VOL 1 (2016) ISSUE 1

EUROPEAN CYBERSECURITY MARKET

RESEARCH, INNOVATION, INVESTMENT

THE KOSCIUSZKO INSTITUTE

EUROPEAN CYBERSECURITY MARKET

RESEARCH, INNOVATION, INVESTMENT

European Cybersecurity Market is a new publication designed to promote innovative solutions and tools in the field of cybersecurity. In order to raise awareness and increase cooperation in the developing digital economy, this periodical will be openly distributed to all interested parties and stakeholders.

European Cybersecurity Market is a quarterly publication.

THE KOSCIUSZKO INSTITUTE

Published by:
The Kosciuszko Institute
ul. Feldmana 4/9-10
31-130 Kraków, Poland

Phone: 00 48 12 632 97 24
E-mail: robert.siudak@ik.org.pl

www.ik.org.pl
www.cybersechub.eu

CO-FINANCED BY

European Funds
Regional Programme

KRAKÓW REGION
MAŁOPOLSKA

European Union
European Regional
Development Fund

FOREWORD

ROBERT SIUDAK
Chief Editor of European Cybersecurity Market
CYBERSEC HUB Project Manager
Research Fellow of the Kosciuszko Institute, Poland

The unprecedented rise in our dependency on ICT technologies, both in our work and private life, has significantly changed the rules of the game. Cybersecurity is no longer a distant and secondary problem managed by IT "geeks". It has become a vital part of our businesses, our financial activities, and our personal lives, and thus a force to be reckoned with.

According to different surveys, 60% to 90% of us do not feel secure in cyberspace. The manner in which to approach the fundamental problem of ICT vulnerabilities is one of the key challenges our world is facing today. On the one hand, it is a strategic challenge for national governments and international institutions. On the other, the very nature of the Web and network technologies promotes the role of the private sector as the best source of innovative solutions. This is where we come into the picture...

We are proud to announce the launch of European Cybersecurity Market (ECM), a platform where all key stakeholders can present, discuss, and share their ideas concerning the commercial side of secure cyberspace: from investments, through research and development, product and service provision, to monetisation, future trends and technological predictions.

As it was widely discussed during the European Cybersecurity Forum – CYBERSEC 2016 that took place in September in Poland this year, there are a number of key issues which Europe needs to address in the coming years. Among them is the quest for the European model of the cybersecurity market that will help answer the following questions: how to enhance global competitiveness of European cyber-products and cyber-services? How to support cyber-innovations and which technologies might provide the best security solutions for the second digital revolution driven by the Internet of Things? We believe that ECM has every chance to become a leading platform for tackling these as well as a number of other cybersecurity challenges.

This first issue of our quarterly is a prime example of such an ambitious programme. Inside, you will find articles by contributors from a wide range of cybersecurity sectors: startup representatives, SME CEOs, experts from technology transfer centres and academia. Their analyses, opinions, interviews, and policy reviews are voices to be heard and valued in the ongoing debate about our cyberfuture.

It is my great pleasure to present to you this very first edition of our European Cybersecurity Market. I truly hope it will be an informative, enjoyable and relevant read that will also stimulate further debate about the role of the cybersecurity market in securing our digital world. At the same time, I would like to invite you to take part in this discussion by contributing to our journal. ECM is an open platform built in collaboration with stakeholders from different sectors and backgrounds. Join us and have your say on things that matter most on the cybersecurity markets.

Robert Siudak

CONTENTS

With the Industrial Revolution 4.0 having come to reality, the current shift in workforce expertise is founded on digital skills that, on the one hand, are increasingly demanded by the private and the public sector, but on the other hand are poorly supplied to the market.

JAKUB KRUSZELNICKI

In addition, the current debate about cybersecurity education is missing a bigger picture – namely, it fails to address the problem of unfilled positions for cybersecurity specialists. In this context, all parts of the equation share the same interest in educating and training cybersecurity professionals, which requires a consistent framework and a long-term strategy.

The market is in constant evolution and the cybersecurity (CS) experts are becoming strategic players in any IT-related industry. McAfee's conclusion on the actual state of play of cybersecurity summed up in 2012 Threats Report[1] is that "the areas of cybercrime, hacktivism, and cyber warfare are in a continual state of evolution and, in certain cases, revolution. Governments, enterprises, and consumers face a wide range of digital threats from these forces." These facts are putting added pressure on governments and the private sector, emphasizing the uncertain future of their assets. The unstable future can be affected by unfilled positions and delayed knowledge transfer to the CS area. The attention on CS issues is rising in parallel to threats emerging from the ITC market: "It is not enough for the information technology workforce to understand the importance of cybersecurity ; leaders at all levels of government and industry need to be able to make business and investment decisions based on knowledge of risks and potential impacts"[2].

Cybersecurity stakeholders should approach this challenge in a more complex manner, i.e. by recognizing a multidimensional nature of cybersecurity education. According to the report conducted by one of the leading cybersecurity companies, the facts are straight: a global figure of demand is at one million now and will rise to 6 million by 2019[3]. Moreover, the data published by the European Commission indicate that the demand for professional ICT workers in the IT domain across many sectors in Europe is growing at a rate of approx. 3% annually and it could amount to ca. 825,000 unfilled vacancies for ICT professionals by 2020[4]. Therefore, the focus on "cybersecurity modules" should be appropriately reflected in computer science courses and, to some extent, in traditional courses such as law, international relations, economics, management, psychology, etc.

The growing demand for stimulating the education of cybersecurity professionals has already been addressed by international organisations. The Network and Information Security (NIS) Platform has started highlighting the problem of the needs of the market exceeding the supply of specialists in the CS area[5]. Although the number of good practices is rising, the skill shortage in the area is still prevalent, with no standardization of learning curricula whatsoever even at the EU level. The shortage of CS professionals is felt most strongly in top roles where multi-disciplinary skills and extensive experience are required. In order to deal with the skill shortage, more training courses and programmes need to be created. Whilst these programmes have to create synergies with the key cybersecurity needs, they must also prepare professionals with strong basic skills for rapid changes in the technological environment. New teaching, collaboration, and internship models need to be established in order to keep abreast with the dynamic nature of cybersecurity.

Based on these assumptions, several cross-border initiatives have been started to evaluate the spread of existing CS learning curricula around the globe in order to capture and define a possible framework that could be common and implementable in different countries.

1 | Sun Bing et al., McAfee Threats Report: Third Quarter 2012, McAfee Labs.

2 | Executive Office of the President of the U.S., Cyberspace Policy Review: Assuring a Trusted and Resilient Informa-tion and Communications Infrastructure, 2009. http://www.whitehouse.gov/assets/documents/Cyberspace_Policy_Re¬view_final.pdf.

3 | Morgan S., One million Cybersecurity job opening in 2016, Forbes magazine, 2016. http://www.forbes.com/sites/stevemorgan/2016/01/02/one-million-cybersecurity-job-openings-in-2016/#58ea3287d274.

4 | European Commission, Digital Skills and Jobs Coalition, Digital Single Market information, 2016. https://ec.europa.eu/digital-single-market/grand-coalition-digital-jobs#Article.

5 | Vishik C., Heisel M., Cybersecurity Education snapshot for workforce development in the EU, Network and Information Security (NIS) Platform, Working Group 3, September 2015.

On the one hand, the NIS Platform Working Group (WG3) on Secure ICT Research and Innovation identified a snapshot of the education and training landscape as one of the input deliverables needed for the creation of the Network and Information Security Strategic Research Agenda (SRA)[6]. On the other hand, the ECESM project[7] has been designed to enhance the overall cybersecurity posture by accelerating the availability of educational and training resources intended to improve the cyber behaviour, skills, and knowledge of every segment of the population.

As the above-mentioned studies show, the most advanced countries have already implemented such pilot activities that public administration uses to stimulate the development of cyber education curricula. The examples of such initiatives come mainly from the USA and the UK:

- **The National Science Foundation CyberCorps® SFS programme**
  (USA) is designed to increase and strengthen the cadre of federal information assurance professionals who protect the government's critical information infrastructure.
- **The National Cyber Security Programme**
  (UK) is a five-year government and industry partnership backed with £860m of funding to improve security and resilience.
- **The National Initiative for Cybersecurity Education[8]**
  Led by the National Institute of Standards and Technology (USA) which provides the National Cybersecurity Workforce Framework to define the cybersecurity workforce and provides a common taxonomy and lexicon to classify and categorize workers.

However, the existing cybersecurity educational programmes suffer from limitations when it comes to focus and the unity of efforts. In order to effectively ensure continuous technological advantage and face future cybersecurity challenges successfully, cybersecurity education should be built around technologically skilled and cyber savvy workforce and provide future experts with adequate skills.

During the 2nd edition of the CYBERSEC Forum in Krakow we had the pleasure to hear different interdisciplinary expert opinions on how to prepare ourselves for the upcoming necessity to generate new professional profiles that would fill in the emerging niche on the IT market. We tried to look at the staff generation issues from different points of view, taking into account two perspectives: the institutional TOP-DOWN approach, represented by the public administration and other international organisations as well as the BOTTOM-UP perspectives of academia, NGOs, and business. After a short discussion during the event, we formulated the following common statement:

"For the future of cybersecurity we need more cooperation between academia, public administration, and business in the format of PPPs." *Amelia Phillips, Highline College*

We were able to define the end-to-end value chain by looking at different examples of best practice from all over the world, from North America, Europe, and South Africa to some more "surprising" countries such as Namibia or Moldova. They all showcased great ability to generate strong and sustainable approaches to solve the problems at different stages of the process, but they had one weakness: they were disconnected and did not cover the entire pipeline, from basic education to strong market absorption. In this sense, it is necessary to show the main recommendations for building CS workforce as a comprehensive, integrated value chain that would be built upon success stories presented by the best-practice roadmap involving public administration as resources, legal framework providers strongly connected with academia and industry as well as bottom-up inclusive actions emerging from IT-focused NGOs.

6 | Op. cit. Vishik and Heisel.

7 | ECESM, Enhancement of cyber educational system of Montenegro, Cyber Crime 2014 conference, 12-13 November 2014, European Commission Tempus Project: 544088-TEMPUS-1-2013-1-SI-TEMPUS-JPHES.

8 | Op. cit. Vishik and Heisel.

JAKUB KRUSZELNICKI

Jakub Kruszelnicki is working in EU-funded projects since 2007 starting from collaboration with Cracow University of Technology. During his Master Studies (European Integration on UAB) he was involved in FP7 proposals development for GEDIME investigation group. After studies, the internship in European Institute of Public Administration has expanded his experience to other EC calls (EuropeAid). Since February 2010 he was working in LEITAT Technological Center as International Project Manager responsible for NMP area. After 2 years in LEITAT, in September 2011, Jakub was assigned as Responsible for International Projects to KIM SLU where he is in charge of International Projects managing ongoing European projects and looking for opportunities to join European consortia, as well as coordinating proposals for KIM. After establishing European Projects Office with 6 FP7 projects gained the responsibilities of Jakub have been extended from European to international scope assigning the role of opening new markets in Latin America (Mexico, Colombia, Argentina) as well as European (Eastern Europe). Starting from November 2014 Jakub has relocated to Cracow and assumed the charge of Director of Technology Transfer Centre of Cracow University of Technology, at the moment he is supervising staff of 30 persons divided into 3 teams: Commercialization, Structural Funds and Framework Programmes. The Office is at the same time Regional Contact Point for H2020 as well as Europe Enterprise Network office. Additionally Jakub supports creation of special purpose company for launching spin-off initiatives.

This brief outline of the possible method to be further developed has also been inspired by one of the CYBERSEC panellist:

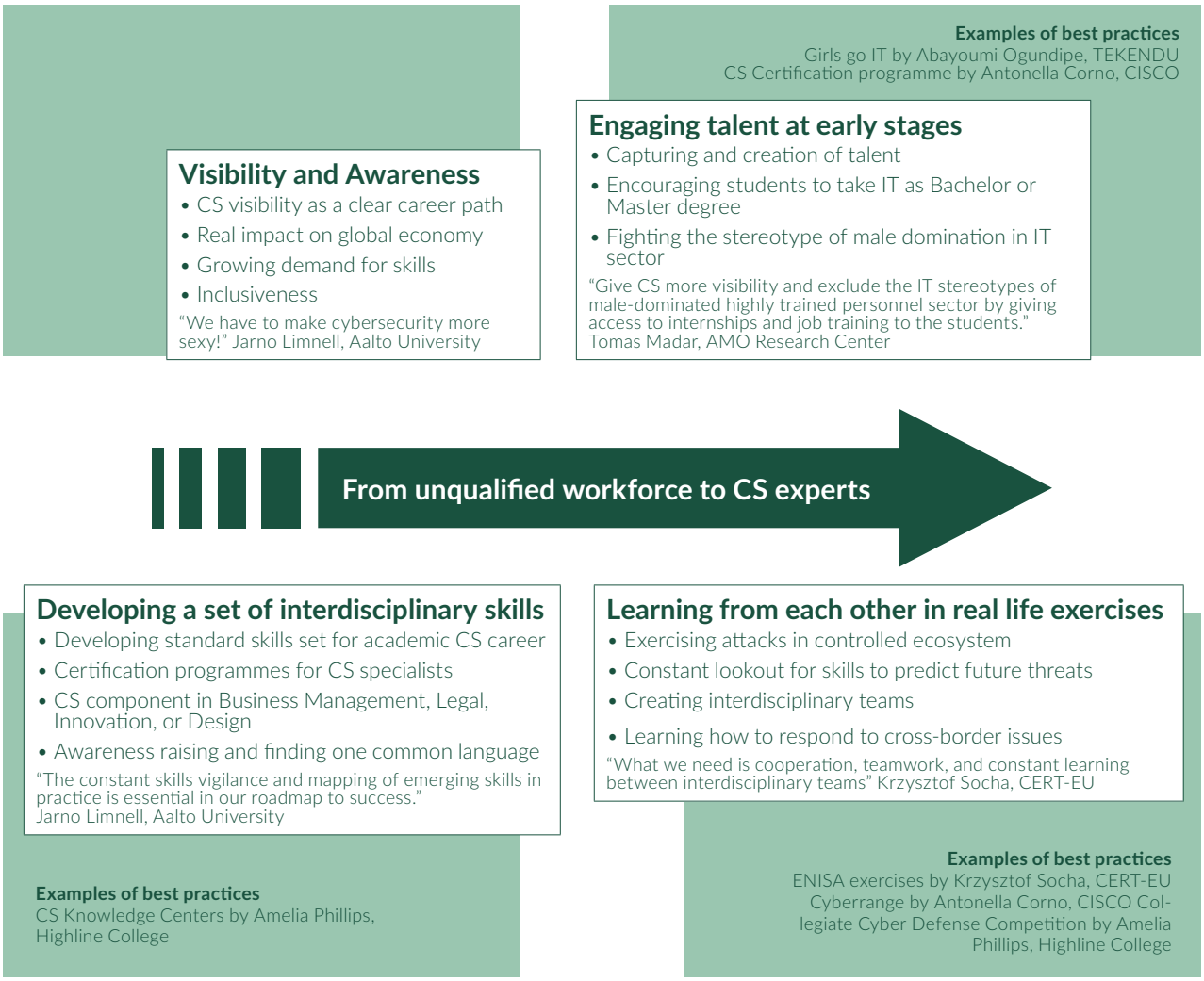
"Scale up existing best practices and stimulate cross-border cooperation." *Dan Cimpean, Deloitte*

Looking at the value chain from the point of view of best practices, we can divide it into different stages of staff development and knowledge acquisition, taking into account both professional path requirements and individual motivation factors. In this sense, the overall challenge that the CS sector workforce is facing right now is creating a pipeline that would cover all those afore-mentioned processes, from boosting visibility to delivering constant improvements in the knowledge of high-level CS experts.

"The challenge is on ramping up the educational process by creating a complete pipeline of the workforce from academia to industry, and connecting the existing dots of best practices into a sustainable ecosystem."

Antonella Corno, CISCO

To respond to this challenge, it is necessary to group the stages of CS expert's professional development into an interrelated process strengthened by the existing examples of initiatives that could create a basis for a complete workforce creation value chain.



Following the CYBERSEC breakout session "Preparing Workforce for Upcoming Cyber Challenges", we have established four areas of intervention that could fit into the pipeline as different stages of professional development activities.

1st stage of the value chain stimulation is a qualitative change in the perception of cybersecurity as a clear career path, able to make a real impact on the global economy by showing security as a thrilling adventure and not a purely men-oriented and "only-for-gigs" profession. As Jarno Limnel, Professor of Cybersecurity Studies at Aalto University, stated, we have to make cybersecurity more "sexy" for young people.

2nd stage would be the capturing and creation of talent among disadvantaged groups such as youth, women, or post-military collectives. This can get us to reach out a very wide scope of workforce that does not seem to be potential staff at the moment. Good examples of such inclusive initiatives are programmes like Girls go IT[9], presented during CYBERSEC by Abayoumi Ogundipe from TEKENDU, or the CS Certification[10] programme introduced by Antonella Corno from CISCO.

3rd stage, represented by academic actors, is the one that would professionalize students by developing a set

9 | See more at: http://girlsgoit.md.

10 | See more at: http://www.cisco.com/c/en/us/training-events/training-certifications/certifications/specialist/security/cybersecurity.html.

of necessary and interdisciplinary skills in order to not only create high-level professionals, but also enable them to work together and look at problems from different perspectives: IT, business management, law, innovation, or design. This diversity of views should underlie the CS value chain. The challenge is to activate them by raising awareness and finding one common language that could connect them through linguistic codes based on a variety of professional expertise. These kinds of initiatives were presented by Tomas Madar from AMO Research Center in the Czech Republic, or by Jarno Limnel, Professor of Cybersecurity Studies at Aalto University in Finland. Also the creation of CS Knowledge Centres that learn from each other is the best practice to follow up with Amelia Phillips from CIS and Computer Science at Highline College in the USA.

4th and last stage, i.e. predicting the future of cybersecurity by learning from each other in real life ecosystems, proves the biggest challenge once we have filled the gap in the supply of highly qualified cybersecurity experts. All the speakers agreed that at this most sophisticated level of career development, the interdisciplinary approach of exercising new threats by simulation is the tool that stimulates the most. The dynamics of learning from each other not only gives the high-level experts the ability to predict, but it also keeps a sharp lookout for skills that need to be incorporated into the educational value chain. In this context, the best practices were introduced by Krzysztof Socha from CERT-EU showing the example of ENISA exercises[11], followed by programmes such as Cyberrange[12] by CISCO or Collegiate Cyber Defense Competition[13] showed by Amelia Phillips.

Only a complete approach covering all those stages can lead us to success. This complex challenge has to involve all the actors and has to be linked to existing initiatives connecting the dots and working together for constant improvement. The CYBERSEC breakout session exercise showed us a common understanding of the problem and emphasized the urgent need to react. This approach has also been adopted in the ECESM project[14] which has identified the following key initiatives of prime importance:

- increase awareness and expertise;
- treat security education as a global issue;
- approach security comprehensively, linking technical and non-technical fields;
- seek innovative ways to fund labs;
- pursue real-world projects and advance a "science of security".

As we can see, different experts working in the CS environment are demonstrating a common approach that should be implemented en masse. By breaking down barriers and working in concert, it is possible to better address current and emerging challenges. The multi-disciplinary approach that is needed to feed multi-disciplinary programmes also continues to be fragmented. Although a great effort has been made to support these approaches to cybersecurity, funding resources and the availability of publications and conferences that engage multi-disciplinary work are still insufficient. Finally, the fragmentation of cybersecurity knowledge impacts all aspects of society, from the technological environment to legal and policy frameworks. In order to deal with the lack of skills, more training programmes will need to be created to respond to crucial cybersecurity needs and, at the same time, prepare professionals with strong basic skills for retraining as the technology environment changes. New teaching, collaboration, and on-job training models will have to be created in order to respond to the constantly evolving nature of cybersecurity.

Following the above-mentioned examples, it may be necessary to start with the creation of a repository of best practices in cybersecurity. Such project-specific compilations initiated by the private sector or academia already exist, thus we hope the cybersecurity community expands its potential in order to ramp up cybersecurity education across the EU. ■

11 | https://www.enisa.europa.eu/topics/cyber-exercises.
12 | https://www.servicesdiscovery.com/en/article.php?idx=218.
13 | http://www.nationalccdc.org.

14 | ECESM, Enhancement of cyber educational system of Montenegro, Cyber Crime 2014 conference, 12-13 November 2014, European Commission Tempus Project: 544088-TEMPUS-1-2013-1-SI-TEMPUS-JPHES.

We project, implement and support:
- wire LAN networks
- wireless LAN networks
- IP VPN building
- Firewall UTM systems
- Network managing and monitoring applications
- AAA access authorization systems
- Web security and filtering systems
- E-mail security and filtering systems
- load- balancing systems
- telecommunications and IT audits

ASESKO ICT
Information Communication Technology

Asesko ICT provides advanced IT solutions including telecomunications and safety for LAN and WAN Network.

We are specialized in selling combined solutions for computer Network safety based on installation, configuration and trainings for computer Network administrators.

Many customers wonder how to secure their IT sources efficiently. In the beginning the IT audit should be carried out.

Thanks to the audit ASESKO ICT will be able to design the most optimum technical and cost-based solution.

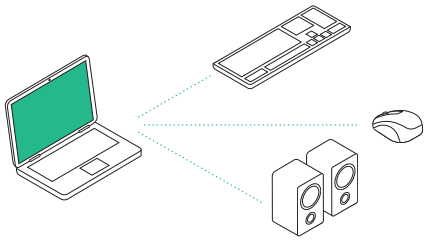
In our company we have experienced engineers with many certificates from leading IT providers (FortiNet, HPE, CheckPoint, Cisco) and managers for whom the customer satisfaction is the most important point. We put on perfectionism, predictability and long-term cooperation.

www.aseskoict.pl

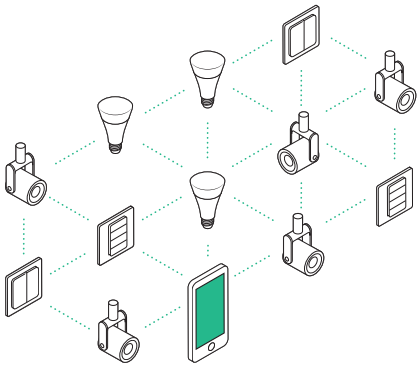
The lighting sector is going through a particularly exciting period these days. Software and wireless technologies are turning upside down the more-than-century-old lighting control paradigms, and traditional lighting standards are being challenged by connected lighting systems that promise to deliver so much more than just a well-lit space. However, this collision of the worlds of IoT and lighting is still in its infancy, and there are challenges that need to be overcome. Security is one of them.

In addition to being a platform for big data, connected LEDs are also a tempting target for cybercriminals. Lighting systems are becoming more and more integrated with building automation controls, which amplifies the potential harm caused by a successful attack. Disappointed with the capabilities of available low-power communication protocols – both in terms of network performance and security mechanisms – the Polish startup Silvair has built a proprietary mesh technology based on Bluetooth Smart which enables robust communication in the company's commercial smart lighting platform. It has performed so well that multiple concepts developed by Silvair are now being used as the foundation for Bluetooth Mesh, a new flavour of the good old Bluetooth. It is expected to be adopted early next year so we're yet to see its full specification. But according to **Szymon Słupik, CTO at Silvair** and Chair of the Mesh Working Group at Bluetooth SIG, it is the first wireless communication standard designed with commercial lighting applications in mind, ensuring wire-like reliability and performance, as well as government-grade security. It will be interesting to see how Bluetooth Mesh tackles security challenges. In the IoT, security is paramount but most difficult at the same time. That's because of the resource-scarce nature of IoT devices which typically have very small storage and very low processing power.

Topology of Bluetooth® Classic



Topology of Bluetooth® Mesh



A new European Public-Private Partnership on cybersecurity

Interview with Luigi Rebuffi

Secretary General of the European Cyber Security Organisation

Sir, the public-private partnership on cybersecurity is the key endeavour that should lead to the development of European market of products and services. Why do we really need European solutions?

European solutions are needed to ensure a certain level of Europe's digital autonomy and to protect the Digital Single Market. In Europe, we have a lot of solutions being developed and produced by global companies, originating mainly from the United States or from Asia. But Europe has different sensitivity requirements that are specific to each Member State and stemming from sovereignty and national prerogatives, such as the exchange of information. This allows the national administrations of European Member States to retain some control over their cybersecurity. For this reason, we have to foster a certain degree of digital autonomy and develop an offering for adequate cybersecurity solutions that are in line with these specific needs. These solutions must be closely linked and consistent with solutions developed and produced by companies based outside Europe. I believe it would be counterproductive for Europe to start developing all types of solutions from scratch, thus wasting large amounts of money that could be invested elsewhere. Therefore, it is necessary to support the development of adequate European solutions following a strategic investment plan.

What kind of participants would you like to have involved in this initiative?

For the public-private partnership to work successfully, we require a wide spectrum of participants, including both public and private stakeholders. We need to engage all private actors, from ordinary citizens to different infrastructure operators like SMEs and large companies that can be both solution providers and end-users. In parallel, since national, regional and local administrations should be considered an essential stakeholder, it is also important to involve them as well. Finally, as cyber is part of our everyday life, I would say – everyone is touched by it and should therefore join in.

What are the objectives and priorities for the public-private partnership?

The overall objective of this public-private partnership with the European Commission is to support the growth of the Digital Single Market. This is why we need to develop European solutions. This is really the role of the public-private partnership: to support research and innovation. Our goal is to facilitate the growth of a European cybersecurity industry which is competitive both locally and globally.

We have to find the right balance between solutions that must be developed in Europe to address our region's specific needs or requirements, and solutions coming from abroad that can be tested and then certified. All these elements comprise a trusted supply chain.

What do you think about the European Cybersecurity Forum?

This Forum is growing every year and has already become a major event in Europe. During this year's edition, there was a real debate and the opportunity to get interesting feedback on the discussions we had. I would like to congratulate the organisers on such an excellent event, especially the Kosciuszko Institute on their ambition to build a Polish cyber community and set up a practitioner hub for European and international stakeholders. CYBERSEC brings us together and allows us to learn from each other. I believe this event will continue to grow in importance and increase its visibility in Poland and throughout Europe.

ABOUT LUIGI REBUFFI

Luigi Rebuffi is the CEO and founder of the European Organisation for Security (EOS) as well as the Secretary General (and Chairman of the Board ad interim) of the European Cyber Security Organisation (ECSO). Having graduated from the Politecnico di Milano in nuclear engineering, he worked on the development of high power microwave systems for the next thermonuclear fusion reactor (ITER).

He continued his carrier at Thomson CSF/Thales where he took on increasing responsibilities for European Affairs (R&D) in different sectors: telecom, industrial, medical, and scientific, eventually becoming Director for European Affairs for the civilian activities of the Group in 2003.

In 2007, he proposed to create EOS and coordinated the efforts to establish it while still holding the position of Deputy Director for Security at ASD. He is a member of the Protect and Security Advisory Group on EU Security Research and President of the Steering Board of the French ANR for security research.

About the European Cyber Security Organisation

ECSO is a non-for-profit organisation established in June 2016 under the Belgian law. It represents an industry-led contractual counterpart to the European Commission for the implementation of the contractual cybersecurity Public-Private Partnership (cPPP). ECSO members encompass a wide variety of stakeholders including large companies, SMEs and start-ups, research centres, universities, clusters and associations as well as European Member State's local, regional, and national administrations, countries that are part of the European Economic Area (EEA) and the European Free Trade Association (EFTA) as well as H2020 associated countries.

The main objective of ECSO is to support all types of initiatives or projects that aim to develop, promote, and strengthen European cybersecurity. It particularly aims to:

- Foster and protect the growing European Digital Single Market from cyber threats;
- Develop the cybersecurity market in Europe and contribute to the growth of competitive cybersecurity and ICT industries with an increased market position;
- Develop and implement cybersecurity solutions for the critical steps of trusted supply chains in sectorial applications where Europe is a leader.

Concrete actions to achieve these objectives are among others:

- Collaborating with the European Commission and national public administrations to promote Research and Innovation in cybersecurity;
- Fostering market development and investments in demonstration projects and pilots to bring innovation to the cybersecurity market;
- Supporting the widest and best possible market uptake of innovative cybersecurity technologies and services for professional and private use;
- Promoting and assisting in the definition and implementation of a European cybersecurity industrial policy;
- Supporting the development and the interests of the entire cybersecurity and ICT security ecosystem.

Find out more at www.ecs-org.eu. ■

Sandbox for secure project management

BŁAŻEJ MARCINIAK
is the Founder & CEO of Sher.ly. He is a network security and data transmissions technologies expert. After 20 years of experience in ICT, the lack of suitable security in communication services was the reason to start working on Gateless VPN technology.

Everything is a project, really. In this article, we want to focus on data related projects and propose a better way of managing shared data without compromising security.

Data sandbox concept for business project teams

When a new business project is formed, the team involved usually starts with project kick-off meetings, emails, calls, and chats to discuss the scope of work lying ahead. Emails become a synonym for "nothing urgent" and countless "FYA" and "FYI" threads rapidly fill our inboxes. The best way to get things done is by getting people involved in a distraction free environment, focusing on the issue at hand. It is easier for people than data which lives in countless locations and is hard to gather together in one place. There are many tools available for cross business teams to collaborate, like Dropbox for Business, Slack, Teamwork, Basecamp, Asana, Trello, and many others; yet they share one common denominator: the user must choose between security and convenience. Most services work well in a convenience mode, but all the data is exported and owned by the service in question. You can find a way to use some of those tools in a secure mode, under your own control, but it tends to be complex and far from convenient.

Our goal was to find a tool that is both secure and convenient to use.

In software development, a “sandbox” is a dedicated testing environment that isolates untested code changes and outright experimentation from the production environment or code repository.

A sandbox for business is like a virtual room created to have a project meeting. Over time, we bring more information and put it in the room for other team members to use. Each project member can use the materials and take what they need, instead of getting a full copy of whatever is in the room. Another factor here is that the room is not connected to the rest of our office infrastructure, and only invited people have the “keys” to that room. To maximise the benefits, data should be synced in a smart way and separated from the devices on which it is stored.

Why does it matter?

A common Project Manager’s headache is information flow; how to make sure everyone knows what they need to know and is not being flooded with too much information? Notifications are a typical problem: too few cause frustration and miscommunication, too many are just noise.

A common requirement from a new client or a business partner in a project of a confidential nature is “I want to know who is doing what with my data, and when this is being done”. This means an on-demand virtual room or a data sandbox is needed. Better still, if it is so easy to set up that no IT guy is needed to get it done.

Have a closer look at a use case

Back in my pre-start-up life, I had the pleasure to manage a project for the first mobile transaction system for one of the leading online banks in Poland. Today, it is a synonym for online banking in Poland, a ubiquitous and versatile system working in every browser and on any mobile device. It was the most challenging project I have managed so far, yet the people involved were phenomenal. Yes, we were encountering issues on a daily basis, finding problems under every rock, but with the "can-do" attitude we were able to "tear off the head of each hydra" we came across. Obviously, security and project confidentiality was a big concern, both from a pure IT standpoint and a marketing perspective as a big announcement was planned.

200 MB project brief file and a team meeting in an hour? That's... Tuesday

We started with designing a whole new user experience for mobile, an uncharted territory. Although Marketing and Business teams had nailed down the desktop experience well, mobile was an experiment. I had quite a difficult role explaining the mobile platform possibilities and limitations to the business and marketing people, which was key to designing the best user experience. We exchanged hundreds of ideas each week, and a picture is worth a thousand words. The project brief quickly grew to a whopping 200 MB Word file, mostly because of screenshots and brainstormed versions of each app screen. We had weekly meetings over video and each person edited a brief file from the last meeting for delivery to all project members; usually, the lucky winner was a PM on the developer side (me) or my counterpart in the bank.

...just throw it in Dropbox and email the link to everyone. Simple enough, eh?

This is a bank and this is a top security project. Dropbox is not allowed. Skype is not allowed. Any form of a third party service has to be approved by the IT department first. And they are busy, very busy. It is not a matter of cloud storage which risks being hacked. Executives at the bank will not debate encryption with a contractor: if you expose any confidential data, you are liable to the full value of a contract. A "bit" high stake to rely on Dropbox or another cloud. So we used crummy FTP servers.

It was no fun trying to guide people over the phone as to which link they need to click, how to merge a broken file link by email and so on... File context? We tried to stuff the filename with the whole document history, which made it even more difficult to distribute: project%20version_3.1%20app-release%20c-B_MC.AB.docx

- *Hey, have you seen the latest revision?*
- *Umm, which is the latest?*
- *The one I wrote to you about in my email on Monday.*
- *Which email was that? [...] Got it. Downloading now... Oh wait, it doesn't work.*
- *What do you get?*
- *No such website?*
- *Do you have the whole link in the address? Does it end up with .doc or .zip?*
- *Hmm... no.*

Secure site-to-site VPN? Sure. Wait for it...

It took us three months to set up a secure site-to-site VPN connection to access several levels of development platforms. It was not because of a lack of good will, it was because of the level of complexity and corporate departments involved. We had to wait for network configuration, then again for VPN tokens. We were able to deliver new software packages to integration teams which had a huge headache working out which version was the latest: are we really testing the version we are supposed Is the bug related to an upgrade gone wrong or to something else? We had to create separate sub-projects to figure out package naming procedures, and to make sure everyone involved knew which was which. It was easy to get lost in 40+ versions for the server and client side, all changing rapidly. VPN-based networks offer good security, but they are complex to set up and maintain.

Typical scenario:

- Guys, the tokens we use are about to expire (a month left)
- Hello, these tokens are walking out on us (two weeks left)
- Hey! In a week we won't be able to work! (one week left)
- Guys? Weren't we supposed to get the new package revision yesterday?
- Yes, but we are cut off from the network. VPN tokens have expired.
- Really? Why didn't you say anything?
- [...] stunned silence.

Although it was really hard work (especially in the communication field), I am very proud to have been part of this project. A few months after the launch, the mobile transaction platform was used by over 800 000 XXX customers.

In 2013, I entered the market with Sher.ly, a start-up dedicated to creating innovative software for file sharing among business organisations, on desktop and mobile devices. Sher.ly is a SaaS data smart syncing and collaboration service for business. It delivers a new way of sharing your sensitive files with your co-workers and business partners by creating an on-demand, secure, and invite-only network. It works like a cloud, but data stays on your own storing device.

Create a sandbox via Sher.ly

Using Sher.ly, every Project Manager can easily create a closed data sandbox using their own computers, without calling IT. Simply create a folder for a project, invite people and add the data they are supposed to see. Files are shared but nothing is uploaded to a “cloud” because Sher.ly works with data directly from your computer or other data storing devices without accessing the device itself.

Sher.ly does not host your files

Every file or folder you add to a project will be analysed by the Sher.ly software. The metadata of that file will be generated containing key information about it such as its name, size, extension, creation date, modification date, and checksum. The application uses the latest secure file transfer encryption protocols and allows you to track the full history of file sharing with individual users. With this solution, the owner of the file has full control of data confidentiality and can control the identity of the recipients from the start.

The files are immediately visible in your Sher.ly app thanks to its intelligent metadata synchronisation, which allows you to set preferences for sync and access depending on the project you have created, device you have used, as well as file name, file size, modification date or a sharing party. There are no bulk uploads and

downloads, no data size limits – only encrypted metadata that is synced to your Sher.ly account, your other devices, and your invited project members.

Timeline for data context

Data itself is just raw material. To make use of it, we need the context and purpose it serves. That is why shared space for files on its own does not solve all needs because filling the space with data alone does not say much to other team members. To communicate effectively, we have added a Timeline, a chat-like auditing tool for every project. Each action is notified and going backwards to review steps taken by each member is easy. Deadlines are easier to follow up on and less email is the best thing for everyone. Mentioning a specific file to a team member makes it easier to coordinate work. Fine tuning member privileges prevents accidental overwrites, a common problem in synced data environments.

Let's go back to the use case. How well it would work if Sher.ly were there!

- First of all, Sher.ly would go to the IT Department for evaluation. Since all connections we use are secure SSL and certificate authentication based, with data being exchanged locked only to the people directly involved, it would be accepted as a better FTP working directly. It is quite easy for the IT guy to check if the app is really syncing only metadata instead of whole files, what addresses it communicates with, what network locations it moves files into.
- The Project Manager would update a 200 MB project brief file and simply put it into a shared project folder, all members would sync it directly.
- All chatter about a particular file would happen right next to it, making it easy to find and use at once.
- The whole project file archive would be kept in order, updated and available to all project members right from the project folder on their computers.
- Even if someone does delete a file by accident, this mistake does not get replicated on other project members' computers, because only local copies are deleted – a perk of smart, metadata file syncing.
- Every project member can access and sync the files they need: dev's sync software packages, Project Managers sync only project specs and office documents, finance people can sync only spreadsheets.
- All connections are secure and direct; it is like having a VPN connection on demand.
- Each Project Manager could have separate project files managed by the same tool, with separate teams and resources:

Sher.ly is a great example of how to easily improve workflow within any business and make it highly secure. To learn more about our solution, visit

www.sher.ly
www.sherlybox.com

INTECH PK CEO and expert on commercialization, Izabela Paluch shares her thoughts on the usefulness of the Sher.ly solution for creative processes and innovation implementation.

Smart Security

Knowledge. This is the most precious asset of my 20-year professional experience, especially the knowledge gained from commercialising innovative solutions. Original know-how, ideals, expertise in business models, all this is a priceless resource that defines any company and its intellectual capital. Therefore, knowledge ought to be protected in a special way. None of us would want it to fall into the wrong hands, would we? All in all, these physical systems used for transferring and storing data and influencing a company's organisational capability, determine the management, sales power or business models. Let us imagine that our market, client, strategy, distribution channel data or available resources are lost.

How badly would our image suffer? What would be the impact of such a loss on our relationships with shareholders or new partners? These are rhetorical questions which should never be asked and answered in real life. No matter if we manage an international corporation or are the leaders of a relatively small start-up; in every case, knowledge ought to be protected in the very same way, the most effective way. As I work closely with entrepreneurs, scientists, and inventors on implementing innovative service and products, I would rather not risk making confidential data public. Any negligence in the field of sensitive data protection is equal to economic risk, both in internal and external company relations.

Let me remind you that data security should not be analysed only from the point of view of technical standards, material resources, or their functionality. We need to understand that a company's potential also comes from intangible market assets. These assets are lost simultaneously with the loss of control over material assets (e.g. our company's market position will deteriorate simultaneously with our relational capital).

I am perfectly aware of how important creativity and the opportunity for free flow of ideas between all process participants are for creating innovative solutions. Every barrier in the form of burdensome protection, so precisely described by the Sher.ly CEO, makes an optimal solution more difficult and slower to reach. It is equally important to have a chance to run real-time tests of following prototypes. Only under such circumstances can mistakes be eliminated and improvements implemented.

We should also ask ourselves for whom our product or service is being developed. The main target group is always people: managers, representatives of companies, institutions, and research centres. Our idea is to help them to work in a friendly environment, combining knowledge, skills, and experience.

Are we forced to choose between safe yet uninspiring or risky but smart creative processes? Luckily, we do have some options. The golden solution is offered to us by Sher.ly and its sandbox. It allows us to implement changes put forward by all authorised users. Hence, innovators do not have to focus on technical issues, but can fully concentrate on the functionalities and market utility of their invention. Thus, it is not just a product, but a bundle of benefits that is given to the final customer. ■

NIEBEZPIECZNIK.PL

Do you think your company would be able to protect itself against such an attack? If you would like to find out, contact us at: security@niebezpiecznik.pl

It is not cyberweapons or APT attacks that Polish companies should be concerned about. We have reached this conclusion after analysing the results of penetration tests conducted by our team in the recent years. In engagements where our client allowed us to attack their employees (and not just company servers and web applications), we had a 100% success rate. We did not even have to use malicious software, so there was no need for convincing employees to open attachments that would have infected their devices. The employees gave us what we wanted themselves, meaning particular documents or access data to company systems.

All we needed was to send several emails with appropriately adjusted content to carefully selected employees/victims. When designing phishing emails and selecting the victims, we took into account the results of one week long reconnaissance (the time when our analysts collected anything that could be gathered to learn something about the company/victim from public resources, like structure of departments, employee data, list of contractors). On the basis of this information we determined who we will pretend to act as (colleague, superior or client of the victim).

To our surprise, even technical staff fell for our fake emails and the key to success often consisted in the appropriate time when such emails were distributed.

After a surprisingly high percentage of victims (approximately 40% of company employees), it was also astonishing to see that the IT departments of all companies that were able to detect our attacks, were unable to correctly handle the incident. They either did not manage to remove our presence from their company systems completely or were unable to inform the personnel about the attack in a reliable manner to prevent people from becoming the victims.

Cybersecurity Venture Capital

"Cybersecurity Venture Capital: Investment or Necessity?" was the topic of one of the Discussion Panels held during CYBERSEC 2016 in Krakow.

Investment or Necessity?

The time when both public and private sector leaders had to be persuaded of the importance of cyber resilience is long gone. With the so-called Industrial Revolution 4.0 unfolding, cybersecurity is becoming an integral part of the manner in which countries, organisations, businesses, and societies function.

On 26-27 September 2016, the second European Cybersecurity Forum was held in Krakow. During the event, the Kosciuszko Institute, the organizer of the conference, created a platform for discussion about investments in cybersecurity. The panel devoted to this matter entitled "Cybersecurity Venture Capital: Investment or Necessity? Can We Make Money by Investing in Cyber Technologies?" gathered prominent speakers from all around Europe. The debate raised a few essential questions concerning the concept of cybersecurity investment itself and the role of venture capital as a supporting investment vehicle.

At the beginning of the debate, Paweł Surówka, PZU ŻYCIE CEO and the moderator of the session, identified several crucial challenges for the cybersecurity investment landscape in the EU:

- The magnitude of cyber threats and their cost to the general public;
- The European angle to investing in cybersecurity;
- The European approach (if there is one) towards cybersecurity investments.

European approach to the cybersecurity market

Luigi Rebuffi, Secretary General of the European Cyber Security Organisation (ECSO), began the discussion by emphasizing the importance of public-private cooperation in the field of cybersecurity. The fact that ECSO signed a contractual Public-Private Partnership on Cybersecurity (PPP) with the European Commission on 5 July this year sent a clear signal that this topic is becoming one of the top priorities for the European Union. Mr. Rebuffi observed that even though cybersecurity remains a national prerogative and responsibility of the Member States, the European level might serve as a framework to jointly define the scope of requirements and possible common solutions, synergy, and coordination in developing competences and competitiveness by investing in SMEs and startups. Thus, one of the objectives of the PPP is to support investment in research and innovation that will contribute to achieving more competitive cybersecurity industry, both internally and globally, as well as to strengthening the protection of the digital single market.

Patric Gresko, Head of Division, Innovation and Technology Investments, European Investment Fund (EIF) drew attention to other aspects of the current investment trends on the European cybersecurity market. Besides the emergence of specialised players who focus predominantly on cybersecurity, the generalist ICT investment funds still play a huge role in building the ecosystem and a friendly environment for the sector to thrive. Additionally, Mr. Gresko highlighted the added value of the VC funds such as Paladin Capital Group that offers their beneficiaries both funding and opportunities to make connections with the most significant players in the cybersecurity field such as the NSA, the GCHQ, corporate players, and academics.

Cybersecurity as an irregular investment theme

The main issue raised by Alex O'Cinneide, Managing Director and Head of Europe for Paladin Capital Group, was the fact that investing in cybersecurity is different from other investment themes and, therefore, it does require some degree of specialisation. Moreover, the state has a particular responsibility in this sector since the cybersecurity market is mainly driven by government intervention. Cybersecurity ramains a regulatory-driven investment thesis, covering a set of soft services and software which, if you looked at them 50-60 years ago, through the lens of traditional application, they would have been viewed as offensive. These are things that could cause damage; therefore, the government has to be considered an essential stakeholder, much more than, for instance, a regulator of ordinary online services or mobile apps. Investing in cybersecurity requires specialisation and a set of skills that make it a successful endeavour.


Paweł Surówka, PZU ŻYCIE CEO

Furthermore, Mr. O'Cinneide emphasized that any good company on the market looking for capital will eventually get it, which automatically raises the question: are there enough good companies and ideas on the European market? In the opinion of Andrew Boyce, Assistant Director, Cyber Research & Innovation Europe, Data, Digital & Security Directorate at the UK government, at least in the UK, there are a lot of cybersecurity companies, but still not enough of them. Therefore, the priority should be to stimulate healthy competition on the market, which would lead to the growth of a proper ecosystem. As he underlined, the priority of the UK government for the next five years is to try to develop a long-term, strategic approach to research and innovation and reduce uncertainties by allowing for long-term commitments. The cybersecurity PPP will gather industrial and public resources to deliver excellence in research and innovation and maximise the use of available funds through greater coordination with Member States and regions. The goal is to help Europe's cybersecurity industry take advantage of the booming global cybersecurity market.

Contractual Public-Private Partnership on Cybersecurity[1]

The EU will invest €450 million in contractual Public-Private Partnership on Cybersecurity (PPP) under Horizon 2020 research and innovation programme. Cybersecurity market players, represented by the European Cyber Security Organisation (ECSO), are expected to invest three times more. The PPP will also include members from national, regional and local public administrations, research centres and academia. The aim of the partnership is to foster cooperation at early stages of the research and innovation process and to build cybersecurity solutions for various sectors, such as energy, health, transport and finance.

The PPP in the area of technologies and solutions for online network security is one of the 16 initiatives put forward in the European Commission's Digital Single Market strategy. Specific gaps persist in the fast-moving area of technologies and solutions for online network security and a more joined-up approach can help step up the supply of more secure solutions by industry in Europe and stimulate their take-up by enterprises, public authorities, and citizens. Existing Public-Private Partnerships proves that they enable the partners to

The aims of the PPP on cybersecurity are to:

- build trust among Member States and industrial actors by fostering cooperation on early-stage research.
- establish a platform for discussions between stake holders in order to align the demand and supply sec tors for cybersecurity products and services by allowing the industry to understand better the requirements of end-users and customers of cybersecurity solutions (e.g. energy, health, trans port, finance).
- develop common, sector-neutral and replicable building blocks such as encrypted storage and pro cessing or secured communication. These should help ensure compatibility of solutions across bor ders, while allowing flexibility for products to be further adapted to the needs of specific markets or customers.

1 | European Commission - Fact Sheet, Commission boosts cybersecurity industry and steps up efforts to tackle cyber-threats, Questions and answers, http://europa.eu/rapid/press-release_MEMO-16-2322_en.htm (access: 26/10/2016).

grow that ecosystem, so that there is a right collocation of investment, government, and academia that enables it to support companies with potential to grow and reach the global audience.

Venture capital: is it the right investment vehicle for cybersecurity?

However, as Mr. Surówka aptly observed, the question remains whether venture capital is really the right investment vehicle for cybersecurity. It is undisputable that cyber threats are changing rapidly. Therefore, the companies have to evolve quickly and adjust to emerging challenges and market demands in order to avoid a situation in which the solutions they offer have already been provided by other players or are simply obsolete.

Richard Seewald, Managing Partner at Evolution Equity Partners, argued that it is essential for VC leaders to be able to pick out companies that are platform businesses leveraging global assets and actually building businesses that have the potential to be market leaders. Judging by the number of companies, the cybersecurity market is huge. For instance, in Israel, there are several thousand cybersecurity companies, and in the US several thousand more. That is why taking a company from small to big is essential for any venture investor focused on cyber. In this way, cyber is a good place to invest, but the investor has to be aware and experienced, which is often not the case. Most definitely, the market is growing simultaneously with the temptation to invest in cybersecurity companies.

Richard Seewald from Evolution Equity Partners (left) and Patric Gresko from the European Investment Fund (right)

Cybersecurity market size and estimated average growth perspective[2]

Cybersecurity Markets	2014 value (bln EUR)	Global market	Average growth in the next 10 years
US	26	39%	4%
*EU (c.a.)	17	25%	6%
P.R. China	5,5	8,2%	10%
Japan	5	7,5%	5%
Germany	4,3	6,4%	5%
UK	3,7	5,5%	5%
Russia	3,1	4,6%	6%
France	3	4,5%	5%
South Korea	2,6	3,9%	5%
India	2	3,0%	15%
Italy	1,9	2,8%	8%
Canada	1,2	1,8%	9%
Israel	1,2	1,8%	7%
Australia	0,9	1,3%	8%
Rest of World	6,3	9,4%	9%
TOTAL	66,7	100%	8%

Piotr Wilam, co-founder, General Partner and Leading Investor at Innovation Nest (seed/VC fund), looked at investing in cybersecurity from a different angle. He perceived cybersecurity as a much broader domain including both cybersecurity companies sensu stricto and enterprises that deliver a different kind of value, but with a substantial embedded cybersecurity component, the so-called "security by design".

This puts a few other adequate remarks made by Mr. Gresko concerning the diverse funds available on the market in context. First of all, we should not antagonise the investors present on the market: generalists, cybersecurity focused players, and corporate actors. The entire ecosystem is strengthened when we can connect those players and start leveraging, as each of them can bring added value to the entrepreneurs. He highlighted that funding opportunities abound on the market, so any good company should be able to get it. However, it should be a demanding task, both for the company itself and the fund manager it would be engaging with. The companies should not take cheap money offered by a venture capital player who will provide no other added value than the funds only. He warned that companies should be very careful who they are partnering with and insisted they ensure the venture capital fund manager of their choice would add value to their business. On top of that, Luigi Rebuffi pointed out that even though there are a lot of funding opportunities available on the market and Europe has many

1 | European Cybersecurity Industry Proposal for a Contractual Public-Private-Partnership, June 2016, p. 21-22. [online] http://www.ecs-org.eu/documents/ecs-cppp-industry-proposal.pdf (access: 26.10.2016).

excellent and innovative ideas, startups, and highly qualified specialist, a fundamental challenge is to teach those people how to perform fundraising effectively.

Meanwhile, as Mr. O'Cinneide stated, we need to be aware that the four biggest investors in cybersecurity are the governments of the US, the UK, Russia, and China. They are by magnitude bigger than anyone else. By the same token, it is crucial for private companies to cooperate with governments, especially in the EU, and observe what technologies they are developing and how they can work with them to commercialise things and tap into human capital in the public sector. Mr. Seewald also confirmed the need for close cooperation between public and private entities on cybersecurity investments. A clear evidence of that is the history of clusters in the US (Silicon Valley), Israel, or Singapore. What we can see in the development of those clusters is an overwhelming financial support from their governments. In 1950s and 1960s, Silicon Valley was driven by the military industrial complex, while in Singapore and Israel by government investments in the technology sector. Recently, the UK government announced a direct investment programme into cyber worth £2 billion. Even though those trends did not sound good to Mr. Seewald as a venture capitalist, he stated that it should be acknowledged that the role of governments is to provide capital in safe environment.

So what is the perfect combination? According to Mr. Rebuffi, looking for symbiosis in public-private cooperation is crucial now. Defining the right way to go is a challenge and opportunity at the same time. Mr. Rebuffi expected the government to set the scene and establish the ecosystem by enacting legislation and implementing the EU regulations, or providing suitable education. Clearly, the government would not become a venture capitalist itself, but it is supposed to invest in several domains – especially in the protection of critical infrastructure.

On the other hand, from the client's perspective represented by Stanisław Fendryk, Director of the Informatics Office at PKP Cargo, what really matters is the price. However, the potential customer has to be aware of the fact that the marginalisation of cybersecurity will not bring savings to the company. Quite the contrary, the client will have to pay much more to mitigate the negative effects of a cyberattack once the company data has been compromised. Therefore, Mr. Fendryk advocated openness of the corporates and large companies towards innovative cybersecurity solutions offered by startups; however, he admitted that such products must be customised to meet individual needs of customers. Moreover, startups must be ready to enter into long-term cooperation with their clients instead of looking for one-off selling opportunities.

There are a lot of funding opportunities available on the market and Europe has many excellent and innovative ideas, startups, and highly qualified specialist, a fundamental challenge is to teach those people how to perform fundraising effectively.

Polish cybersecurity market – has it great potential for success?

The debate partially focused on the Polish cybersecurity market. First, it is really important to stress that there is no such thing as a unified approach and pattern countries can adopt to foster their development process in this domain. Mr. Seewald portrayed Poland as a state which has great potential for success. In the CEE region, Poland probably surpasses all its neighbours in size, the capital market, the drive for success, and the number of top-flight engineers. At the same time Mr. Gresko noted that just a few years ago, the VC market in Poland was inexistent and today it is still at a very early stage

of development. Furthermore, according to Mr. Gresko, the EIF has been operating as a VC fund-to-fund investor for almost seventeen years. During this time, the EIF has not received any high-quality proposal from Poland, but this is changing quickly. What is more, Poland is trying to position itself as a startup nation and increasingly often is being referred to as a startup hub.

No room for shortcuts and simple imitation

The cybersecurity market is a complex one: it is constantly changing and evolving, with no room for shortcuts. You cannot simply launch an R&D project, seek available funding, adopt already existing patterns, and expect to create a new Silicon Valley on a whim.

Poland has to find its own niche and build its power and reputation on something that is characteristic and unique to it. Therefore, the Polish government must engage in initiatives that promote local solutions and innovations.

Although the challenge is still out there, Poland has to find its own niche and build its power and reputation on something that is characteristic and unique to it. Therefore, the Polish government must engage in initiatives that promote local solutions and innovations. Mr. O'Cinneide suggested that Poland should define its competitive differentiation within Europe. The UK has an enormous ecosystem comprising top-tier universities, while in Germany there are multiple cities that are home to companies with established business credibility. Small niche nations such as the Republic of Ireland or Luxembourg offer legislation that provides for the development of privacy protection solutions. According to Mr. Wilam, Poland should make IT its own niche as it already has a thriving digital entrepreneurship ecosystem and strong IT assets. However, the selection of a cluster within the IT niche that merits further development may be a sensitive matter as cybersecurity is not the exclusive theme (e.g. there are also IoT companies). As believed by Mr. Wilam, there are close ties between these two sectors. The investors should observe and support them, invest in companies and help them to grow – and somehow support these networks, communities and their development. The government should play a similar role. Mr. Wilam stated that it was very difficult to choose a single investment thesis today that Poland should focus on. There should probably be multiple theses within IT that should be pursued in order to see if any one is successful.

The debate raised a lot of difficult questions and brought a lot of opinions and approaches which might be considered as the most compatible. The only obvious thing is that the challenge is huge and in order to turn it into a great opportunity it is necessary to harness not only funding, but also appropriate tools and highly specific knowledge as they are the cornerstones of a long-lasting, innovative and flourishing cybersecurity ecosystem. ■

This article has been written by Ziemowit Jóźwik and Magdalena Szwiec, Project Coordinators of the Kosciuszko Institute.

How much can the wrong IT management cost?

No room for shortcuts and simple imitation

The optimization of IT infrastructure management processes brings about a number of business benefits. The most prominent ones can significantly reduce both the ongoing and potential operating costs as well as increase an organization's overall cybersecurity level. How much can you benefit from implementing the right tools and policies in this area? And most importantly, how much can you lose because of wrong IT management?

Network failure worth millions

An IDC survey[1] showed that the average downtime resulting from failures in computer networks, systems, and applications in mid-size companies and organisations was 11 hours per year. Many of those failures were caused by cyberattacks. The costs of stoppage in the organisations participating in the survey amounted to USD 10,000 per hour. Gartner analysts suggested[2] larger companies could lose up to a staggering USD 300,000 per hour during IT infrastructure failures. The prolonged unavailability of IT systems can result in multi-million losses, as was the case with Delta Airlines[3] and Southwest Airlines Co, for example. For many smaller companies, not backed up with robust budget provisions, such downtime may even lead to bankruptcy. The British Chambers of Commerce reported that 93% of companies, which lost their data for more than 10 days because of an IT failure or leakage, disappeared from the market within a year after the incident.

How to minimize the risk?

Even the largest and best protected organisations must eventually face the cruel fact that there is no such thing as guaranteed protection against potential failures and latest hacking techniques. However, the foreseeable threats, such as equipment breakdown, system infections via USB sticks, phishing, etc. or even server room fires can be eliminated – at least to a certain extent. The previously mentioned IDC survey stated that the consistent use of IT management software could minimize costly computer network and system failures by as much as 65%. With tools to monitor the condition of the infrastructure, the network administrator has access to knowledge about e.g. service statuses, the condition of hard disks, and – with additional sensors – also the temperature and humidity in the server room.

1 | R. Boggs, J. Bozman, R. Perry, Business Operations Disruption Risk: Identify, Measure, Reduce, IDC White paper, December 2009, https://www.mercurymagazines.com/pdf/IDC_RiskAssessment_WP_Final.pdf.
2 | A. Lerner, The Cost of Downtime, July 2014, http://blogs.gartner.com/andrew-lerner/2014/07/16/the-cost-of-downtime.
3 | Benjamin Zhang, Delta is flying again after a massive computer outage shut down the airline, August 2016, http://www.businessinsider.com/r-delta-says-flights-grounded-nationwide-after-system-outage-2016-8?IR=T.

Wrong IT management **costs**

Every company loses **11 hours** on average each year due to downtime caused by IT system failures.
Source: IDC

One hour of downtime due to an IT system failure can cost as much as **USD 300K.**
Source: Gartner

93% of of companies that lost their data due to an IT system failure went into liquidation within a year from the incident.
Source: British Chambers of Commerce

80% of critical service **outages** are caused by unauthorized user activities.
Source: Gartner

A company based in eastern Poland had to pay **USD 1 million** in penalties for using illegal software.
Source: BSA The Software Alliance

Benefits yielded by IT management software implementation

The implementation of IT management software can minimize infrastructure failures by **65%**.
Source: IDC

By installing employee activity monitoring software, an IT company employing 5,000 people increased its annual profits by **USD 2 million.**
Source: Boston Globe

Following the deployment of staff activity monitoring software, the time employees spend performing job-related tasks has increased by **90 minutes** a day on average.
Source: Boston Globe

One of the major US federal agencies reported that in 2012 only made **USD 181 million** of savings by establishing a software licence inventory.
Source: Government Accountability Office

axence®

The weakest links in the security system

One of the sources of IT infrastructure failures is the proverbial sheer perversity of inanimate objects. Another is unauthorized acts of the employees. However, the costs generated by the former and the latter are potentially avoidable. One of Gartner's reports[4] reads that 80% of critical service stoppages result from unauthorized user activities. Employees are often responsible for strategic data leaks or the inadvertent introduction of viruses or spyware to the network. Sometimes education falls short, so the corporate security policy should provide for the preventive monitoring of potentially harmful employee-caused incidents. The IT department should be also equipped with the right tools to detect suspicious user activity.

Professional IT management software perfectly complements security systems and antiviral programs. At the same time, you need to remember that the purpose of the software is not to invigilate, but to increase corporate protection against data leaks and external attacks. The software solution for IT management, supported by the user activity monitoring module, is the right choice when you want to protect your business against high financial losses resulting from the unauthorized acts of the employees, emphasizes Marcin Matuszewski, Senior Technical Support Engineer at Axence.

The implementation of employee activity monitoring tools does not only strengthen the network protection chain, but also increases the employee productivity, which means that a potentially higher profit can be generated within a specific time span. For instance, an IT company employing 5,000 people increased its

4 | R. Colville, Top Seven Considerations For Configuration Management for Virtual and Cloud Infrastructures, Gartner RAS Core Research Note G00208328, October 2010, https://img2.insight.com/graphics/no/info2/insight_art6.pdf.

yearly profit by USD 2 million[5] after the deployment of employee monitoring software. As this fact had been communicated to the staff upfront, it turned out they spent 90 minutes more on average on their professional tasks. The very awareness of being monitored had the effect of self-control, making them less preoccupied with private affairs whilst at work – despite the fact that the administrator was not following their every step, but was only informed about suspicious activities.

The overarching purpose of monitoring tools is to effectively respond to incidents, not to track every keystroke. Another argument for the implementation of such solutions is the growing number of threats taking advantage of social manipulation, such as spear phishing. An employee might be unaware that by clicking on a link or downloading an attachment, he or she can contribute to a critical data leak or infection of the corporate network with a dangerous virus.

Costly licenses

Hardware and application failures or the risky behaviour of the users are not the only incidents which can be potentially damaging to a company's finances or image. The improper management of licenses for the utilized software also poses a high risk. Mass media often relate the cases of companies which have had to pay millions in penalties for using illegal software. An administrator equipped with the right software can quickly audit the applications used to see which ones do not have a valid license. The collected knowledge will help IT professionals to decide what licenses should be purchased and what software should be uninstalled.

An equally valuable element is the insight into the usage of specific licenses, which can be obtained with IT asset inventory software. It helps the administrator to decide which licenses are redundant, i.e. are paid for by the company, while the software remains unused. For instance, following an audit, the US Government Accountability Office has identified that the proper management of software licenses may produce huge savings in the public sector. One of the most prominent US federal agencies (its name was not disclosed) reported that in 2012 only, it saved USD 181 million[6] in that regard.

Smart management

Comprehensive network management allows the risk of costly stoppages and data leaks to be significantly reduced and penalties for the possession of illegal software to be avoided. This, in turn, means shorter downtimes and the increased productivity of expert employees, which reduces the fixed costs. Data collected by survey institutes and the case studies of companies and organisations from all over the world show that in order to maximise profits on the balance sheet, it is worth considering the deployment of suitable tools for monitoring the network and its users, as well as for hardware and software inventory management. There are several all-in-one solutions on the market which allow all of these issues to be addressed from the level of one console. What is more, they include mechanisms which automate some of the processes, enabling the person responsible for IT management to focus solely on the important alerts.

In our conversations, the administrators often emphasize that, for them, managing the infrastructure with one comprehensive tool is much easier and faster as they do not need to become accustomed to different systems, and keep switching between them. This is especially significant for large networks consisting of a few hundred workstations. It is another argument for the deployment of an all-in-one tool, which will enable the administrators to save time and focus on other, more important aspects of the job, adds Marcin Matuszewski from Axence. ■

5 | K. Johnston, Firms step up employee monitoring at work, February 2016, http://www.bostonglobe.com/business/2016/02/18/firms-step-monitoring-employee-activities-work/2l5hoCjsEZWA0bp10BzPrN/story.html.

6 | US GAO, Better Management Needed to Achieve Significant Savings Government-Wide, May 2014, http://www.gao.gov/products/D07403.

sharptec

Nowadays, technology helps us like never before in history. We utilize digital products and services to make our lives easier, more comfortable and much more productive. For many of these technological developments, we probably cannot imagine to live without them. It is very good until it is safe.

Unfortunately, most of the people do not pay enough attention to their digital security. To feel safe, we need to protect not only our passwords but also our devices, especially mobile ones, which carries all our sensitive data.

IT experts have been working on secure encryption algorithms and secure software architectures for many years, but it is known that each solution is as safe as its weakest element: the human component.

I think we still wait for an appropriate security mechanism to overcome known vulnerabilities. I also believe that one of the strongest successor will be a biometric-based security. So far, we know many physiological or behavioral human characteristics which can be used as authentication method like fingerprint, retina, palm, scent, voice or DNA. Not all of these biometric mechanisms are useable yet, but they will for sure be available in the future. Even right now RFI's card-based authentication could be easily replaced by a fingerprint scanning in places like offices or sport facilities.

It is essential that, using biometrics, security features are preserved while gaining end user comfort (we cannot forget our finger in the rush to work). Biometrics is the future of digital security. We need to remember it developing IT products and services.

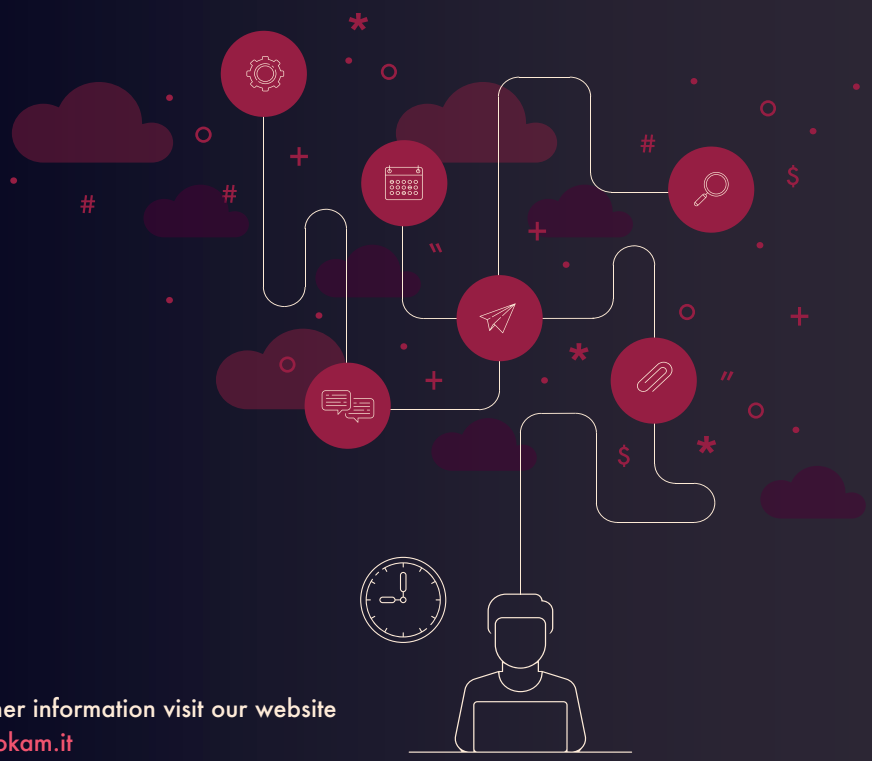
GYMMANAGER

Bloober Team SA is one of the leading game development companies in **Poland**. This year alone we released **3 products** on the market, **increasing** the company's **revenue** by the end of Q3 by **100%** in comparison to the analogical time frame from the previous year.

Bloober Team SA – don't fear to invest in horror. Follow us and see what is **Behind the Darkness**.

lookam

We are a team of professionals in IT sector.
We created lookam, to make our client's websites
SAVE, and it's functioning CONSTANT and STABLE.



For further information visit our website
www.lookam.it

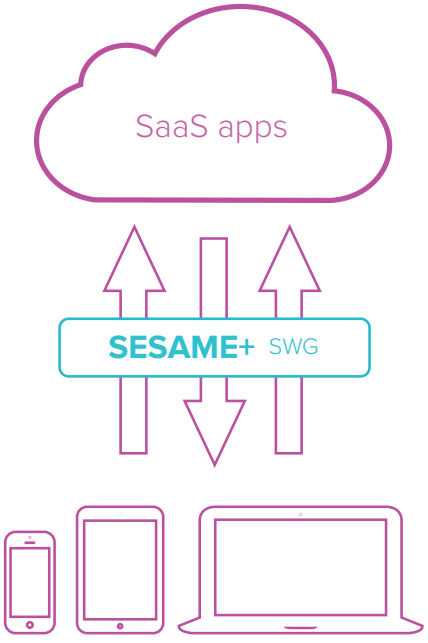
BASIC

- unlimited back-ups
- unlimited archive storage for your site on our server
- 3 hours set aside for testing new versions of plug-ins and installing Wordpress updates
- access to an online panel displaying information about all work carried out on your site
- customer service provided directly by a dedicated programmer
- a monthly report of work done and changes to your site

PREMIUM

- unlimited back-ups
- unlimited archive storage for your site on our server
- 3 hours set aside for testing new versions of plug-ins and installing Wordpress updates
- 2 hours set aside for other maintenance work on your site (such as content management, changes to graphics/CSS/HTML)
- access to an online panel displaying information about all work carried out on your site
- customer service provided directly by a dedicated programmer
- a monthly report of work done and changes to your site

Your sensitive data is already in unsanctioned cloud apps, protected by weak and repeated passwords. This will eventually lead to a disaster. We'll help you prevent it.



SESAME+ Secure Web Gateway helps you regain control over security of data scattered around different SaaS applications. SESAME+ SWG actively monitors cloud traffic, supervises user authentication, enables password policy enforcement and ultimately frees users from password usage in favour of a single, secure access point.

Password policy enforcement and Single Sign-on (SSO) for any cloud application on any device

SESAME+
Secure Web Gateway

http://sesame.id/swg

Are we really safe?

Ubiquity, usability, and ease of use – this is what we expect from various online services and mobile apps providers today.

Numerous spheres of our everyday life are increasingly being moved to cyberspace. It is almost a parallel reality in which half of the world's population[1] already lives their lives. Similarly, mobile technology development has made us more and more connected to the Web. With the surge in mobile apps use, it now stands for 86% of the time we spent online[2]. Fast access to all kinds of services is supposed to make our lives easier and save our time.

However, online services have always faced an eternal dilemma: the right balance between the security of end-users and the ease of use. Can Internet-based services be easy and secure at the same time? As we know, additional layers of security require extra authentication methods, external devices, more codes, and then even more passwords and so on. Therefore, the security level of our online activities is frequently lowered to a minimum level in order to deliver satisfactory user experience when navigating through online services and applications. This raises a legitimate question: are we safe in this "easily accessible" virtual world? And the answer is simply: NO.

In its 2016 cybercrime report, RSA noted that 45% of all online transactions in 2015 were made via mobile channels whereas 61% of attack attempts were made with the use of mobile devices. Additionally, the report mentioned a tremendous 173% increase in this kind of attack that was observed between 2013 and 2015.

1 | We are social, 2016 Report, 2016, http://wearesocial.com/uk/special-reports/digital-in-2016.

2 | Flurry Analytics, eMarketer USA, April 2014.

MAREK OSTAFIL

COO and Co-Founder of Cyberus Labs. He has 20 years of experience in managing international teams and projects. He has gained experience in Digital Sound Processing since '90 at the Eloctroacoustic Music Studio of the Music Academy in Kraków, Poland and was a manager and co-organizer of many international projects in Europe that combined sound and new technologies. He worked also as an Associate Producer for Discovery Channel and RAI. Guest lecturer at the Jagiellonian University (Cracow Poland) and guest speaker on management and fundraising. He has a Masters Degree in History of Art from the Jagiellonian University and a recipient of a scholarship from the International Center for Culture and Management (Salzburg, Austria).

CYBERUSLABS

For a long time, we have been focusing on the use of technology and the ease of access that it offers. Unfortunately, the security factor is still very much neglected by those who design systems and their end-users. Many users of online banking services put the ease of use above security. They seem to care more about fast access to the service than the security of their private data or money. There are many reasons for that, but one of the most obvious ones is that we do not see the direct threat until:

- access to our e-mail account holding valuable private or business information is taken over by cybercriminals;
- our identity and personal data are put up on sale on the DarkWeb;
- our identity is used for money laundering and other illegal transactions;
- our money from bank accounts, ATMs, or credit cards are stolen;
- our intellectual propriety and business confidential information are taken over by competition.

However, none of the above seems to concern most of us. We think that the probability of such an event to happen to us is low, or that the consequent costs are negligible. But we cannot be more wrong. It is highly possible and highly probable for these events to occur to us every day as the access to all the information and data is “protected” by the weakest possible system: the username and password. On top of that, online transactions are confirmed by other compromised systems: SMS and hardware token verification mechanisms.

"Wait a minute! But everybody uses that system. Why should we use anything else if our existing systems work fine and have been around for years?" Or even worse: “Why should we change our system that our users are used to?” Yes, everybody either uses or is accustomed to a popular yet broken, and highly vulnerable "protection" system.

Taking over usernames and passwords to gain access to user accounts and stealing their identity is very easy. Users behave recklessly, saving their passwords in browsers, or in spreadsheets that are saved on their hard drives. Both locations are among the prime targets for hacking attacks. Almost every day brings breaking news about another credential theft, hacking login elements. One of the biggest breaches so far has been the Yahoo’s account hack where 500 million user credentials were stolen.

Michael Chertoff, former secretary of the U.S. Homeland Security Department, has recently very precisely pointed out where the problem lies: “A closer examination of major breaches reveals a common theme: In every "major headline" breach, the attack vector has been the common password. The reason is simple: The password is by far the weakest link in cybersecurity today”[3]. So are all the systems and services that are "protected" by usernames and passwords.

Building complex data protection mechanisms, equipped with latest antiviruses, fire walls, hack detection and monitoring systems, password aggregators, or second factor authenticators, has little sense if this data is still accessible by relying on “the weakest link”. Password aggregators are much easier to use than passwords. But the problem is that they are still... password aggregators. It is quite likely that while you are reading this text, another 1,800 credentials have just been stolen, so the issue should be taken seriously.

This also concerns transaction authorisation systems based on SMS, tokens, or FOBs. The common denominator for all the above-mentioned mechanisms is a naive faith in their protective role and security. When the systems using SMS as a payment confirmation were designed, the present technology that allows this channel of communication to be hacked was not even taken into consideration. It was not meant to be secure. It was designed to be popular. In September 2016, NIST issued

3 | M. Chernoff, Passwords are the weakest link in cybersecurity today, CNBC, October 2016, http://www.cnbc.com/2016/10/06/passwords-are-the-weakest-link-in-cybersecurity-today-michael-chertoff-commentary.html.

a negative recommendation for SMS as an authentication method. SMS has been officially deemed "compromised".

On the other hand, we have recently witnessed a boom in the popularity of a new cybersecurity solution that has been widely hailed as a virtually universal cure for the "password problem" – biometrics.

It is important to acknowledge the enormous effort put into the development of this technology in service of cybersecurity, unfortunately many of the proposed solutions seem to be rather marketing gadgets. It is another fast and easy fix that is supposed to replace usernames and passwords: a fancy selfie, fingerprint, or iris scan that, again, creates an illusory sense of protection. But it will not guarantee full user safety. While the accuracy of the systems is one problem, the storage of biometric credentials is another. And there are other issues as well. Certainly, biometrics is safer than traditional technologies that use usernames and passwords but.... only until they are taken over by cybercriminals.

When this happens, the user loses the chance to use their biometric credentials – forever. Together with 5.6 million US federal employees whose credentials (including biometric information) have been stolen by cybercriminals[4]. The incident has had an immediate life-threatening impact on many secret agents who can now be easily identified by using their biometric information, even after they have been given new identities, including first names and surnames. While stolen usernames and passwords can be changed, fingerprints or eyeballs – cannot.

This may happen to any of us and, therefore, we need to focus and look for a real and highly secure protection of our credentials, data, money, and intellectual property.

Fortunately, there is a solution to all those problems. Our Krakow-based company Cyberus Labs has recently rolled out a highly innovative and passwordless login system called CYBERUS KEY. The system delivers something that until now was impossible to combine: ease of use and high-level security. CYBERUS KEY is a login and authentication platform that may be used for many different online services including e-commerce, fintech, banking and financial services, online media platforms, or e-healthcare. The core of the CYBERUS KEY solution is a one-time password based on the system of One-Time Pad called also a Vernam Cypher, proven by Calude Schannon from MIT to be unbreakable. Additionally, CYBERUS KEY uses out-of-band communication to prevent "man in the middle" attacks and the interception of transaction confirmation details.

The system is both fast AND secure. It also does eliminate the need for usernames, passwords, SMS, tokens, FOBs, etc. Among other unique features of CYBERUS KEY is guaranteed credential protection. This solution ensures that user login details will never be intercepted by cybercriminals as our system does not transmit any actionable user credentials during the login process. Another one is that our system identifies both sides of the online transaction – an authorised user AND a legitimate website or online service. This allows CYBERUS KEY to eliminate cyber threats such as phishing and "man in the middle" attacks.

CYBERUS KEY is a cutting-edge solution that makes users free from remembering passwords. It is the future of both easy and secure login and online transaction confirmation systems. ■

4 | Sanger, David E. (2015-09-23). http://www.nytimes.com/2015/09/24/world/asia/hackers-took-fingerprints-of-5-6-million-us-workers-government-says.html. The New York Times.

KRAKOW

THE PLACE WHERE CYBER MEETS SECURITY

CYBERSEC HUB

In CYBERSEC HUB we believe that connecting means creating and that every network is more than the sum of its parts. That is why we launched our platform which brings together people from across boundaries. From the private to public sector, from the technical to political spectrum, we connect all those who want to forge a secure cyber future.

CYBERSEC HUB builds on the synergy between stakeholders from the Małopolska Region in Poland, with the city of Krakow as its strategic center. Krakow is one of the largest startup hubs in Europe with over two hundred ICT businesses, unparalleled investment opportunities, and access to talent, funding and the entire EU market. This unique environment is what attracts global IT companies to the area, many of whom have already moved their Research, Development and Security Operations Centres to Małopolska. Krakow also hosts the European Cybersecurity Forum – CYBERSEC, one of the main public policy conferences on cybersecurity.

We are open to those who want to build the CYBERSEC community with us. Whether you are in academia, a CEO, an investor or the owner of a startup, you are invited to become an important part of our network. If you are interested in the project visit our website www.cybsersechub.eu or contact us at cybersechub@ik.org.pl.

THE KOSCIUSZKO INSTITUTE

The Kosciuszko Institute is a Polish think-tank founded in 2000. As an independent and non-profit organization, it gives itself the mission to contribute to the social and economic development of Poland in the European Union and as a partner of the Euro-Atlantic Alliance.

The experts of the Institute regularly cooperate with national and international organizations in the process of policy-making and initiating public debate on strategic issues.

Among its various areas of research, the Kosciuszko Institute leads its flagship projects in the field of cybersecurity, among them CYBERSEC HUB and the European Cybersecurity Forum – CYBERSEC.

We invite you to follow our initiatives and get involved.

Kraków, Poland.

www.ik.org.pl

THE KOSCIUSZKO INSTITUTE

is the publisher of

EUROPEAN CYBERSECURITY MARKET