecurity specialists were analyzed: legislatively approved qualification requirements of the Republic of Moldova state institutions; requirements for civil servants working in the field of cybersecurity; recently appeared professional standards in the field of IT and IS; various international standards for the protection of information, from which you can learn a lot of valuable information about what different levels specialists should be able to do; regulatory documents existing at enterprises describing the functional responsibilities of such specialists, etc. Education in the field of cybersecurity, in addition to methods and technologies for protecting information resources, always includes the study of means of attack too.

Mass issues on the specialties of the cybersecurity group appeared recently, and only now, the effectiveness of their preparation can be analyzed. The peculiarity of cybersecurity as an educational subject is that it must combine knowledge in the field of natural sci-

ences and technology, as well as in law, management, a number of humanities, therefore, in addition to courses on methods and means of data protection, fundamental mathematical disciplines, advanced IT training, and the study of organizational and legal aspects of ensuring cybersecurity should be included in the limited scope of the curriculum. The complex of technical disciplines for students of the cybersecurity is also optimized — they study various aspects of cybersecurity in the physical environment and the features of the organization of this environment itself, mastering the theory and practice of building computing systems. In addition, graduates of this specialty should be able to solve all organizational issues of cybersecurity, which is also dedicated to a separate discipline. Also, between July 10 and October 31, 2017, a survey was conducted to identify the target professions and training needs in the field of IT security in Moldova. The questionnaire containing 23 questions was completed by 199 companies (the only case in the Moldovan practice when a questionnaire in the field was completed by such a large number of enterprises), IT companies, the provider-companies of electronic communication services and banks, which demonstrates an increased interest from companies in the field of cybersecurity.

Based on this survey, in the recent years, at the Technical University of Moldova, the State University of Moldova, the Academy of Economic Studies of Moldova, and Alecu Russo State University of Balti new learning programs in cybersecurity are emerging.

For the design and development of license and master programs in Cybersecurity, also, an analysis of European curriculum documents has been carried out: European Agency for Network and Information Security (ENISA) — Cyber Security Education, National Institute of Standards and Technology (NIST) for Cybersecurity Education (NICE), Information Systems Security Association (ISSA), Information Systems Audit and Control Association (ISACA), Toward Curricular Guidelines for Cybersecurity (ACM), IEEE Computer Society, etc.

At these universities is conducted the targeted training of specialists for the Central Bank, the Ministry of Internal Affairs, and other state institutions of the Republic of Moldova. This approach has a number of advantages. The organization, recruiting graduates who actively collaborated during the last years of training with the university, receives not only the necessary specialist but also a person whom they already know from both professional and moral points of view, which is important for working in the field of cybersecurity. On the other hand, specialists of enterprises with whom the faculty cooperates, actively participate in the educational process, and this involvement of practitioners in teaching allows maintaining the relevance of the courses. Now there is a technical-scientific center at the Technical University of Moldova. In fact, it has also become the center of crystalliza-

tion of educational processes on cybersecurity — teaching experience is spread through it, advanced data protection technologies being actively developed and introduced into the educational process.

Today, this center is gradually turning into a mini techno park that teaches students and provides various services in the field of cybersecurity, solving quite complex tasks in the development of new protection methods for the state or commercial enterprises.

Such a synthesis of business and education allows the university independently to earn money to improve its educational process, attract highly qualified specialists to teach and improve the professional level of its employees. For higher professional education in the field of cybersecurity, the cooperation with companies, which are developing data protection tools, is vital. For universities, such cooperation is not only an opportunity to get modern equipment and software, but also a way to make students feel the pulse of the industry. For market participants, it is an opportunity to influence the university environment, to help universities prepare really necessary industry specialists. Therefore, university professors and practical workers from the company, highly appreciate the level of theoretical training of specialists in the field of cybersecurity in universities, but note its insufficiency from the practical point of view. The main difficulty that university graduates face in finding employment is the lack of skills in the applied use of their knowledge. According to both teachers and practitioners, close cooperation with companies makes it possible to remedy this situation.

The main objectives of such cooperation programs are: the dissemination of advanced knowledge and experience into the field of information protection from modern computer threats; the support of the most talented students interested in studying cybersecurity issues; teachers' training in the field of cybersecurity, as well as the formation of a platform for the exchange of teaching experience with colleagues; providing affordable antivirus protection for higher education institutions, centers of advanced training and retraining of teachers. Therefore, we believe that the effect brings only an integrated approach to the implementation of the program, which involves a combination of its three main elements: training, research activities and practice. The university partners "Bitdefender", "Endava", "Academia Cisco" provide free training courses, teaching materials, analytical and statistical data, research and reviews of the company leading experts on computer and cybersecurity. Distance seminars are held for teachers and students, master classes and meetings with experts are organized. Under the guidance of experts, students write graduation projects on topics proposed by the company, prepare analytical reviews and articles. Leading experts review all these materials, and the results of the most interesting student studies are applied in the work of the company.

The second line of study at the faculty is cybersecurity aspect of future students whose activities are not focused on the direct provision of cybersecurity. In this case, we consider the method of using the educational-research cryptographic system at the State Engineering University of Armenia, a success [3]. In this respect, TUM initiated a project to develop the Security e-Learning Platform, a teaching-learning tool, individual and distance learning, research and demonstration of real-world security solutions based on case studies. For the start, 5 modules are provided: Criminal Investigation Forensic, Malware Analysis, Reverse Engineering, Clean Code and Capture the Flag (CTF Competition with Various Security Exercises). Such an approach can be used not only by cybersecurity teachers and students, but also by those who do not have a professional background in the field, but intend to study this area whether they are interested in increasing their security skills or to better understand security issues.

With the development of information technologies and the growth rate of their implementation in all socially significant spheres of the society, the problems of information protection become more substantial, which determined the emergence of specialties related to information protection in the list of areas for training specialists in most technical universities. However, knowing the basics of cybersecurity is necessary for almost every user of electronic means of processing and exchanging information. In essence, cybersecurity tends to turn into "third literacy" along with "second literacy" — computer skills and information technology.

To summarize it all we can conclude that the university education in cybersecurity (mostly higher) is not without flaws. According to some representatives of the state institutions, modern education does not meet modern challenges of cybersecurity; graduates are good in physics, mathematics, crypto algorithms, but cannot name the attack vector, the penetration testing methods, not to mention practical skills. It gives the feeling that education in the field of IS got stuck in the 80s of the last century, when the state was in a great need of cryptography specialists; a major bias in the field of fundamental knowledge; the lack of practice (again pen tests and all this here).

4. Reinforcement period — respecting a viable cybersecurity strategy at the workplace

One of the important directions in ensuring cybersecurity is the implementation of it at the workplace in each institution, public or private. You can use advanced software and hardware methods and means of ensuring cybersecurity, write the most correct and complete cybersecurity policies, but without the participation of all the employees of the company/institution, the effectiveness of the cybersecurity framework will be minimal. The human factor is the weakest link of any ISF.

Risks associated with human resources, the so-called personnel risks, are basic for all other types of risks that pose a threat to the stability of an economic entity. Moreover, in the area of risk formation again, the personnel decide everything. The entire enterprise management system directly depends on the personnel management system. The prevention and minimization of personnel risks is the main task in the human resource management process. It is necessary to take into account the fact that the conditions for the occurrence of such risks are present at each stage of the personnel management process.

The process of managing human resources in a company is continuous and is conditionally divided into several stages: the formation of personnel structure, the use of human resources and the release of personnel. Personnel and cybersecurity at all stages should be built at the forefront. The discrepancies between the qualitative and quantitative composition of the staff, the ineffectiveness of the selection procedures are only the main aspects that the organization may face [4]. The fact that the weakest-protected link in any process or system is the human being has been known since pre-computer times. Therefore, among other cyber-criminal situations prevail those in which, as a component of the information system, it is he (the man) who is being exposed. Cyber- criminals are actively using social engineering techniques when attacking him: according to Symantec Corporation, almost 70% of successful attacks are associated with it [5].

Practical implementation of all the provisions of the established cybersecurity policy will require from the company long-term practical efforts. One of the main and most difficult areas of employment is to work with the staff whose goals are the selection and preliminary inspection of personnel recruited (for service); staff training; achievement of mutual understanding of managers and employees in matters of cybersecurity; psychological training in order to withstand the methods of the so-called "social engineering". In one of his books, Bruce Schneier, a well-known cybersecurity specialist, noted that the "mathematical system is impeccable in the general system of cybersecurity measures, computers are vulnerable, networks are generally lousy, and people are just abominable. I have studied many issues related to the security of computers and networks, and I can say that there is no solution to the problem of the human factor" [6]. This statement most clearly and vividly demonstrates the importance of targeted measures for the selection, placement and work with the personnel of the enterprise in order to prevent the creation of "bottlenecks" and so-called information systems and so on; the human factor has not become the most significant source of threats to cybersecurity. The main reason determining the importance of the human factor in the general system of information protection is that, with all the sophistication of modern automation tools, information systems continue to be man-machine complexes and their (systems) functioning depends largely

on the work of individuals. It is for this reason that inadequate treatment of information system components by employees of an enterprise can cause serious damage to cybersecurity even if there are well-developed security policies and highly efficient software and hardware information protection.

In addition to careful selection, one of the important bases for working with personnel is its training in methods of ensuring cybersecurity and safe work with information systems. Training and the subsequent control of the received (available) knowledge can be both primary, and repeated. In general, the employee of an enterprise cannot be allowed to perform his or her duties and work with information systems until he/she has been trained in cybersecurity and will not: be familiarized in details with all the requirements and general applicable rules at the enterprise; be fully trained in the methods and techniques of ensuring cybersecurity necessary for the performance of his/her official duties; be acquainted with all possible measures of responsibility (disciplinary, administrative, criminal) that can be applied to him/her in case of violation of the requirements, as well as in the event of damage caused by his/her fault.

At the end of all preliminary work, the employee must give all the necessary commitments not to disclose confidential information, and testify in written form that he/she is fully familiar with the basic provisions of the security policy. In the course of work, an enterprise may also conduct periodic monitoring of knowledge and skills related to cybersecurity in order to attest to the competence of employees in this field. In addition, one of the training tools may be periodic staff familiarization with actual examples of recent incidents related to cybersecurity. Besides, additional training of enterprise personnel can be carried out in the following cases: the introduction of new automated information systems; changes in business processes of the enterprise; changes in security policy requirements (for example, due to changes in legal requirements).

The need for additional training in the implementation of new information systems and, in particular, integrated enterprise management systems, as a rule, may be due to the emergence of new software functionality and changes in information processing procedures. Also, the access to integrated information systems can potentially give access to previously inaccessible information and provide previously unavailable opportunities to influence various information flows. In this regard, it may be necessary for employees to make additional commitments to comply with cybersecurity measures. Similar organizational measures, to ensure the protection of information, may be necessary when changing the enterprise business processes, when its structure changes, the distribution of functions between departments and employees' duties, and accordingly, changes are made to organizational charts, staffing tables and job descriptions of personnel. Changes

in security policy requirements can be associated with the emergence of new threats, changes in legal requirements, expansion of markets, changes in the attitude of management and owners of the company to cybersecurity issues and other factors — all these clarifications and changes must also be fully and promptly communicated to staff.

In the process of learning, a clarification of rational reasons for which the company applies such a security policy may have some significance. This can serve both, better to understand and assimilate the positions of the security policy, as well as to relieve some of the psychological tensions that inevitably arise when taking restrictive measures and imposing additional duties, the necessity of which is not always obvious and understandable to ordinary employees and specialists.

A separate area of ordinary training and advanced training can be the development of company personnel skills to counter the methods of so-called social engineering (this approach is also sometimes called "sociotechnics"). The use of social engineering methods for illegal entry into information systems is associated with the so-called "human factor", which is a combination of certain psychological inclinations and characteristics of thinking and behavior, which are peculiar to almost all the people. To the number of such propensities and features can be attributed: inability to adequately assess the danger in some situations; specific relation to rarely occurring events (dulled attention); excessive trust and reliance on automation; susceptibility to manipulation, based, for example, on the desire to help people (including strangers) or on excessive trust to people dressed in a special uniform, etc. [7].

To minimize the risks associated with human factors, it is necessary to organize a documented and approved work of the staff by the bank/company management towards awareness increasing and training in cybersecurity, including the development and implementation of plans, training programs and awareness-raising in the field of cybersecurity, as well as monitoring the results of the implementation of these plans. Education of the personnel in the field of cybersecurity is necessary for the following purposes: developing and maintaining awareness among employees of the importance of safety in the use of information technologies, knowledge of the procedure for handling undesirable events and incidents; awareness of the employees of their role and place, as well as the duties and responsibility for ensuring the protection of information in the company; increasing the level of knowledge by employees of the basic rules of cybersecurity; communicating to employees the main positions, restrictions and requirements of existing documents (policies) in the field of cybersecurity; bringing to employees facts about which cybersecurity tools are used, as well as how to use these tools correctly and effectively. The need to train and raise awareness of cybersecurity personnel is governed by the GD No. 201

Mandatory Cybersecurity Requirements of 03/28/2017, which requires public institutions to implement the Cybersecurity Management System. The head of the authority shall designate by administrative act the person (subdivision) responsible for the implementation of the cybersecurity management system in the institution and the responsible person shall be required to participate, at least once a year, in cybersecurity training courses and, respectively, to organize courses for the employees of the institution.

Cybersecurity education should include the following areas: raising awareness of workers in matters of cybersecurity (general course); safe work with personal data in the company; organization of business continuity and recovery after interruptions. The main forms of education can be individual training (introductory, repeated and extraordinary briefings); special training with the involvement of external training centers; awareness raising: distance learning, social engineering methods (memos, posters, screen lockers, etc., reflecting all the requirements of the enterprises' regulatory documents on cybersecurity).

In accordance with the State Norms of Moldova, training and awareness plan requirements should be established for the frequency of training and awareness raising.

Unfortunately, a survey conducted last year on a sample of about 160 companies and institutions within a project to raise IT needs to increase cultural information and cybersecurity in Moldova shows that companies and institutions do not pay suffice important to cybersecurity (62% of respondents) and that they have a training program and awareness on cyber security (81% of respondents).It is also necessary to determine the list of documents that appear as evidence of the implementation of training and awareness-raising programs in the field of cybersecurity. Individual training (instruction) should be completed with an oral survey, and an assessment of the acquired skills of safe ways of work. The employee who conducted the briefing checks the knowledge. With a distributed institution structure, it makes sense to impose responsibilities for training and awareness raising in the field of cybersecurity to a special employee appointed in each remote unit. As part of the self-assessment, the internal auditors of the institution should regularly monitor the level of awareness of employees of the audited units, the completeness and accuracy of the training documents, the timeliness of communicating new cybersecurity requirements.

The cybersecurity service should monitor the effectiveness of training by quantitative and qualitative analysis of the actions of employees, followed in response to certain events. The training system under consideration is a scalable process aimed at constantly improving the level of knowledge, skills and qualifications in the field of cybersecurity of employees and integrates with existing business processes. As a result of the introduction of a training system and raising awareness in the field of cybersecurity in an institution, the

number of incidents in this area related to human factors will be significantly reduced, as well as the misuse of resources.

Success and high security, including cybersecurity provides a continuous process of education and training of personnel in the field of cybersecurity. Training can be carried out in some areas and forms. Namely, the Complex Program: full-time courses; E-courses; Introductory briefings; posters; screensavers; animated and video clips; computer games; booklets, brochures, memos; souvenirs; efficiency mark, a comprehensive program to improve awareness of the company's staff. What is good about an integrated approach in addressing issues of raising the awareness of company personnel in matters of cybersecurity? — It guarantees a high level of security of the company information resources; involves staff training cybersecurity on an ongoing basis; helps to manage the risk more effectively; has a positive effect on the company image; testifies to a high level of responsibility of the company management towards its employees; helps to prevent losses that are inevitable when staff of the company violates cybersecurity.

Introductory briefing for new employees. The familiarization with corporative security regulations for hiring is an important step towards conscious and strict adherence to corporative security rules by company staff. There can also be developed: an e-learning course on the rules of corporative security adopted by the organization; tests to check the level of knowledge of the company staff; educational flash and video clips on corporative security rules; illustrated memos on the main issues of the corporative security.

Posters. Thematic posters about corporative security issues are one of the most effective means of maintaining an atmosphere of corporative security and building a corporate culture of personnel on working safely with the company's information resources. Posters placed in all places accessible to the personnel of the company make it possible regularly to remind about the rules and requirements for ensuring corporative security adopted by the company.

Screensavers. The installation of corporative security screensavers is an effective way to remind the staff about the company's corporative security rules and regulations. It is recommended to update screensavers every 2 months to increase their effectiveness.

Animated and video clips — a bright and visual tool that allows in an attractive, unobtrusive way to convey to staff the rules and regulations for working with information resources of the company. Creating a corporative flash video on security issues: the flash

movie script is developed in accordance with the organizational and administrative documentation of the institution in the field of corporative security and the corporate culture adopted by the company. The recommended duration of a flash movie is no longer than 1.5 minutes. The film assumes the use of announcer dubbing, including staged scenes with the involvement of actors, graphics. The shooting is carried out using professional equipment on the territory of the institution. The recommended duration of the video — 15–20 minutes.

Security Competitions (Cyber Drill, CTF**) or Computer games.** We offer a new look to the problem of compliance with the cybersecurity rules adopted by the company and to invite colleagues to participate. An entertaining cybersecurity quest is the best way to convey to employees the most important skills and knowledge.

In 2018, Information Technology and Cyber Security Service, in collaboration with European partners, Technical University of Moldova and some Moldovan private companies, managed to organize several Cyber Drill sessions for security officers from national companies and institutions. Also, the Technical University students organize annually CTF competitions and also participate in the international ones (Suceava, Bucharest, Volga, etc.)

Booklets, pamphlets, memos — are a convenient way to inform new employees about the company rules and regulations on corporative security. The memo written in simple, accessible language, the content of which reflects the main provisions of the safety regulations, is easy to use, has a bright, attractive aspect.

Evaluating the effectiveness of implementing an awareness-raising program is a very important phase of the awareness program. It is advisable to evaluate the effectiveness of the program after the staff has been trained and a number of measures have been implemented to maintain the corporative security atmosphere in the company. As part of the events, aimed at assessing the effectiveness of implementing an awareness-raising program. In this regard, you can send authorized provocative messages by corporative e-mail and SMS / MMS, which motivate users to violate corporative rules and corporative security policies. The purpose of the work is to assess the implementation of basic corporative security rules by employees when using corporate e-mail and business cellular communications, in order to improve the program for raising awareness of corporative security issues. In the framework of the work implementation to achieve the stated goals, the tasks of checking the elements of the program of raising awareness on the following issues are solved: password policies; compliance with license fairness; anti-virus attacks;

complying with the rules of the IT services use in terms of the e-mail and the Internet utilization; abidance with cybersecurity rules when using service mobile devices and service cellular communication. Typical ways in which an enterprise can constantly remind its employees of the need to be careful are: placing and periodically changing (updating the design and content) reminders of the need to comply with the requirements of cybersecurity policies on items constantly in sight of employees during the working day: wall and desktop calendars, coffee mugs, covers of notebooks, desk exhibits, pens, pencils and other stationery; periodic emailing of relevant messages; use of screensavers containing relevant reminders; use of voice mail and speakerphone for periodic transmission of messages about the need to comply with cybersecurity rules, etc. [8].

Conclusions

We need to make security more of a realistic notion for the general public. A lot of users do not necessarily know where their data go. Rather than just corporate security awareness training, as professionals, we need to be bringing cybersecurity culture into the home as well. Cybersecurity truly is a public safety issue. We have seen weaponized social media posts, IT devices turning into attack droids, and phones being hacked to see GPS locations. These issues are everyday occurrences. Therefore, we need to regulate the idea of security into our everyday culture, exactly the way we have normalized other safety issues. It could be illustrated by a simple example with cars. When it was found that the cars were unsafe, the seat belts were added. For the Internet, we need a security-focused and educational mindset. This is especially the case in regards to innovations within technology. A scary awareness video is insufficient. In contrast, cybersecurity should be an ongoing education. The more we equip the public with this knowledge, the more efficient we will be in the future [9]. We would like to note that one of the main qualities that should be developed starting from school and cultivated at all subsequent stages is consciousness and awareness that a person is part of a whole class, group, working team, and that success, prosperity and security depends on his intellectual, spiritual and physical contribution. By instilling a sense of consciousness, the person will rejoice with all his might for the work that he is doing, and this is the best guarantee that cybersecurity and success in any business will be achieved.

References

[1] HAIBER, O. and MORRILL, S., Passport to the Future: A Secondary School Cyber Education Case Study, https://www.uscybersecurity.net/csmag/passport-to-the-future-a-secondary-school cyber-education-case-study/

[2] IVEROS, M., Cyber Security Depends on Education, https://hbr.org/2013/06/cyber- security-depends-on-educ
[3] Геворг Маргаров, Воспитание защитников информации, https://www.osp.ru/os/2009/04/ 9298350
[4] Анастасия Богатырева, Кадровые риски, https://bisjob.ib-bank.ru/publikaciya/104
[5] Валерий Васильев, Дмитрий Сергеев, Человек — самое слабое звено в ИБ, http://www. infosecurity.ru/_gazeta/content/100305/art3.shtml
[6] Шнайер Б., Секреты и ложь. Безопасность данных в цифровом мире, СПб.: Питер, 2003.
[7] Александр Анисимов, Менеджмент в сфере информационной безопасности. Департамент информационной безопасности и работа с персоналом, http://www.intuit.ru/studies/courses/563/419/lecture/9580?page=2
[8] MITNICK, K. and SIMON, W., The Art of Deception: Controlling the Human Element of Security, Indianapolis (Wiley), 2002.
[9] TRICIA A. H., Cybersecurity Culture: The Root of the Problem, https://www.uscyber security.net/cybersecurity-culture/

Take your network to where the data is.

Accelerate to multicloud with Cisco ACI.

cisco

MUK
Classics of distribution

Assistance in projects by email cisco@muk.md

ABOUT THE FUTURE OF SECURE REMOTE WORK REPORT

In February to March 2020, organizations sought to protect their workforce by mandating and enabling their employees to work from home. While necessary for protecting people and communities, this experience physically separated security professionals from their own teams, from the employees who depended on them, and from the critical systems they were responsible for. The remote work arrangement also placed greater strain on existing digital policies and business continuity planning during an already stressful time.

That's not to say that we couldn't find ways to adapt to this new way of working. In the spirit of this reality, more than 3000 IT decision makers from small to large organizations were surveyed from June 16 to September 4, 2020, across a spectrum of 30 industries, including financial services, healthcare, architecture, transportation, etc., to understand how they have been impacted by the COVID-19 crisis from a cybersecurity perspective.

3196 respondents in **21** markets

AMER:
- Brazil
- Canada
- Mexico
- United States

EUROPE:
- France
- Germany
- Italy
- United Kingdom

APJC:
- Australia
- China
- Hong Kong
- India
- Indonesia
- Japan
- Korea
- Malaysia
- Philippines
- Singapore
- Taiwan
- Thailand
- Vietnam

Industries:
- Accounting
- Architecture
- Business Consulting
- Chemical Engineering or Manufacturing
- Construction
- Education
- Financial Services
- Government
- Healthcare
- Manufacturing:
- Non-computer Related
- Retail
- Software Development
- Telecommunications
- Transportation
- Wholesale and Distribution
- Non-Profit/ Charitable

Audience:
Professionals responsible for their company's IT

These organizations include:
- small (between 1 and 249 employees),
- medium (between 250 and 999 employees), and
- large businesses (1000 employees or more).

XONTECH
SYSTEMS

Push on technology

"XONTECH Systems" - the confidence we gained is due to well-thought-out working principles developed on the basis of the experience gained within company's years of activity. Every service delivery goes through a process in which the whole XONTECH team is involved, from project initiation, to delivery assurance, integration, and product configuration prior to production. This is entire process where is involved all the team to deliver the best results.

XONTECH Systems has a team of specialists with skills gained through experience and adapted to the current needs of IT sector.

The main focus is to provide IT solutions:

- Information security;
- Hardware and software infrastructure;
- Telephony & Unified Communication;
- Document management;
- Network management and monitoring;
- Mobile device management;
- Xontech Academy training and education;
- Certification on management systems;
- IT infrastructure outsourcing.

Constant investment in employees is the guarantor of our customer's success, inasmuch as our entire team participate in training courses and events dedicated to the latest trends and products in the IT industry.

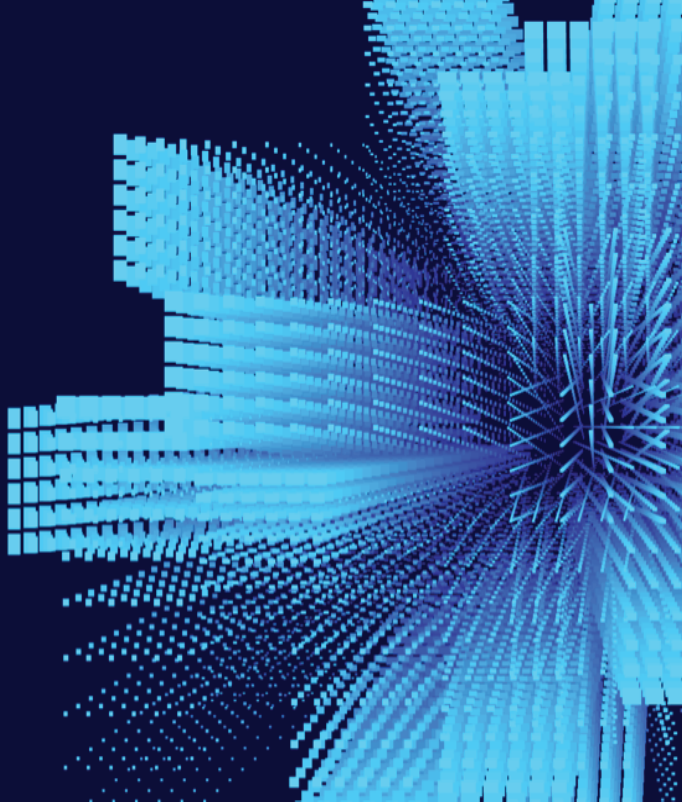
We belive in trusted partnership with each customer and partner. This objective is achieved through the implementation of successful projects, consulting and solving customer issue, integration and implementation of IT solution and best marketing tools to move further each customer business.

xontech.md

MICRO FOCUS

Secure What Matters Most

Security, Risk & Governance



Cyber threats are escalating. Aging apps and processes (along with new ones) are full of unforeseen risks. Privacy and compliance requirements are mounting. And point solutions don't offer the scope, vision, or cross-silo analytics needed for these company-wide challenges. With our solutions, you can take a holistic, analytics-driven approach to securing what matters most— identities, applications, and data.

https://www.microfocus.com/en-us/cyber-resilience

The new risk equation: Motives — Means – Opportunity

Mr. Ramsés GALLEGO,
Security, Risk & Governance International Director with Micro Focus

One of the simplest definitions of risk that I have found in my career is expressed in the form of an equation, with its variables, its factors, its result. This is (or was) the following: for risk to exist there must be a threat that uses a vulnerability, with a probability of that happening and there has to be an impact (Threat — Vulnerability — Probability — Impact). There must be someone (or something) who wants to harm, our systems must have a hole (which will be exploited by the attacker), there must be a probability of this occurring (the greater exposure and/or holes, the greater the probability) and, of course, there has to be an impact, a damage, a loss (otherwise, we could talk about residual risk or even existing risk without real consequences).

Taking into account the previous equation and with the aim of mitigating that risk, we can only work on three of the four variables that build it. We can only reduce the exposure factor by reducing existing vulnerabilities, by closing those holes; in doing so, we will naturally reduce the likelihood of an attack occurring and that is also working on the dimension of dwarfing the risk. And protecting the assets with the appropriate countermeasures — always knowing the value of what we want to protect — we will be reducing the impact. Fantastic. However, what we cannot avoid is that there are agents who want to cause evil, who want to steal corporate information and/or who simply want to cause disruptive situations for the entity. We cannot avoid that there are malefactors (beyond social and educational policies for society that are not subject to these lines) and, consequently, we must comprehend that the threat factor, with that external element — usually — that wants to damage the reputation or economic-financial situation of an organization will always exist and we can do nothing about it.

Reflecting on that factor over which we have no control of the risk equation, another 'equation' came to my mind that could well be an explanation of why these threats exist and why the society in which we live experiences an amazing increase in some types

of threats —1500% — (no, not a typo) as with formjacking and other innovative attacks. It's about Motives — Means — Opportunity. A digital attacker -as in the physical world — needs a reason to harm, an ultimate goal that 'authorizes' her/him to perform the action. Currently two fundamental reasons are cited: money and social or political disruption. These are the two main reasons that move cybercriminals to perform their acts. However, if the adequate means are not available, the will to carry out an attack would only remain in the design phase …unfortunately, though, there are very advanced means… with costs that have dramatically reduced the ARPA (Average-Revenue-Per-Attack) and they are even 'borrowed' by groups of larger attackers to smaller groups sharing benefits (!). We have reached the democratization of the attacks. We have arrived to the extent of a concept taught in first year of Business and Economic Sciences: a cartel (an organization that reaches agreements with other companies in the sector -the bad ones- and eliminates the competition — the good ones —). Finally, in this new risk approach, attackers need a window of opportunity, which does root with the 'old' risk equation in its facet of exposure factor, company visibility, vulnerability management, … The Internet allows the invisibility of the attacker … or if there is visibility, the international judicial system does not always facilitate the prosecution of the crime. Thus, the opportunity aspect is as relevant as the other two factors.

If we add sophisticated Tactics, Techniques and Procedures to this mix (TTP is the acronym), sometimes even using mechanisms that are used for protection (let's not forget that the main pillar of ransomware attacks is the encryption of the data), we are facing a situation of weakness in front of these attacks.

I would not like to end these lines without addressing a positive aspect of all this: these Motives — Means — Opportunity are also available for those who want to PROTECT and DEFEND. Today, companies know the reasons to safeguard information — not only the law but common sense should play an instrumental role here. They have the means to do so (obfuscation in the use of the cloud, isolation chambers, safe navigation, encryption of communications, etc.) and, above all, the opportunity. There has never been so much information or technology to perform that protection and defense effectively. You have never had so much threat intelligence - captured with millions of points of information at the endpoint, in the network, in storage cabins, in the gateway, in mobile devices, …). Therefore, there is a 'new' risk definition with new variables to consider: Motives — Means — Opportunity. For the bad guys … but also at the reach of us, the ones who have to defend. We, the good ones.

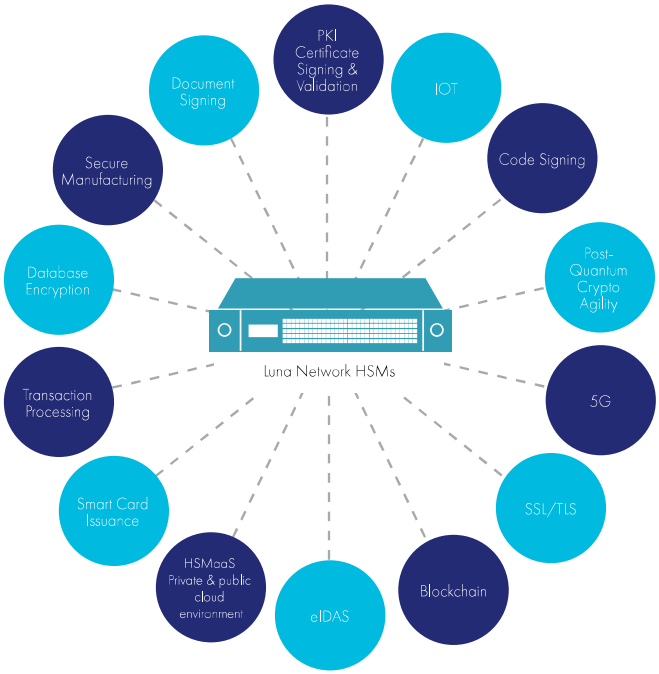
thalesgroup.com

THALES

Thales Luna Network HSM

Secure your sensitive data and critical applications by storing, protecting and managing your cryptographic keys in Thales Luna Network Hardware Security Modules (HSMs) - high-assurance, tamper-resistant, network-attached appliances offering market-leading performance.

Contact us to learn how you can integrate Luna Network HSMs into a wide range of applications to accelerate cryptographic operations, secure the crypto key lifecycle, and provide a root of trust for your entire encryption infrastructure.



What you need to know:

Superior Performance:

- Meet your high throughput requirements with over 20,000 ECC and 10,000 RSA operations per second for high performance use cases
- Lower latency for improved efficiency

Continuing to Strengthen International Connections on the Cybersecurity Framework

Ms. Amy MAHN,
International Policy Specialist,
National Institute of Standards and Technology, Applied Cybersecurity Division

In these uncertain times, our most important focus is on health and safety. Like so many of you, most of us at NIST are working remotely. But we are still working hard to support our cybersecurity mission. While NIST had to cancel the Advancing Cybersecurity Risk Management Conference scheduled for May 2020, we look forward to continuing our cybersecurity efforts through virtual meetings and discussions with you. We continue our international work and welcome your feedback on how we can strengthen our engagement in different and creative ways. After all, our international connections are more important than ever.

This was one of the very clear messages NIST received when we first convened stakeholders in 2013 to discuss a potential Cybersecurity Framework. We were asked to ensure that it be aligned with other cybersecurity approaches used in all the places U.S. organizations operate. We are fortunate to be able to continue engaging with stakeholders to improve international awareness of and engagement with the Framework, which will also help us improve the Framework.

Since our last update for Cybersecurity Awareness Month, I had the opportunity to work with some of our international peers during a six-week work detail in Vienna, Austria, as part of the Department of State's Embassy Science Fellows program. While at the U.S. Tri-Mission Vienna Embassy, I focused on cybersecurity policy and collaboration as part of the U.S.-Austria Strategic Dialogue, which was launched in February 2019. This detail aligned well with my role in engaging internationally to support the Cybersecurity Framework and NIST's broader cybersecurity risk management approaches.

During my time in Vienna, I met with key players in Austria's cybersecurity landscape, including representatives from various ministries, industry groups, research institutions and universities. I learned through these conversations about cybersecurity and critical infrastructure protection efforts in Austria and shared information about NIST resources, including the Cybersecurity Framework.

I'm grateful to the Political Economic section of the U.S. Tri-Mission Embassy in Vienna and all those I spent time with for the amazing opportunity to work on this project and to lay the groundwork for continued collaboration. I also owe a debt of gratitude to the Office of Science and Technology Austria at the Austrian embassy in Washington, D.C., for helping me to prepare for my detail and for the continued engagement upon my return. I look forward to working with all of these colleagues on future opportunities for cybersecurity collaboration, work that has no doubt been enhanced by my time spent in Austria. I'm also excited to use this experience to advance NIST's international work on the Cybersecurity Framework and other programs. Much of what I discussed with colleagues in Vienna will be valuable in better understanding how others around the globe view the Framework and other NIST cybersecurity efforts. These and other international engagements help to support our efforts to improve alignment.

I am pleased to report that NIST has seen an increase in the number of translations of the Framework, including a soon-to-be available Bulgarian translation. All translations and adaptations are available on our recently reorganized Framework International Resources site. We continue to add other resources related to the Framework to the site, including a white paper from the Coalition to Reduce Cyber Risk (CR2) on elevating global cybersecurity risk management through interoperable frameworks.

This project is funded
by the European Union

Ms. Benik LIMAJ,
Team Leader, the European Union Project
"Cybersecurity EAST"

Project Summary

Project Title:	**Cybersecurity East**
Regional Scope:	**Armenia, Azerbaijan, Belarus, Georgia, Republic of Moldova, Ukraine**
Duration:	**27 November 2019 – 26 November 2022** (36 months, renewable)
Budget:	**EUR 3.121.600 mio** (funded by the European Union)
Implemented by:	**GFA Consulting Group (DE)** in Consortium with the E-Governance Academy Foundation (EE), Detecon International (DE), Action Global (CY) and in partnership with the German Federal Office for Information Security (DE)

Background and Context:

The EU adopted in November 2018 the regional programme **'EU4Digital: Improving Cyber Resilience in the Eastern Partnership Countries**[1]**'**, as part of its commitment to enhance the overall security across the region. Managed by DG NEAR, this first-ever regional programme includes two components: cybersecurity and cybercrime.

Cybersecurity incidents generate significant costs for the global economy and undermine trust in the digital society. With the evolution of cybercrime to an affordable crime-as-a-service-based business model that supports the entire cybercrime value chain and drives the digital underground economy, the range of threat vectors has multiplied significantly. At the same time, cyber tools are used to pursue particular political, economic, financial and strategic interests, including through disinformation campaigns or hybrid operations targeting critical financial, energy, or transportation infrastructure. Due to the multi-dimensional nature of threats in cyberspace, they require flexible and adaptable governance models to counter them, accompanied by comprehensive and crosscutting policies that engage the many levels and with different actors, institutions and individuals involved. Consequently, the focus on risks and vulnerabilities in the context of building cyber resilient states and societies addresses security not merely as an objective in itself but rather as means towards achieving broader developmental objectives.

In 2016, the European Union adopted the **Directive on Security of Network and Information Systems (NIS)** representing the first comprehensive EU-wide legislation governing its cybersecurity at European level. It aims to achieve harmonization between Member States by obliging them to adopt national NIS strategies and create single points of contact as well as CERTs in order to reach a common level of cyber resilience. In addition, it sets out security and notification requirements for Operators of Essential Services in critical sectors such as energy, banking, digital infrastructure, transportation, water, health, etc., and enables cross-border collaboration through a network of CSIRTs and the strategic NIS Cooperation Group. The NIS Directive frequently features as blueprint and best practice in the EU's cyber capacity building initiatives supporting its partners developing cyber resilient societies and economies.

Project Objectives:

Coinciding with the EU-EaP '20 Deliverables for 2020'[2], listed in its deliverable 12 (Security),, this regional action focusses on further developing the approximation of all EaP Partner countries to the EU basic pillars on cybersecurity, taking into account the different level of advancement between the EaP countries. It pursues the **overall objective** to develop technical and cooperation mechanisms that increase cybersecurity and preparedness against cyber-attacks, in line with the EU standards.

The Project's Framework: 3 Fields of Activity

The project intends to facilitate the legal and institutional harmonization of the Eastern Partnership countries with the European Union by focusing on the tailored approximation to the NIS Directive as a best practice to enhance levels of cyber resilience. Two fields of activity include strengthening **national cybersecurity governance and legal frameworks**, and developing **frameworks for the protection of Operators of Essential Services (OES) and critical information infrastructure (CII)**. These also include supporting the reinforcement of public-private partnerships as well as building networks with multiple stakeholders and raising (public) awareness and improve cyber hygiene. Through a third activity area, the project seeks to increase the **operational capacities for cybersecurity incident management of national, respectively governmental computer emergency response teams (CERTs)** and enhance their cooperation with providers of CII and OES as well as cooperation between them on a regional and international level.

To achieve its objectives, the project will address the specific needs of each of the EaP countries while, at the same time, fostering capacity development and cooperation at a regional level between the six EaP countries, and between them and EU Members States and European institutions.

The Council of Europe (CoE) implements the sister component CyberEast Project dealing with the prevention and prosecution of cybercrime. The close links between cybersecurity and cybercrime allow the realisation of synergies addressing the issue of cyber resilience comprehensively.

Approach and Strategy

The geographical focus of the project includes the six EaP countries: Armenia, Azerbaijan, Belarus, Georgia, Republic of Moldova, Ukraine. These partner countries continue to make progress regarding different cybersecurity aspects highlighted, for example, in the Global Cybersecurity Index of the International Telecommunication Union for 2018/19. However, there are considerable differences and challenges between the six countries with regard to their level of cyber resilience. Given the project's wide regional scope and technical focus, it needs to take these differences carefully into account in order to provide meaningful and comprehensive capacity development measures. Another important factor are the varying levels of cooperation between the individual EaP countries, and between them and the EU. For example, Georgia, Moldova and Ukraine have signed Association Agreements as well as Deep and Comprehensive Free Trade Agreements with the EU, while no such agreements are in place with Belarus, Azerbaijan and Armenia. These differences have direct implications in terms of the countries' specific needs for technical support as well as for opportunities to strengthen the approximation of their national governance frameworks to the EU's legal frameworks for cybersecurity and the NIS Directive. The project strategy therefore focusses on **differentiated and tailor-made activities** based on sound and in-depth analysis of the status quo at the country and regional levels.

Contacts:	
European Commission: Roberto SEGUNDO NAVARRO, Programme Manager Roberto.SEGUNDO@ec.europa.eu Good Governance and Security Directorate-General for Neighbourhood and Enlargement Negotiations (DG NEAR) Directorate Neighbourhood East – Unit C1 European Commission https://ec.europa.eu/	**GFA Consulting Group:** Besnik Limaj, Team Leader besnik.limaj@gfa-group.de https://www.gfa-group.de/

Cybersecurity: Managing the Risk and the Opportunity

Mr. Mihai (Ion) DANTIS,
Expert, the European Union Project "Improving Cyber Resilience in the Eastern Partnership Countries"

In the words of Benjamin Franklin: ***"An ounce of prevention is worth a pound of cure."***

Cybersecurity – The Importance

Cybersecurity is today a lever for competitive advantage in a world accelerating forward with intense digitalization. Along with being a shield that protects organizational innovation and intellectual property, it is foundational to digital trust, market making, and inclusivity. The state of cybersecurity is now a concern that transcends the interests of the any organization and holds the attention of executive management and the board.

Data triumphs everything'. The one who controls data; controls people, controls governments, controls the future. The most vulnerable link in today's times is **"Breach of Data"** and the biggest investment in the entrepreneurial mind is 'How to secure Data Breaches?', because once data is compromised, confidentiality, integrity or availability are compromised.

COVID-19 changed how we work, shop, and interact. Lockdowns accelerated the rise of remote work, and 'DATA' became the center piece of the 'New Normal' which became the buzzword of the year. In 2020, credential stuffing attacks gained in popularity and sophistication due to the COVID19 situation, which increased the use of collaboration tools, such as WebEx and Zoom.

Globalization that had transformed the economic markets into a strongly interconnected system at the international level, came to a standstill. Critical links in the global supply chain were broken, supply chain disruption rippled across every industry. Consumer fear, bottlenecks, and shipping delays created surges in demand and shortages in supply. All these risks for companies aggravated during COVID19.

Cybersecurity ecosystems have seen the toughest ask from entrepreneurs, governments and most importantly citizens. Cybersecurity has scrambled to manage the 'New Normal'. The opportunities for profiting from espionage, IP theft, ransom, and other criminal activities increased while the world directed their attention to the clear and present danger of COVID19 have been immense.

As more and more organizations adopt cloud, automation, and digital transformation and prepare themselves better for future disruptions, the need for a secure cyber foundation has never been stronger.

Cybersecurity: The Threat and The Risk

Every year, new strains of malware emerge that attempt to exploit weaknesses in Enterprise IT defense mechanisms. While threat-hunting teams pool their energies toward identifying new persistent threats that are sometimes undetected by traditional toolsets, most Security Operations Center (SOC) teams need to also deal with the volume of regular threats that slip through the weak links in a layered defense. These cyberweapons cannot be ignored and consume SOC resources already crunched for time.

Obtaining confidential information without the information holder's consent has serious business implications because the stolen data generally includes intellectual property, personally identifiable information (PII), or financial data.

Cyber threats continue to evolve, dovetailing with the emergence of new technologies and attack surfaces. The cybersecurity industry has, mostly, responded with technology controls that can help prevent or detect such risks as they materialize. However, what continues to be the elephant in the room is the human dimension of the cyber problem. Organizations continue to grapple with how to protect the first line of defense. For example:

1. Ransomware continues to be an integral part of an attacker's strategy. It managed to shake up a few things. Trojans continue to be the most favored agent to launch malware attacks. Organizations need to minimize the availability of system/asset landscape data in the public domain and increase efforts to improve cyber hygiene. Worms, a tried and tested technique for attackers, are always an attractive malware type.
2. Cryptominer attacks have continued to dominate and the majority of attacks belong to this category. This technique has lured attackers to use it for financial gains. Also, attackers can easily embed cryptomining capabilities into the compromised machines handled by them, making these attacks a preferred choice.

The hard truth is that this new reality has only exacerbated the status quo for cybersecurity professionals. Security leaders were already struggling to address the challenges of today's fluid network boundaries. This is now exponentially compounded as millions of workers connect remotely to corporate networks while working with critical data that has moved seemingly overnight to newly deployed software-as-a-service.

Cybersecurity Regulations:

Laws and regulations play a pivotal role in the cybersecurity environment, helping shape rights, obligations, and behaviors. Thus, regulatory changes can have a macro-level impact across jurisdictions. Legal directives across the cybersecurity landscape are

changing around the globe. More countries are adopting methods of imposing huge fines for non-compliance to data protection laws. Countries across the globe are responding to citizen concerns, consumer demands, globalized trade imperatives, and geopolitics to strengthen their privacy and data security legal regimes every year.

Mitigating cyber risks involves establishing organizational policies ranging from employee behavior to technical security controls. At a minimum, the organization must achieve compliance with applicable regulations as GDPR, and industry standards, such as PCI DSS. So beyond ensuring compliance, leaders must consider and manage risks that apply to them based on the nature of the business, the scope of operations and so forth. This also means adequately funding cybersecurity resources consistent with a plan that implements critical security controls (like the CIS Controls).

It is important to ensure that the means of complying with legal obligations align with business objectives and areas of real risk; cyber security management should not be a box-ticking compliance exercise. In practice, this means that the legal obligations permit a degree of flexibility to carry out a risk assessment and to tailor security measures to mitigate against areas of real risk. If a cyber security breach occurs despite having taken all these measures, then there will be no legal breach.

Cybersecurity: Governance & Resilience

Enterprise security governance goals must be aligned to corporate governance objectives to manage risks through the effective rollout of control measures. For organizations to achieve continuous cyber resilience, they need to assess maturity at the point of departure and draw short-term and long-term strategies to predict attacks, protect from attacks, detect intrusions, and activate timely response and recovery mechanisms. In addition, the role of government agencies in aiding the private sector against state-sponsored attacks will be increasingly under scrutiny.

In the COVID-19 scenario, the cyber resilience framework had undergone stress tests as threats, events, and incidents will need to be identified and mitigated. A cyber-resilience framework that provides mechanisms for communication of roles and responsibilities, feedback, and critical imperatives between various layers of the enterprise hierarchy is urgently needed. Cyber-resilience is required to prove itself across dimensions of assessment of cyber risks and threats; prevention of cyberattacks and response mechanism to cyberattacks.

Post COVID19:

Ready or not, enterprises today have to manage a new normal that includes a distributed workforce and new digital strategies. A major trend over the next 6–12 months will be preparing companies to secure their employees and brand in the new normal.

The world post-COVID-19 will look much different than it did just a few months ago. There will be employees that never return to the traditional office, with businesses having had their eyes opened to the fact that they can operate securely without being in a building.

There will also be businesses that do return to working side-by-side with their colleagues but with the understanding that disruption could happen again and that they must be equipped to quickly and efficiently switch back to working remotely.

Cloud adoption, digital transformation initiatives, and hyper-automation are expected to accelerate in the post-COVID-19 world. Cloud-enabled scalability and automation can address the need for future business resilience during similar disruptive situations. However, rapid migrations of enterprise services to the cloud need a secure foundation.

Zero trust architecture will play a critical role in managing threats as organizations shift their traditional approaches to keeping data, people, and systems secure. In zero trust-centric approaches, the trust zone is compressed to narrow segments where continuous decision-making occurs. This approach works under the assumption that the threat actor is already present in the environment.

Cybersecurity: The Future

Strong collaboration between the public and private sectors is a necessary enabler for identifying new threats in cyberspace and evolving strategies to counter them. Collaboration becomes even more pertinent when it comes to protecting 'Cyber Critical Infrastructure'. Shared responsibility is the foundational principle in cybersecurity. Information sharing between organizations in the private sector directly or through government intermediaries is critical to stay abreast of threat actor actions.

The future of cybersecurity is indicated by the high number of patents filed in the 'data security' and 'device security' areas followed by 'network security'. With the rise and growth of emerging technologies such as Artificial Intelligence and Machine Learning (AI/ML), the use of these technologies will rise in both cybersecurity practice areas and their widespread adoption.

The emergence of Decentralized, consensus-based identity verification solutions; gain in Serverless security; computer vision and ML-based identify verification; and Internet of Things (IoT) device security solutions using quantum driven key management are some of the promising areas in Cybersecurity.

Thus, as more and more cyber threats emanate from nation-state actors, the home government's role and military doctrine around cyberattack response would play a critical role in protection of 'Cyber Critical Infrastructure' and the engaged collaboration and cooperation between all actors of cybersecurity would remain a key to protecting our citizens and our nations.

Don’t just automate, address the root cause

Mr. Adli WAHID,
Expert, the European Union Project “Improving Cyber Resilience in the Eastern Partnership Countries”

Automation is becoming an increasingly important tool within cybersecurity. However, like all ‘new’ tools, it’s important not to get wrapped up in the hype surrounding them. Before considering what automation techniques, you want to employ, I recommend you consider these three fundamental steps.

Think left of the hack

The first step of securing your network is being aware of the need to secure it. A lack of awareness leads to a ‘not-my-problem’ or ‘let’s wait until something happens’ attitude. Awareness, on the other hand, leads to proper assessment, preparation and action. While there’s no doubt that the community cares and is generally aware of security, more often than not, the focus is on “what affects me”, like that crippling DDoS attack or system compromise leading to customers’ data being exposed. Trying to understand what solutions are available when faced with an incident is fine but you must also get to the root cause.

Normally, folk don’t think about the ‘left of the hack’, that is to say, what happens before the attack. Nor do they give much thought about how criminal enterprises plan, operate and monetize their business by using legitimate and illegal services that are acquired through hacking and system compromise.

Understanding how criminals can leverage your infrastructure to achieve their goals helps with focusing your monitoring and developing strategies and policies to react to and mitigate such attacks. More important, however, is continuous monitoring to prevent attacks. I can already hear someone saying ‘automation!’, but before getting into that I think you should get your team to be aware of the nature of the problem and discuss possible solutions.

Monitor the health and reputation of your network

You all most likely have a great understanding of what is happening on the inside of your network but many of you may not know what your network looks like from the outside. What I mean by this is how others in the Internet perceive your network, in particular, if it has a bad reputation because of some rogue ports or misconfigured routes. Recently, APNIC launched two new tools, DASH and NetOX.

Using DASH, APNIC Members can get insights from the APNIC Community Honeynet Project (ACHP). This is a platform APNIC established in 2017 to assist network engineers and network security personnel throughout the Asia Pacific region with setting up individual honeypots in their networks. Members can see if any of their IP addresses are hitting any of the ACHP honeypots — by right, the devices in your or your customers' network have no business in our honeypots. Normally in describing what is happening to those asking for further insights, we mention that this particular IP address is not just hitting our honeypots, it may have a reputation already! Aside from these products, the Shadowserver Foundation also provides feeds related to different types of threats seen coming from your Autonomous System Number (ASN). It is also important to understand that in most cases what you are getting is a symptom of something. So yes, there is a high possibility that the device has been infected but further work is required to understand the when, how, what and who.

Policies maketh the machine

Apart from the technical considerations, other aspects are equally important such as best practice policies and processes. Management may need to get involved at this point and understand the context and why additional resources, such as that nifty new automation tool, are needed to support the work. It's equally important to continually update these too — this will allow you to react to new instances quicker, which means less downtime and/or time losing face within the community. To give a real example of the latter, I contacted an ISP about an infected small office/home office router seen in our honeypots daily since February this year. The response I got was that they have informed the customer and that was that. My assumption is they just simply have not worked out what to do to help the customer secure the device beyond rebooting and, more importantly, prevent malicious activities — in this case, multiple telnet and SSH brute force attempts from the customer's device. In the context of automation, it's important to understand how automation can/will affect your policies and procedures. To make the right decision based on your policy, you will need to curate these automation tools to increase their effectiveness.

GTB Technologies

Data Security that Works™

GTB Data Protection that Works™ Secures Insurance Enterprise

Used by the Who's Who of Global Enterprises, Governments and Organizations

1. Powerful Knowledge
2. Trust of clients
3. Technology Leadership
4. Solutions that Work

Market Leading DLP & The Audit

A healthcare insurance enterprise was experiencing difficulty using their "market-leading" DLP solution. With a major audit approaching, along with the cybersecurity groups' concern of a possible PHI, PII or PCI breach, the decision was made to test the remaining Gartner Magic Quadrant Market Leaders including the GTB Technologies DLP that Works platform.

No Clue Where the Data Is (CCPA, GDPR, PII, PHI & PCI)

Many regulatory statues require PII data to be encrypted and / or redacted with the ability to destroy the data per request. Even with a "market leading" DLP solution, the data administrators were unsure if they were compliant, nor were they able to monitor and control sensitive data from being synced to cloud services or sent out through non-sanctioned email (e.g. Gmail).

Main Challenges

- **Protect PII**, (HIPAA) of 150 million accounts, Scan **Oracle** Databases with 14 Billion records
- Scan **Exchange** Mailboxes for **PCI** compliance
- **Reduce / eliminate** false positive events

The Solution - GTB DLP

- **Detection** accuracy - **ZERO false positives!** leads to ease of use and management
- Redaction of images - **unique to GTB**

The Results

- **Redaction** project completed on time, **under budget**
- **Prevented theft** of PCI data, detected sensitive data within a few hours of implementation
- IT resources for data protection **reduced**

About Us

For over 14 years, GTB Technologies has provided data protection solutions that accurately prevent sensitive data loss/ ex-filtration from within the network, at the endpoint, in the cloud or anywhere else; either agent or agent-less, in files or data streams..

Contact Us

West Palm Beach, FL USA

T: (800) 626-0557
E: info@gttb.com
W: www.gttb.com

Three generations of cyber resilience

Mr. Iulian CHIFU,
President, Center for Conflict Prevention and Early Warning,
Bucharest, Romania

Cyber resilience is the concept that become the reference for managing the communication and facing the side effects related to security threats in the digital word. Even in that area, of a concept so recently developed, we have already three generations related to the type of approach to resilience.

Prevention and stability. Resilience 1.0.

The first generation of cyber resilience is linked to maintaining stability of the existing system and prevention of the cyber-attacks, at a "normal" level. This means taking the best measures for a decent hygiene of the working place: a licensed soft, an antivirus, updates of the programs at due moments, protection of the PC/Laptop/terminal with personal and secure password/passwords that are changed often, maybe once every two weeks, but especially when we have travels or meetings in places that could have presented risks. Prevention could mean, for the institution, following the bulletins of the CERTs and license providers with the last most intrusive threats.

Proactive action and early warning. Resilience 2.0.

Once this level is achieved, or for the most exposed users, involved in the access to more sensitive resources, the rules should be improved dramatically. Besides the separation of the circuits between those connected online and those in a protected intranet, an institutional center for dealing with cyber defense is needed with qualified specialists and enough resources to face the more elaborated threats. Those institutional instruments should involve a pro-active action, looking for the threats and going after them, when it's up to defense against current threats, and building early warning systems to help alert than prevent breaches of security and the most invasive and destructive attacks.

Resilience in contemporary societies. The three levels of cooperation and limitations

A true resilience cannot be built without the three layers of the cooperation, based on trust and mutual support: the state and its institutions, the society – involving business and private actors, NGOs and civil society, and the citizen. In all the threats of hybrid nature, terrorism and cyber attack, the resilience cannot be achieving except if this three track cooperation exists, is in place, functional, and the citizens are trusting and addressing the official authorities and institutions for help and signalling problems, and the civil society assists in the education of the people regarding the levels and types of threats and possibility to protect, including the roles of each institution. Any breach of confidence or abuse of authority could harm the mutual trust and undermine the cyber resilience that we would like to achieve.

Resilience 3.0. Dynamic adaptability and the resilience of the future

The third level of cyber resilience is about dynamic adaptability and the capacity to reform during an attack or during a crisis. It is an approach far more elaborated which means that the whole internal system of an actor prepared in advance to deal with the new generation of threats should adapt in real time and have proper means to face the evolution of those threats, in order to protect data and privacy, procedures and means.

This would imply, for instance, building characteristic markers for each access in the network, creating the actor's own viruses, going after those who do not have markers or have duplicates or fake markers, making tails and signals for each such breach and going after the perpetrator, with an action of exposing the identity, breaching its relative anonymity, even sending him a virus to destroy his own system, computers or data bases once it breaches without proper title into a forbidden or private actor system. All these comes from a dynamic adaptability.

This would be an offensive action, usually coupled with a capacity to quickly evade from a giving physical system and move into a different one or being able to work alternatively in cloud or in a protected intranet secure reserve system. This could lead to an operation of reforming during crisis, meaning avoiding the physical premises or a given system and recuperate all data and continue working with the preservation of the main attributes of the organization/actor.

Reforming during crisis. Lessons learnt from the Covid-19

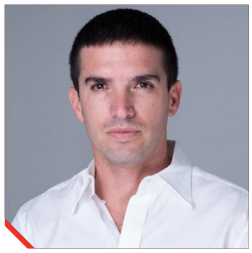
COVID-19 pandemics has been a real challenge and test for resilience, that once proving the need for solidarity and cooperation at a national and international level. The limits of any system of resilience have been forced and different organizations and actors, both

state institutions and private companies, have been forced to develop, practically overnight, skills and capacities in order to adapt to the shift from physical work to work from home and extreme use of digital capacities at hand.

This dynamic adaptation proved the need to move to a third generation of resilience meaning the one with dynamic adaptability, and capacity to reform during the crisis. Lessons learnt from this experience are of first importance and there's the place to act and to collaborate, especially in the field of knowledge exchange, in order to improve the level of resilience of our own institution and country, of our partners and allies.

*Iulian Chifu is the President of the Conflict Prevention and Early Warning Center. He is a professor at the National Defense University, Bucharest, associate professor the National University for Political and Administrative Studies Bucharest. Between 2011-2014 he was Advisor of the Romanian President for Strategic Affairs, Security and Foreign Policy.

About the Israel National Cyber Directorate



Mr. Lavy SHTOKHAMER,
Executive Director at the INCD,
Head of Israel National CERT

The Israel National Cyber Directorate is the national security and technological agency responsible for defending Israel's national cyberspace and for establishing and advancing Israel's cyber power. The Directorate operates at the national level to constantly strengthen the level of defense of organizations and citizens, to prevent and handle cyber-attacks and to strengthen emergency response capabilities. As part of its roles, the Directorate advances innovative cyber solutions and forward-looking technological solutions, formulates strategies and policies in the national and international arenas and develops its cyber manpower. The Directorate strives to maintain a protected, safe and open cyberspace for all of Israel's citizens and to facilitate the State of Israel's growth and power base.

Vision

A secure, safe and free cyber space in Israel that underpins economic growth and enhances Israel's overall strategic posture.

Purpose

The INCD is the state body in charge of defending Israel's national cyber space from cyber threats and is in charge of promoting and establishing Israel's capabilities in the field.

Tasks of the Israel National Cyber Directorate

Defense

To lead efforts to defend the national cyberspace by preventing, detecting, identifying and responding to cyber attacks on the national level.

Resilience

To prepare and enable the Israeli private sector and general public to protect them-

selves from cyber threats by adopting cyber secure technologies, publishing best practices, training personnel and increasing awareness.

Innovation Leadership

To establish and reinforce the cyber science-and-technology base by developing high quality human capital, supporting advanced academic research, engaging in deep technological R&D and fostering the cyber industry; while combining the above sectors in a vibrant ecosystem.

International Posture

To promote the State of Israel as a world leader in cyber, thus strengthening its defense, its economic resilience and its international standing, through international collaboration, capacity building and engaging multilateral processes

Strategy and Policy

To design and formulate national cyber strategy and policy in Israel, as well as internationally, creating a focal point of knowledge and professional authority in the field of cyber policy, and to serve as advisor to the Prime Minister and the Government of Israel.

The Israeli Cyber Emergency Response Team (CERT)

The National CERT handles cyber incidents in the civilian cyber sphere of the State of Israel. Located in Be'er Sheva's high-tech park, the CERT receives and handles hundreds of reports and information about cyber-attack attempts or threats, from local and international partners, on a daily basis. The CERT is part of the operational unit of the Israeli National Cyber Directorate (INCD) - a state-run, defense-technological entity devoted to protect the Israeli cyberspace. The existing model in Israel is considered unique in the world because it incorporates five sectorial sub-centers dedicated to specific industries in the economy, which all operate under the same roof and work in synergy. The Israeli CERT maintains working relationships with most of the world's leading cyber organizations and industries, sharing information as well as providing assistance and advice to state partners and trusted partners.

Among the roles of the CERT: Responding to cyber incidents, promoting preventive activities, creating tailor made partnerships and coordination between industries, government and international partners when dealing with and responding to cyber incidents, enhancing information sharing, and preparing and issuing alerts to the public. The CERT is the heart of the ecosystem built in Be'er Sheba among high-tech companies, academia,

government and the cyber industry. Alongside these, the Israel National Cyber Directorate also established three innovation arenas in Be'er Sheva specifically aimed at exploring innovative ways of coping with new cyber threats in the areas of Transport, Fintech and Energy. Over 2,400 official visitors from Israel and worldwide have visited the CERT in the past year, bringing international exposure to companies that are located in the city.

The CERT has five sub-centers dedicated to different industries and target audiences that operate around the clock. The information they supply allows us to put together a broad picture of the cyber threats and attacks in Israel and provide a unique answer for each industry.

The main center is the National Incident Management Center. The center, which operates 24/7, regularly receives reports on cyber-attacks, threats and attempts, vulnerabilities and security breaches identified in the Israeli economy. The center, which is operated by analysts who graduated from technological units and universities, maintains continuous contact with the public, organizations and companies in the economy in order to share and receive information on cyber-attacks and threats. The center provides incident handling capabilities to the Israeli economy and recommendations in case of a cyber incidents. The center can be contacted 24/7 by dialing the free, emergency number 119 — the world's first initiative of its kind that allows any citizen to report a cyber incident and receive initial assistance.

The four other sub-centers are sectorial centers set up by the Israeli National Cyber Directorate in cooperation with the relevant government ministries, which provide solutions to sector-specific cyber threats: The Financial sector; the Government sector; the Public Security sector and the Energy sector. Sectorial centers in the fields of Communications, Transportation and Environment are also planned to be established within the next two years. The centers receive information from entities in their regular field, guide and share relevant information with them, handle cyber incidents, assist back to functional continuity and investigate incidents.

HUAWEI

Building a Fully Connected Intelligent World

194 000
Employees

49th
Ranking
Fortune Global 500

90bn USD
R&D Investment
In the last decade

170+
Countries

38
R&D Centers

96 000 +
Employees
of R&D

INNOVATION

We focus on innovation and we are one of the wold's largest investors in R&D

- In the next five years, we plan to invest US$100 billion in R&D.
- Huawei is one of the world's largest patent holders.
- We have put forward more than 54.000 proposals to set industry standarts.
- We partner with major industry players to innovate in emerging domains: cloud computing, 6G, the Internet of Things.

CYBER SECURITY

Security is in Huawei's DNA and security requirements are embedded into how we design, build and deliver all our products.

- Since Huawei was founded in 1987, there has not been a single major cyber security incident.
- Huawei has built and will continue to invest in an end-to-end global cyber security assurance system.
- We will invest US$2 billion, over the next five years, to further enhance the security of our products and services globally.
- We are committed to expand and refine a robust compliance system to ensure we abide by all applicable laws and regulations in the countries and regions where we operate.

Huawei – Bringing Cyber Security to Every Person, Home and Organization

In the past decade, we have seen a dramatically accelerating pace in the development and adoption of new technologies. This rapid technological change is affecting almost every area of the economy, society and culture and is likely to continue in the coming years. And while technology is expected to change the world for the better in many sectors such as health, education, clean energy and infrastructure, new risks are emerging, such as exposure or data loss. Lately, cyber security has emerged as the most pressing exposure for business confronting this new "age of risk". The practice of defending servers, electronic systems, and networks from malicious attacks is a must and companies and organizations are becoming more aware of the importance of cyber security.

What is cyber security? It's the application of technologies, processes and controls to protect systems, networks, programs, devices and data from cyber attacks and it aims to reduce these risks and protect against the unauthorized exploitation of systems, networks and technologies. In other words, cyber security is a way to ensure that your network and server are safe from any external threat, including threats to hardware, software and data.

The ICT industry occupies a large part of this rapid technological change and Huawei as the world's largest supplier to communications service providers, has been keeping pace with offering safe access to the newest technologies. Of course, as the new ICT technologies developed, hacking tools have become more advance, making cyber attacks easier. If in the 1985-1990 hacking was at the level of password guessing and cracking, now the types of attacks have become more advanced, such as ransomware, IoT and AI attacks. This is a point when it's critical to manage associated cyber security risks.

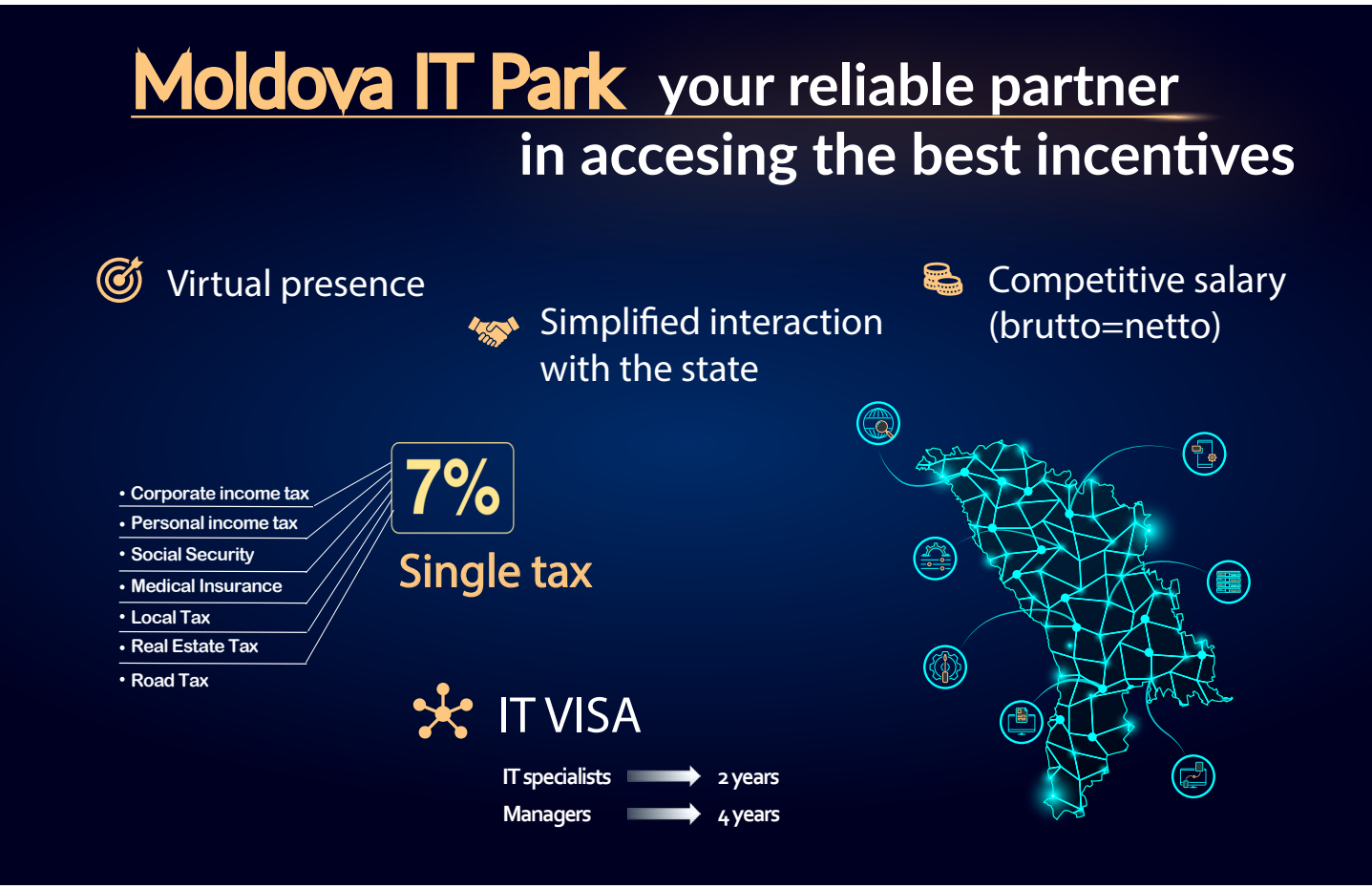
According to Huawei specialists, new security challenges that come with the new technologies are not an excuse to stand still. They are part of technological advancement and social progress and there are some clear steps that can be followed to create a safe ecosystem: integration of security into all business activities, raising all employees' secu-

rity awareness, exploring cutting-edge security technology and use of a more advanced technology to tackle today's challenge and ensure end-to-end supply chain security.

Security and trustworthiness should be a strategic priority throughout product lifecycles and the requirements should always be on top regarding the defensive capabilities of the products, including the ability to protect the confidentiality, integrity and availability of service and data. Resilience and reliability are key aspects in this regard, assuring that systems can continue to be in a known state while under attack and rapidly recover after an attack and ensuring long-term, fault-free operations for the entire lifecycle of the products.

In the field of Supply Chain Security Management, the importance of interplay between various parties, i.e. authorities, manufacturers, distributors etc., to support the fluent and secure flow of goods in the global economy plays a crucial role. For a technological supplier, this means ensuring integrity and traceability from material sourcing and production to delivery to customers.

Following and implementing all these steps, Huawei is delivering cyber security to every person, home and organization. As digital transformation initiatives accelerate across the world, it has a clear responsibility to ensure that security and privacy protection remain a top priority.

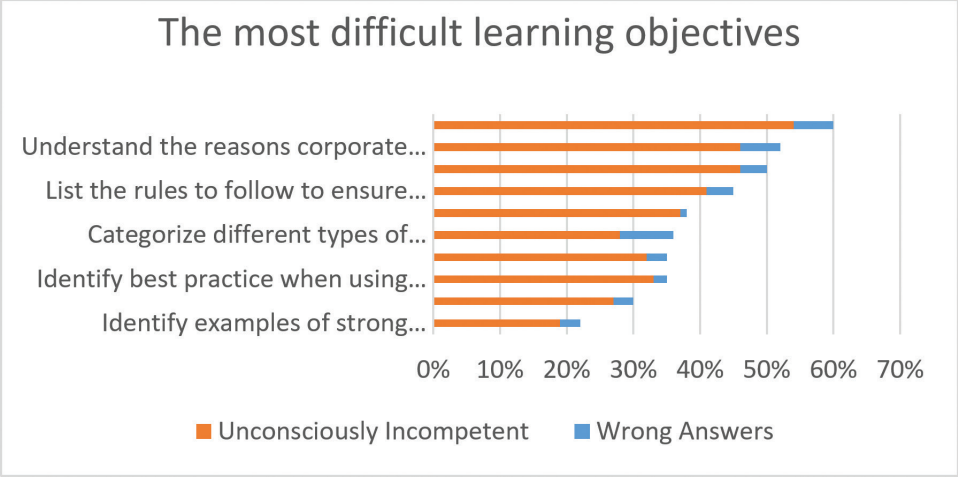

Moldova IT Park your reliable partner
in accesing the best incentives
Virtual presence
Simplified interaction
with the state
Competitive salary
(brutto=netto)
• Corporate income tax
• Personal income tax
• Social Security
• Medical Insurance
• Local Tax
• Real Estate Tax
• Road Tax
7%
Single tax
IT VISA
IT specialists
2 years
Managers
4 years

Working-from-home lessons: employees ‘confidently’ make 90% of all security awareness mistakes

Free security awareness training on remote working from Kaspersky and Area9 has seen participants enact correct responses 66% of the time. However, even when learners were wrong, they mostly remained confident in their competences. The most difficult learning objectives proved to be virtual machines, updates, and reasons why people should use corporate IT resources even while working outside the office.

This spring, due to the coronavirus pandemic, many companies switched to remote working. This change affected corporate security via a growing number of web-based attacks, coronavirus-related phishing, as well as the increased use of shadow IT. To help businesses improve their staff cybersecurity skills, in the beginning of April 2020 Kaspersky and Area9 released an adaptive learning course for those transitioning to at-home working, covering the basics of secure remote operations. Analysis of anonymized learning results revealed that remote staff tend to overestimate the level of their knowledge of

cybersecurity basics. In 90% of cases when learners selected a wrong answer, they evaluated their feelings toward the given response as "I know it" or "I think I know it". This was revealed through an adaptive learning methodology, which asked learners to assess their levels of confidence in responses, as well as answer the test questions.



The study also identified the most difficult learning objectives – the hardest being reasons why to use virtual machines. As many as 60% of the given answers were wrong on this matter, with 90% of respondents falling into the 'unconscious incompetence' category. This means that mistaken learners were still sure that they had selected the right answer or option.

More than half of responses (52%) to questions about reasons why employees should use corporate IT resources (such as mail and messaging services or cloud storage) when working from home was incorrect. In 88% of cases, remote employees thought that they could explain this correctly. Almost the same proportion of mistakes (50%) was made when answering a question about how to install software updates. In this case, a staggering majority of 92% of those who had provided wrong answers, believed they had that required skill.

"If employees see no danger in risky actions, let's say, in storing sensitive documents in personal storage, they are unlikely to seek advice from IT or IT Security departments. From this perspective, it's hard to change such behavior, because a person has an established habit and may not recognize the associated risks." As a result, 'unconscious incompetence' is one of the most difficult issues to identify and solve with security awareness training," comments Denis Barinov, Head of the Kaspersky Academy. To learn more about how the adaptive learning approach can be applied to make employees behave more securely, please visit the official Kaspersky Adaptive Online Training web page.

CENTRALEYEZER

HIGHLY COMPETITIVE

Easily identify and correlate all cybersecurity risks into a single view in order to remediate them faster and easier.

WE HELP :

- CxO and Management Board
  - Transparency
- CISO
  - Risk Prioritization
- Red Teams and VA Teams
  - Fast Integration of datasources
- SysAdmin, NetAdmins, Developers
  - Communication

Prioritize your cybersecurity risks

INTEGRATE & CORRELATE

Integration with web application and network scanners
Correlation of vulnerabilities and de-duplication
Vulnerabilities normalization and standardization

FEATURES

Vulnerability Scanners Integration
Automatic Vulnerability Assignment, tracking and SLA
Standardized Dictionary of Vulnerabilities
Customized Reporting

DEPLOYMENT

Cloud - Software-as-a-Service
On Premise

RISK FACTORS

Vulnerability Severity
Business Context
Network Zone
Threat Intel

+40 722 234 788
Bucharest, RO
contact@centraleyezer.io

Elcore Group was founded in 1996 and nowadays successfully works in 12 countries of Easter Europe and Central Asia. The company is a distributor of **IT equipment, consumer electronics, software and services** from the best IT manufacturers.

Such brands as CISCO, GTB Technologies, Micro Focus, Trend Micro, Hewlett Packard Enterprise, HP Inc., Microsoft, AWS, DELL-EMC, SUSE, Hitachi, ABBY, Nakivo, Axis, Rittal, Rarritan, Xiaomi, Lenovo, DBVisit, DropSuite, Macroscop, MitsubishiElectric DisplaySolutions, TeamViewer, TimeClock365 and others are among our partners.

The mission of Elcore Group is to unite the best IT products and to make IT (informational technologies) easy to access. We help our partners top-managers to make their business easier and more profitable.

We are focused on:

A) **Value Added Distribution (VAD)** – servers, telecommunication equipment etc.
B) **Mobile devices and Consumer Appliances** – smartphones, notebooks, TV's, cameras etc.
C) **Finished Goods** – computers, monitors, commercial notebooks, printers etc.
D) **Software**
E) **Cloud & Services** – cloud services and technologies

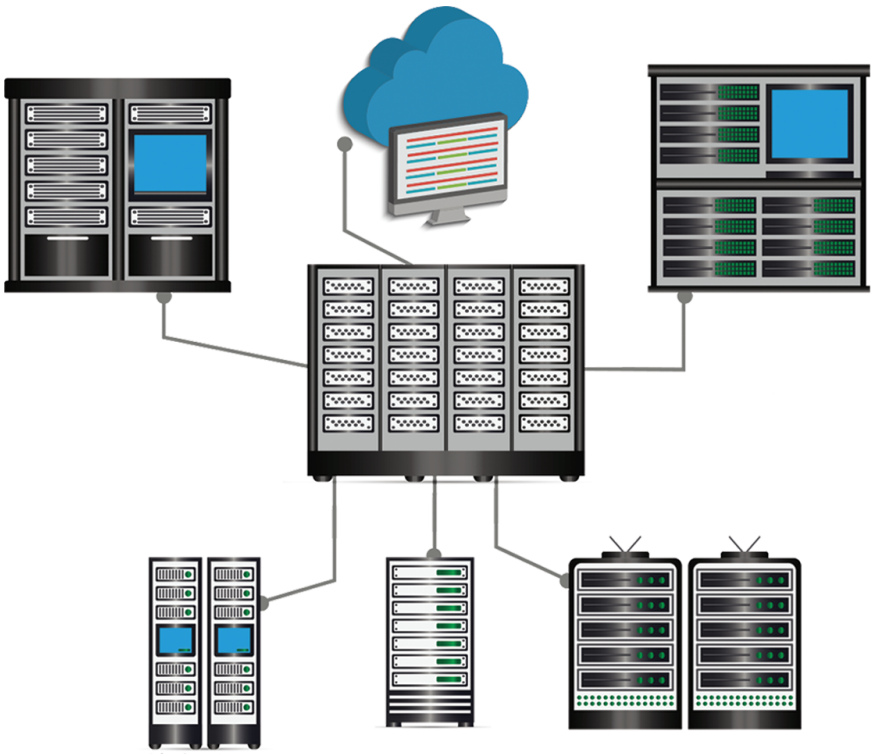
Our clients notice that partnership with Elcore Group is a respect, open knowledge change, implementation of non-standart tasks, common mutual development. Importantly, Elcore Group is a solidity, honest and long-term relationships.

Elcore

it•lab

Certificatele noastre:

The best IT services
for your business



MikroTik

UBIQUITI NETWORKS

CISCO

Hewlett Packard Enterprise

aruba
a Hewlett Packard Enterprise company

FORTINET

facebook

(022) **855-975**

sales@it-lab.md
info@it-lab.md

Str-la Studentilor 2/4, office 217

www.it-lab.md

rapid LINK
The best connection ever

Compania SC «Rapid Link» SRL – integrator de sisteme în Moldova, propune soluții profesionale pentru bănci, instituții publice de stat și întreprinderi mari și mijlocii.
Misiunea noastră este de a asigura tranziția eficientă a tehnologiilor vechi spre cele mai noi tendințe, care corespund solicitărilor pieței.

Fiind în tandem cu noile tendințe și cu tehnologiile noii generații, Rapid Link prognozează succesul afacerii Dvs și oferă:

Servicii de Telecomunicații - soluții pentru operatori TIC sau utilizatori finali de transport de
date securizat, lease- line, Internet, IP telefonie, etc.

Servicii de mentenanță IT - Rapid Link asigură mentenanța IT pentru calculatoare, servere și rețele informatice pe baza de abonament lunar, de asemenea intervenții la cerere, sau de cîte ori este necesar.

Implementare software - în prezent implementam proiecte software personalizate pentru clienți din numeroase domenii, software care doar conțin informații, care administrează informații, cele care oferă informații sau care le integrează pe toate cele trei.

Servicii centre de date - centru de date categoria Premium. Soluții complexe pentru managementul sistemelor informaționale. Un centru de date certificat externalizat este mult mai ieftin decât propriul centru de date.

Servere dedicate - Posibilitatea de a închiria numărul necesar de servere, fără o investiție inițială de capital. Nici un cost pentru întreținere și reparații de hardware. Acces la distanță și siguranță a propriilor sisteme informaționale corporative.

Construirea rețelelor de curent slab - proiectare, soluții integrate, construcții, deservire garanție și post - garanție a rețelelor LAN.

Mun. Chisinau, str. Gh. Asachi 71/7
www.rapidlink.md
sales@rapidlink.md

Economic Policy Advice to the Moldovan Government

Background

Economic growth in Moldova requires a higher dynamic – both quantitatively and qualitatively – to generate a sustainable and inclusive development. Moldova's employment rate was only 40% in 2019 (44.2% for men, 36.5% for women), while EU average is around 70%. Insufficient employment opportunities and a pertinent need for reform induce sizable parts of the population to migrate. A significant number of new jobs is needed to meet the long-term demand of the unemployed and underemployed as well as returning migrants. Furthermore, the existing jobs are unequally distributed between urban and rural areas and between men and women. Persons with high poverty risks, such as ethnic minorities and persons with disabilities, struggle to access the labour market. Overall, it is to be stated, that Moldovans do not have enough opportunities to obtain sufficient income on a regular basis.

Against this backdrop, Moldova has initiated reforms with the objective to become a more attractive investment location. Private investments, both foreign and local, generate jobs and improve living conditions. Attractive labour costs and the fact that Moldova is part of international free trade agreements remain important preconditions for employment generating investments. The further improvement of the general business and investment climate as well as the support structure for individual investors is as important as the dissemination of the positive economic developments to all regions of Moldova and all parts of society, including the most vulnerable ones.

Project goal

The objective of the project is to enhance the opportunities to participate in inclusive growth.

Basic information

Time frame: 01/2019 – 06/2022

Commissioning parties:

- Federal Ministry for Economic Cooperation and Development (BMZ) with a volume of EUR 3.25 m;
- Swiss Agency for Development and Cooperation (SDC), with a co-financing volume of EUR 1.8 m;

Implementation partner: State Chancellery of the Republic of Moldova

Further partners: Ministry of Economy and Infrastructure; Ministry of Finance; Ministry of Health, Labour and Social Protection; Investment Agency; Parliamentary Committee for Economy, Budget and Finance; authorities of the Autonomous Territorial Unit of Gagauzia

Project approach

The project comprises advisory services in the following four, mutually reinforcing, areas:

Output 1: Enabling framework – policy advice for sustainable economic development supports reforms in line with social market economy principles to strengthen competition, enhance social security and facilitate trade. The involvement of private sector expertise and civil society actors in developing reforms play a central role in this regard.

Published by

giz Deutsche Gesellschaft für Internationale Zusammenarbeit (GIZ) GmbH

20 ANI DE COOPERARE ELVEȚIA-MOLDOVA

Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Swiss Agency for Development and Cooperation SDC
Agenția Elvețiană pentru Dezvoltare și Cooperare
Швейцарское управление по развитию и сотрудничеству

Output 2: Investment promotion – strengthening demand-oriented services for investors supports public service providers in the field of investment promotion to facilitate job creating investments. The services comprise the provision of investment relevant information and support as well as individual after-care for existing investors.

Output 3: Linkages – supporting local SMEs in becoming suppliers to foreign investors capacitates economic support structures to provide advisory services for local enterprises to integrate them into value chains of international investors.

Output 4: Disadvantaged groups – facilitating integration into the labour market by capacitating support structures to provide employment services for persons with high poverty risks (especially Roma, persons with disabilities, current and former prisoners).

Impacts achieved so far

As a result of the project´s activities in the previous phases, the creation of over **8,800 jobs** has been facilitated. One example of the direct work with investors is the support to the Japanese automotive supplier Fujikura, which opened its first plant for wire harnesses in Moldova in 2017 with more than 1,700 employees. Based on the positive experience, the company opened a second plant in 2018 in Gagauzia, employing additional 1,000 people with above average salaries in a growing and promising manufacturing sector. With support of the project, the Investment Agency reached out to the company in 2013. When the company started considering Moldova, the joint team supported Fujikura with information, scouting of relevant locations, site visits, organizing official meetings and conducting a labour market research.

37 changes to legislation in line with social market economy principles have been promoted in the same period. One example is a government decision that establishes a programme to provide financial incentives for companies, which create more than 100 new jobs. The regulation, which increases Moldova's regional competitiveness and serves as a strong incentive for labour-intensive investments, already resulted in the creation of more than 1,800 new jobs since its launch in 2018.

To enhance the economic opportunities of vulnerable groups, the project is working directly with civil society organizations while reflecting reform needs in policy reforms. To illustrate this interplay: A new regulation on social entrepreneurship now provides incentives to companies to employ vulnerable groups, while a new mechanism on supported employment facilitates the direct support to vulnerable individuals to take up work.

Furthermore, the project advised the Government and private companies to **cushion the negative effects of the COVID-19 pandemic**. This lead for example to the amendment of the labour law to facilitate remote work and to several companies switching their production to personal protective equipment, which resulted in the preservation of more than 1,000 jobs and even the creation of 100 new jobs.

Published by:
Deutsche Gesellschaft für
Internationale Zusammenarbeit (GIZ) GmbH

Registered offices
Bonn and Eschborn, Germany

Dag-Hammarskjöld-Weg 1-5
65760 Eschborn, Germany
T +49 61 96 79-0
F +49 61 96 79-11 15
E info@giz.de
I www.giz.de/en

Project description:
Economic Policy Advice to the Moldovan Government

Photo credits:
Igor Schimbator for GIZ

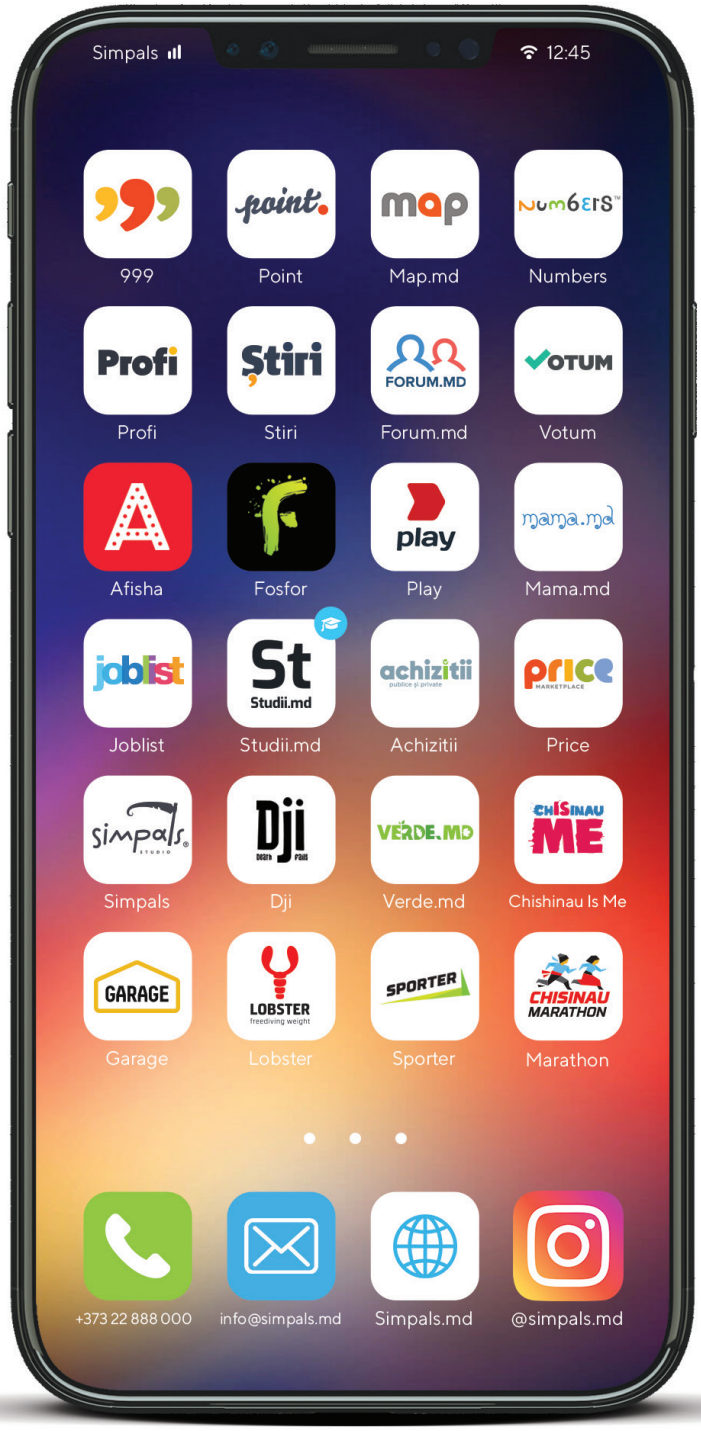
On behalf of
German Federal Ministry for Economic
Cooperation and Development (BMZ)
Division 302 - South-Eastern and Eastern Europe, South Caucasus
Michael Angermann

Chisinau, 2020

On behalf of

Federal Ministry
for Economic Cooperation
and Development

simpals®


Simpals
12:45
999
Point
Map.md
Numbers
Profi
Stiri
Forum.md
Votum
Afisha
Fosfor
Play
Mama.md
Joblist
Studii.md
Achizitii
Price
Simpals
Dji
Verde.md
Chishinau Is Me
Garage
Lobster
Sporter
Marathon
+373 22 888 000
info@simpals.md
Simpals.md
@simpals.md

MOLDOVA
CYBER WEEK 2020

www.moldovacyberweek.md