VOL 1 (2017) ISSUE 2

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.

ISSN: 2543-7259

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

Disclaimer: The views expressed in articles are the authors' and not necessarily those of the Kosciuszko Institute. Authors may have consulting or other business relationships with the companies they discuss.

FOREWORD

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

Cybersecurity is one of the fastest growing sectors of the ICT market. According to various reports, worldwide spending on cybersecurity products and services in 2017 reached more than $120 billion. In the last decade, the market was growing 8-10 percent annually, while predictions for 2017–2020 envisage its further steady growth, estimating cumulative cybersecurity spending at $1 trillion in this period.

The particularity of this market rests in the fact that the aforementioned growth is driven not only by technological breakthroughs or process optimization, but also by the threats that are raising exponentially in the cyber domain. It is hard to estimate total losses from cybercrime for the public and private entities worldwide, but it is believed to be one to three percent of the global GDP. This clearly shows that our economy relies heavily on secure ICT infrastructure, with cybersecurity by design underpinning the materialization of the 4th industrial revolution.

To make it happen, we need to efficiently connect the different parts of the entrepreneurial ecosystem in Europe in order to keep abreast with the fast-evolving world market. Innovative startups, corporates, SMEs, Venture Capital, R&D centres, academia as well as European and national authorities – all these players need to be incentivized to cooperate in order to create a competitive, Europe-wide cybersecurity market.

For this purpose, the latest edition of ECM provides an overview of different perspectives on ICT security and innovation. It gives a voice to academics who talk about different models of research commercialization, and provides an SME's perspective on the most threating business habits in cyberspace. It also features articles by startups and experts on the strategic and technological layers of innovation.

I hope you will find this edition of ECM both interesting and stimulating. Stay cyber, stay secure!

Robert Siudak

CONTENTS

Implementing innovation in the cybersecurity sector:

Strategy planning methods for start-ups

How to prepare for an effective commercialisation and mitigate the investment risk

IZABELA PALUCH
is the President of the Management Board of INTECH PK, a project company of the Cracow University of Technology. She has many years' experience of the market, business projects and investment project management. In 1995-2011, she worked in managerial positions for large international production and trade companies, and was responsible for development planning, financial performance, sales, new implementations, and key account relations. INTECH PK focuses on the commercialisation of innovative technologies, establishment and development of spin-offs with authors of technologies, investment partners and/or industry partners. The Company's operations also involve the licensing or sale of research and development work results by the university to industrial partners.

Among inherent features of innovative technology commercialisation is no access to clear-cut market viability metrics and high failure risk. **Start-ups specifically are entities that operate under conditions of extreme uncertainty and are exposed to the highest risk of failure.** Start-ups are new market undertakings initiated by one or multiple founders, but may also be initiatives launched by multinational corporations. Start-ups vary in terms of legal form, ranging from single-trader companies, through to limited-liability companies and stock exchange-listed companies, and in terms of size – from micro-businesses to large organisations.

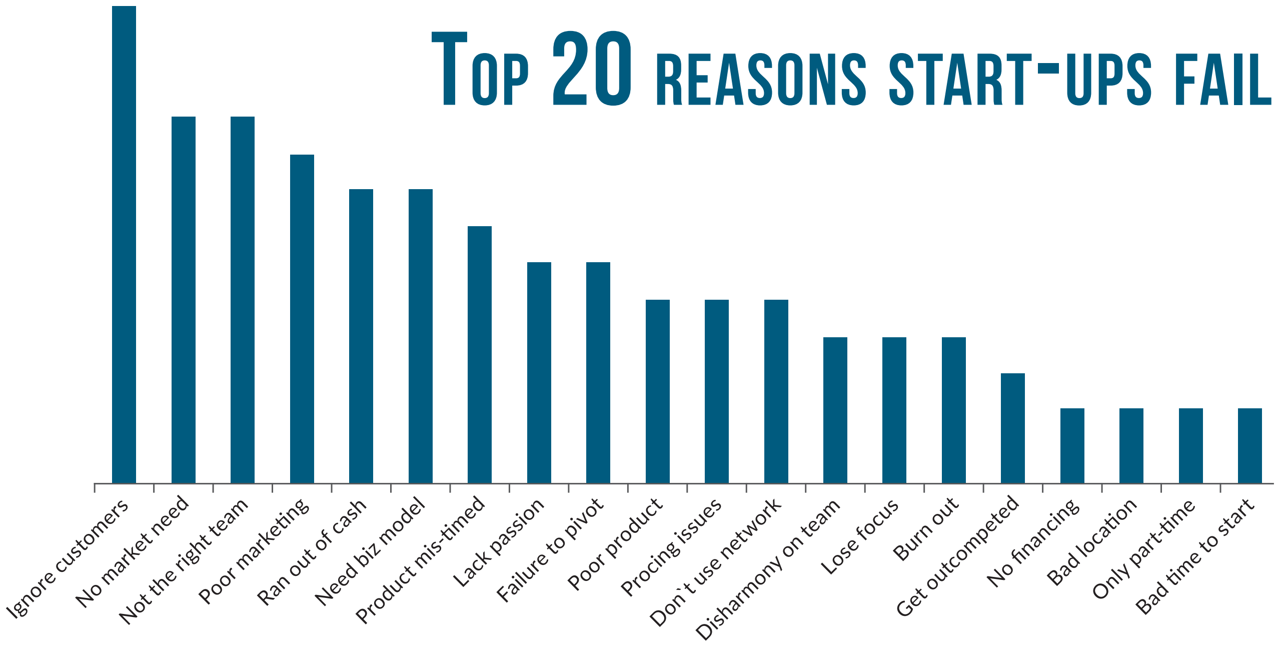
A common feature of start-ups is high investment risk and high likelihood of their failure. The risk inherent in their initial term primarily results from their operating basis – a hypothetical concept of a product that hypothetically fulfils the needs or solves the problems of a hypothetical customer group. Considering that a withdrawal from the market without earning back the expenditures of the investment is considered a failure, it is estimated that from 8 to 9 start-ups fail in the initial two years of their operation[1].

[1] | Dlaczego start-upy upadają (Why do start-ups fail?), www.web.gov.pl/wiedza/prowadzenie-e-biznesu/622_1439.html 14.02.2017
N. Patel, 90% of startups fail: Where Is What You Need To Know About The 10%, www.forbes.com/sites/neilpatel/2015/01/16/90-of-startups-will-fail-heres-what-you-need-to-know-about-the-10/#5813b3e255e1 14.02.2017.

Key tasks of start-ups include securing for themselves resources such as skills, expertise, know-how and funds in order to come up with scalable, repetitive and profitable products on the basis of watershed technologies. Typically, the initial task of a start-up is to create and launch the MVP (Minimum Viable Product), which is not a prototype undergoing tests, but a product that meets the needs defined as a must-have, for which the customer is willing to pay. Then the focus should be to expand knowledge on the MVP, conduct preference and customer behaviour research on the target market, and approve the planned business concept as a profit-generating and efficient project. Start-ups are often temporary and undergo structural, organisational and business model changes having achieved the anticipated objective. **If start-ups manage to secure resources such as highly-motivated teams, unique and innovative know-how, and to obtain funds to conduct their operations, why is it that they fail?** Key mistakes made by start-ups factoring in their failures include:

- no demand for the product: offering a product that does not meet customer needs, absence of flexibility with respect to planning product changes;
- ignoring the significance of early adopters and the need to identify target customer segments;
- no quick "monetisation" of the concept (the concept must become a sellable product/service);
- no funds for further growth;
- focus on the product alone, without considering the importance of other activities, in particular translating into marketing, sales, promotion neglect;
- operating growth too slow, resulting in the loss of competitiveness and leading position in a given market segment;
- insufficient qualifications of team members or conflicts within the team;
- running a number of project-concurrently[3].

Figure 1. The 20 top reasons that the startups fail[2]

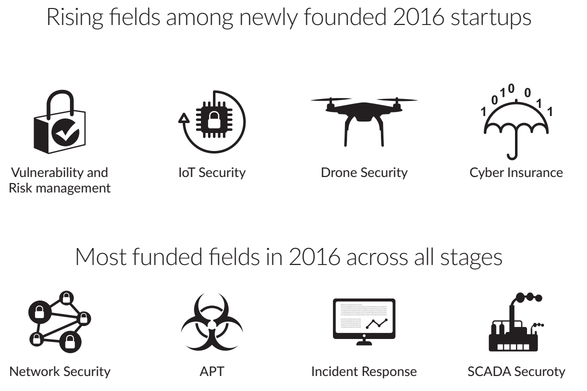


[2] Ibidem.

[3] Analyzing 32 Startup Failure Post-Mortems to Find the 20 Top Reasons that Startups Fail, Jan 11, 2011 www.chubbybrain.com/blog/top-reasons-startups-fail-analyzing-startup-failure-post-mortem/ 14.02.2017.

On the other hand, however, small things can turn into large things, and a rapid growth of start-ups is what markets want, and entrepreneurs and investors need. IT start-ups and cybersecurity (cybersec) companies more specifically perfectly fit in those needs. It is one of the "hottest" sectors for investors (venture capital) because, although the sector has been experiencing a slowdown in investment, it still generates a significant return on capital. As reported by TechCrunch, investors on the Israeli market contributed USD 520 mio. to cybersecurity companies in 2015[4], and investment on leading markets for cybersec technology development, that is the US and Israeli, continued to grow in 2016. In terms of the types of cybersec solutions attracting investors in 2016, the top ones were mobile security, network security, risk management, SCADA safety, Internet of Things, drone security and cyber-insurance solutions. This is connected to the growing demand among business customers for effective solutions which may help meet stringent national regulations on data protection and privacy, as well as combat cyberthreats[5].

Figure 2. Hottest cybersec sectors in 2016 according to TechCrunch[6]. Own compilation based on TechCrunch data.


Rising fields among newly founded 2016 startups
Vulnerability and Risk management
IoT Security
Drone Security
0 1 0 0 1 1 1
Cyber Insurance
Most funded fields in 2016 across all stages
Network Security
APT
Incident Response
SCADA Securoty

In the age of globalised innovative products and services, considering relatively unconstrained access to resources required to commercialise innovation and to the global supply market, what builds competitive advantage in the cybersec sector is the ability to quickly and clearly define key elements of the planned project and select the appropriate business model. This aspect is very important for start-ups, which are in the process of market adaptation. Under conditions of time pressure and facing ever-shorter life cycles of new market solutions, product improvement and search for features that set our product apart from competing product of other entities, and due to high cost of market entry, informed preparation to the market launch helps to mitigate the investment risk. To achieve success, we need to go beyond the comfort zone, that is the conviction that we have a great idea, and test the market, get to know potential customers, assess competitors, define primary revenue streams and the cost structure.

How to effectively and actively manage a project? A business plan will address that need. In late 20th century the business plan grew to be a standard tool used by business from any sector across the world. The development and application of the business plan as a tool correlates with the growth of the high-tech industry in the Silicon Valley, and with the operations of investment institutions (venture capital, banks). Business plans were related to the emergence of high-tech start-ups and high-risk projects[7].

The business plan as a management-support tool has become part and parcel of business operations. The business plan is a plan for an investment project intended to generate profits. It is a detailed plan of project actions, prepared on the basis of market research and historical data, covering the period from three to five years, providing a concrete strategy, projection of business objectives and a description of ways to achieve them, considering all existing constraints and ways to control the execution of the respective tasks.

[4] | S. Hod Moyal, A Global Perspective Of Israeli Tech In 201,] Crunch Network, Jan 16, 2016 https://techcrunch.com/2016/01/16/a-global-perspective-of-israeli-tech-in-2015/ 14.02.2017.

[5] | Y. Leitersdorf, O. Schreiber, I. Reznikov, Trends in Israel's cybersecurity investments, Crunch Network, Jan 23, 2017 https://techcrunch.com/2017/01/23/trends-in-israels-cybersecurity-investments/ 14.02.2017.

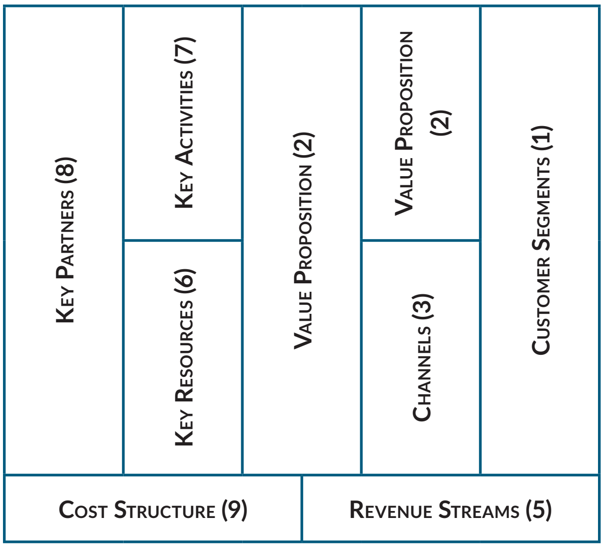
[6] | Ibidem.

[7] | T. Berry, Where can I find a short history of the evolution of business plans for start-ups?, Quora, Jan 9, 2011 https://www.quora.com/Where-can-I-find-a-short-history-of-the-evolution-of-business-plans-for-start-ups 14.02.2017.

The business plan is a good solution when we have access to forecasts or assumptions before embarking on the project, based on analytical data collected during independent market observation, and retrieved from the available databases (e.g. characteristics of a similar or substitute product, customer preferences, market potential observations, price and cost comparison, competitors' offering). By assumption, the business plan has a project structure: after the planning stage, where resources and completion times for the project (milestones) are identified, comes implementation time. Typical of the business plan drafting stage is the forecasting of the implementation profitability in the long-run, which generates two risks. First, there is the need to incur capital expenditures, and second, the uncertain project implementation metric (the measure of success is the achievement of the expected outcome – if not achieved, it is difficult to decide what to do next with the project). These risks are mitigated through assessing each of the implementation stages (milestones), with evaluation of objectives, resources and outcomes. However, if the assumptions refer to project outcomes after 5 years, then minor changes are often introduced along the way. Major changes, in turn with a significant correction to the business plan, involve the cost of repeated analysis of a number of documents, preparation of elaborate studies justifying the strategic change, and convincing investors to trust as again (or actually trust the new profitability factors).

Does the drafting of plans for new projects and business development strategy planning require an elaborate business plan? What if we don't have historical data available? There are simpler, more flexible and less formal methods for business project planning. For example, Alexander Osterwalder's Business Model Canvas is a tool that can creatively, quickly and efficiently revise our knowledge and approach to projects. **"A business model describes the rationale of how an organization creates, delivers, and captures value"[8].** This methodology assumes that the data is collected in action and that a new business plan can be created or an existing one improved in a relatively short period of time.

Figure 3. Business Model Canvas Template / Original template: A. Osterwalder, Strategyzer.com[9]



The Business Model Canvas is a type of a reality snapshot viewed as a single page (canvas) divided into 9 sections, that correspond to the primary business operation areas (customer, offer, infrastructure and finance):

1. Customer Segments

The first area of this business model approach is a place where we define the various specific customer groups (people, institutions, customer segments), which will become recipients of our solutions, and to which we want to extend our value proposition. Recipients – customers help us grow the product/service and obtain revenue streams.

2. Value Proposition

It is a set of values that are key to a given customer segment. In most general terms, it is the offering targeted

[8] A. Osterwalder, Y. Pigneur, Business Model Generation, Published by J. Wiley & Sons, Inc., Hoboken, New Jersey, 2010, p. 14.

[9] https://strategyzer.com/canvas/business-model-canvas 14.02.2017.

at the recipient. We need to define the MVP and reasons why customers will prefer our product and services to other solutions available on the market, and consider whether our disruptive offer aggregates benefits for the customers and solves their existing problems. We describe what the customer will be willing to pay.

3. Channels

Here, we determine ways to deliver our value proposition to each customer segment. These are methods for communication, distribution and sale, including customer acquisition methods, places where we communicate with the customer (where the customers explore our offer, meet our brand and make the purchase), delivery methods and aftersales customer support. We analyse here whether we are in tune with customer routines.

4. Customer relationships

We specify here what type of relations with customers we wish to build. Is our value proposition submitted as personalised offering, or is it rather automatic support of a given customer segment, and how does that relate to customer expectations? What relations will impact customer acquisition and retention rates, and what will boost sales.

5. Revenue streams

Each business project is meant to generate profits. In this field of the canvas, we present all ways to generate profits. We specify how we will generate revenue from each customer segment, for what and how the customers will pay, what is the price mechanism, which items of our offering are free of charge, and how they connect to the items of paid offering.

6. Key resources

Each business model requires access to specific property, intellectual and financial resources, to ensure preparation of an appropriate value proposition, access to customers and relations with them, and the generation of profits. For some organisations, the key resource will be the team, while it will be knowledge and intellectual property, or production base, for others. Key resources depend on the characteristics of our business and may be held as owned property, or can be purchased, or leased.

7. Key activities

In this field, we define the actions we take to create and deliver the value proposition to our customers, establish relations and generate profit. Key activities, similarly to key revenue streams, depend on the features of our business.

8. Key partnerships

In order to optimise our business model, we define partners, suppliers or subcontractors required for our business to operate, plan further outsourcing or infrastructure hire needs, and identify key partners we wish to establish strategic alliances with, e.g. to obtain access to a given customer segment or reduce the cost of key resources. An important aspect here is to realise to what extent we are dependent on key partners, and whether we can substitute them if necessary.

9. Cost structure

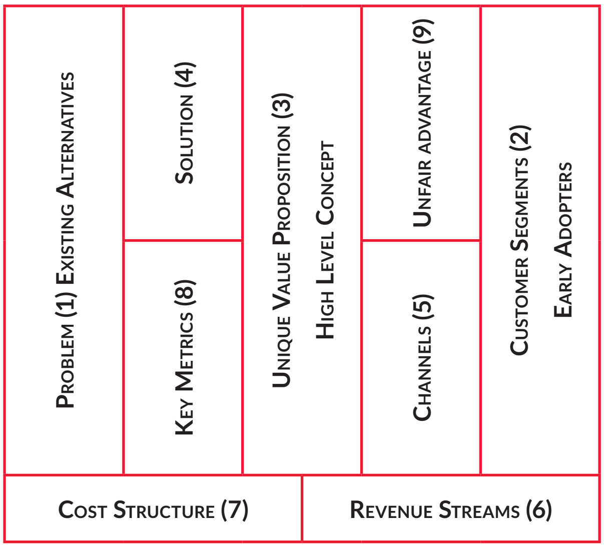
Here we describe the costs incurred to operate our business model. These are calculated on the basis of the previously defined key resources, activities and partners, and channels to access customers and build relations with them. Although cost needs to be minimised in each business approach, it will be useful for our business model to choose whether we minimise the cost wherever possible (cost-driven model), or focus on value creation (value-driven model)[10].

The Business Model Canvas is a convenient tool for start-ups that need improvements or change, i.e. in the area of logistics, cooperation with partners, or wish to redefine their value proposition for customers. A lean canvas model by Ash Maurya was in turn developed for start-up companies which need a structured approach to product development management (including product definition in terms of how it fits in the needs and problems of customers), and in particular for those start-ups that plan market implementation of innovation and which, by definition, operate under conditions of

[10] | A. Osterwalder, Y. Pigneur, Op.cit. p. 20-41.

extreme uncertainty. „Lean Canvas is a business model hypotheses testing and validation tool. It's a companion tool […] that simplifies how you document business models, measure progress, and communicate learning with your internal and external stakeholders" .

Figure 4. Lean Canvas Template / Original template from: A. Maurya, Leanstack.com[11].



> **Lean Canvas is a business model hypotheses testing and validation tool. It's a companion tool […] that simplifies how you document business models, measure progress, and communicate learning with your internal and external stakeholders[12].**
>
> **Ash Maurya, "Running Lean"**

Lean Canvas is a structured approach to product management. The method is user-focused, and assesses such aspects as the search for the appropriate customer needs and problems, as well as defines how our concept solves those problems. Lean Canvas is not so much about the structuring of the business process itself, but rather about the structuring of product development and the product development path. The Lean Canvas, similarly to the Business Model Canvas, has 9 fields, but there are some new elements here:

1. Problem

Here we define what problems of our customers we want to solve with our products or services, and identify key needs of a given customer segment. The existing alternatives need to be looked at, and how customers today solve the defined problems.

2. Customer Segments

In Lean Canvas, this aspect is analysed in combination with the defined Problems. Who is the target of the offer. It is also worthwhile assessing who will be the early adopters.

3. Unique Value Proposition

"Unique Value Proposition: A single, clear compelling message that states why you are different and worth buying[13]." One of the key elements of the developed model. What will set our product apart from competitors, what genuine benefits are there for the customer and why they should believe our UVP?

4. Solution

Here we answer the question how we solve customer problems, describe key properties of the product which are sufficient to prepare the MVP and provide customers with a product offering that offers basic functions they require.

5. Channels

A strategic element in the development of the business concept is how we reach customers and build relations with them, and what actions are the most effective in this respect. It is also important to consider the marketing context for the new project.

[11] | A. Maurya, Running Lean, p. 12, https://danielpandza.files.wordpress.com/2013/01/running-lean.pdf 14.02.2017.

[12] | https://leanstack.com/lean-canvas/ 14.02.2017.

[13] | S. Blank, The Four Steps to the Epiphany [w] A. Maurya, Op.cit, p. 46.

6. Revenue streams

How, on what and how much we can earn. When is the product monetized (revenue). What is the product price. Do we use the "Free Trial" plan. "Your free users are not your customers (yet)[14]", so if the main package of services is available for free, who pays for what other services. How many paying customers do we need to break even.

7. Cost structure

Since the objective of every start-up is not only to launch the MVP on the market, but first of all to establish a scalable business model, we therefore need to consider monthly/annual cost of all operations involved with these two challenges.

8. Key metrics

This is about metrics that the start-up will observe and measure in order to check whether the assumed objectives are achieved, how the business project grows in real time, e.g. how many customers are there in the database, how many tested our solution, how many returned to buy a product or service, how many pay, how many complained...

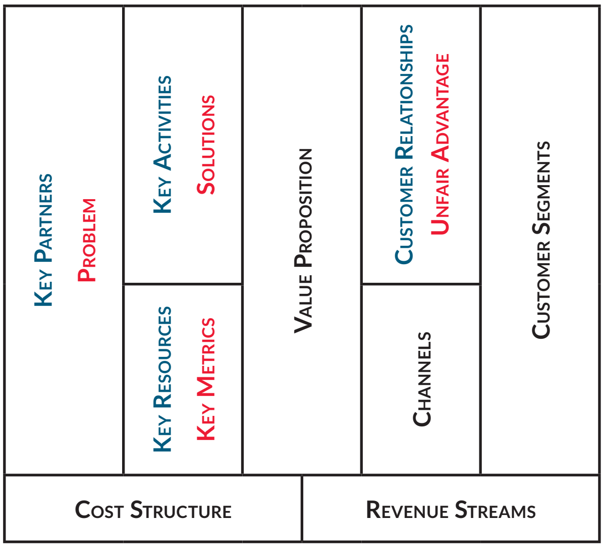
9. Unfair advantage

"A real unfair advantage is something that cannot be easily copied or bought[15]." The condition that is most difficult to meet, but which is also fundamental for start-ups. It is about a genuine advantage that will be difficult to copy by a potential competitor, e.g. a patent, confidential know-how of the inventor, or relational capital with a certain community[16].

PK

INTECH PK

Figure 5. Business Model Canvas Template vs. Lean Canvas Template



Lean Canvas helps to fine tune initial assumptions and key elements of the planned project, is relatively simple and easy to use, and enables start-ups to structure their vision and find gaps and omissions in the original concept.

Summary

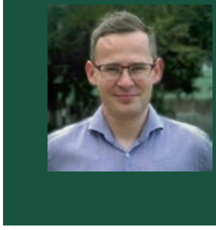
The implementation of new products and services in the cybersecurity sector is an enormous challenge, because this particular sector calls for continuous innovation and latest technology achievements, and its investors look for the most competitive solutions and start-ups that develop in their sector most quickly. A sustainable business model is instrumental in becoming successful, as it enables identification of ways to effectively commercialise a technology and mitigate investment risk, as well as to launch the market process required or strategy planning for investors and businesses alike, the Business Plan, the Business Model Canvas and the Lean Canvas are tools that can be used by start-ups to examine new concepts and proceed with their projects, analyse trends and metrics, and strategically plan their operations. Importantly, the strategy planning-support tools for start-ups can be applied both to entire companies, or their departments, or to selected products/services. ■

[14] A. Maurya, Op.cit, p. 64.

[15] J. Cohen, A Smart Bear [in] A. Maurya, Op.cit, p. 72.

[16] A. Maurya, Op.cit, p. 37-76.

REGTECH AND CYBERSEC: HOW REGULATION SPARKS DEMAND FOR CYBERSECURITY



MARTIN SEBENA
has over 7 years of working experience in the FinTech industry. His expertise is in setting up operations centres and growing business in the APAC region. He has worked in Hong Kong, Melbourne, Hangzhou, and Prague. He holds a Master's degree in finance from the Curtin University and currently pursues PhD research at The University of Hong Kong.

From a Simple Platform

One of the thorniest issues in the financial industry is the onboarding of new customers. The speed of acquiring new customers is a critical deliverable for measuring the growth of companies large and small, and this is not limited to the financial industry. What makes it different in the financial industry, however, are the compliance and regulatory requirements that demand every new customer to be thoroughly examined. Moreover, the regulatory environment is complex, fragmented and ever-evolving, requiring all companies to dedicate a large pool of resources to studying, implementing, and executing compliant processes.

It was about three years ago when the organization I worked for, an established FinTech company, decided to tackle this issue. To expedite the Know Your Customer (KYC) process, the company built a platform that allowed for an easy and secure submission of documents on the customer's side, and an instant access to these data on the bank's side. While the platform offered flexibility, scalability and a neat design, it was still very straightforward and only supported one service. The company even offered it free of charge! I was therefore surprised when more and more banking partners started heaping praise on this product.

The surprise did not last for long. A majority of financial institutions are still reliant on paper-based compliance methods which are arduous, inefficient and time-consuming. Introducing a secure, cloud-based tool for collecting, processing, and approving KYC documents must have been perceived as a revolutionary change. And the results of this revolution were staggering: onboarding time was reduced by two-thirds, which resulted in enhanced efficiency, significant cost savings, and higher customer satisfaction.

Regulatory Revolution

IT solutions that facilitate back office processes are the first examples of how regulatory technology, or RegTech, ventures into the financial services industry and transforms it. The above example shows that even the simplest solutions can have a huge impact. To understand the potential and scope of this transformation, let us first examine the factors behind the creation and growth of the RegTech industry.

Regulatory technology is a concept that has existed for almost half a century now. Early 1970s saw the introduction of this technology into payment processing and payment systems, such as Swift or RTGS, which were the first harbingers of RegTech. Further technological advances allowed for continuous development in this area; systems deployed to monitor and detect insider trading at that time can serve as an example.

While the characteristic feature of RegTech in its first four decades was incremental change, the Global Financial Crisis (GFC) of 2008 dramatically changed the landscape. The GFC sparked a fervent regulatory activity around the globe, which resulted in a steep increase in regulatory and compliance measures in the financial industry.

The imminent result of the post-crisis regulation was the skyrocketing of compliance costs for market participants. Surveys show that financial institutions typically spend about 20 percent of their budgets on compliance activities, thus the industry-wide spending totals tens of billions of dollars annually (we should also include regulatory fines, which have exceeded $200 billion since 2008). To make things worse, the lack of global standards results in diverse regulatory practices and requirements across jurisdictions, increasing costs for companies with international operations.

At the same time, advances in information technology (IT) and data science, particularly in artificial intelligence and deep learning, facilitated the development of tools that enable digitization and automation of reporting and compliance processes. The post-crisis emergence of RegTech lies at the juncture between the desire to lower the compliance costs and technological advancement. Recently, a third factor that spurs the demand for RegTech has emerged – namely, the desire of regulators themselves to use advanced technology in order to carry out their supervisory duties.

Departure From FinTech

Since its inception, RegTech has been closely linked to the financial industry, due to its openness towards the use of technology and the increasing levels of regulatory activity in finance. The year 2008 was crucial for the development of these industries as both use advanced technology to tackle challenges, and both have disruptive potential. Since FinTech saw a much faster growth and a higher number of participants, many find the RegTech industry to be a subset of FinTech. This view has been recently adopted by the UK's Financial Conduct Authority in their Call for Input on Supporting the Development and Adopters of RegTech.

The development of FinTech and RegTech followed different paths. FinTech has grown as a bottom-up movement, spearheaded by a zillion of start-ups. RegTech, on the other hand, follows a top-down path, since it is predominantly demanded by large financial institutions seeking to reduce costs and government regulators looking for more advanced supervisory tools.

What is more important, however, are their future prospects. While FinTech will, by definition, remain limited to the financial industry, RegTech can be applied in a number of sectors, such as healthcare, logistics and transportation, environment, and jurisprudence. Therefore, RegTech has the potential to outgrow FinTech in size and scope.

Demand for Cybersecurity

In the first decade after the GFC, the most characteristic feature of RegTech was the implementation of rather simple technological solutions, predominantly for KYC and Anti-Money Laundering (AML) purposes. The platform described in the first part of this article is one such RegTech solution.

Following the exponential rise of AI and machine learning, the efficiency, complexity, and scope of RegTech products grew rapidly. IBM's recent efforts in this area demonstrate the qualitative shift in the products. IBM has purchased the Promontory Financial Group, specializing in compliance consulting, asking their employees to teach risk management and compliance to Watson, its massive artificial intelligence engine. Watson now conducts much faster and much more accurate checks of customer data than any human could ever do. In a similar fashion, NASDAQ has partnered with a cognitive computing firm to provide surveillance technology to their customers.

This transformation of the financial industry, however, brought a related vulnerability to the forefront: the threat of cybercriminal activity. The shift of focus on big data processing, the availability of huge amounts of digital information and overall digitization of the industry attract the attention of hackers and other cybercriminals. All companies are equally vulnerable to a cyberattack: it does not matter if they are large financial institutions or FinTech and RegTech start-ups. As Sarah Dahlgren from the Federal Reserve Bank of New York has put it, the banks "are all linked to each other, to non-financial firms, and to every system that supports the operations and structure of the industry.[1]" In short, it is the interconnectedness in the financial industry that makes every firm a potential target for cybercriminals.

Large financial institutions often use antiquated technology. There is a strong need to fix longstanding technology and data issues that have built up over the years. Deloitte estimated in 2014 that out of 55 billion euro banks in Europe spent on information technology, only a remarkably low figure of 9 billion euro was spent on new systems. The balance was used to add more systems to the antiquated existing technologies and simply to keep the old technology going.

Smaller, predominantly FinTech companies, face a different type of problems: they operate in a data intensive environment and often have a limited comprehension of security, let alone low perceived need for it. Furthermore, even those that do realize the importance of cybersecurity often find that their scarce financial resources do not allow them to build and implement robust solutions.

Promoting Cybersecurity

As the GFC of 2008 emphasized the high interconnectedness of the financial industry (the 'too big to fail' concept), regulators since then have been well aware of the risk posed by systemic failures. While their focus is on highlighting the 'single points of failure' – the areas that are significantly more vulnerable than others – the final goal is to enhance cybersecurity across the whole financial sector.

One of the most efficient ways of promoting cybersecurity is in the area of risk management. A prudent risk management is able to price the cyber risk to the business. It should ask what the cyber exposure of the company is and find a way to put a figure on it, just as the Value at Risk concept estimates the possible losses of an investment. Once the cyber risk exposure is priced, it can get the attention it needs.

When the regulatory views on cybersecurity are adopted across the whole financial industry, resources will pour towards RegTech and CyberTech firms. This will allow these companies to advance their solutions, further enhancing security within the industry. As mentioned above, other industries where big data and sensitive information is stored, such as healthcare, environment or logistics, will be the next beneficiaries of this progress. Cybersecurity is a clear example of how FinTech demands RegTech. ■

[1] | Sarah Dalgren, Executive Vice President of the Federal Reserve Bank of New York. Speech at the OpRisk North America Annual Conference, New York City: The Importance of Addressing Cybersecurity Risks in the Financial Sector (March 24, 2015)

MY OBVIOUSLY BULLETPROOF SAAS

By Mateusz Olejarka @molejarka

Do you enjoy the feeling that your company is the best, and your products – bulletproof?

This self-confidence, not uncommon among software companies is, in most cases, a positive thing. You can see the exact same confidence when it comes to security: "Of course, we're 100 percent secure. No question."

But as in playing cards, when the stakes are high, at some point someone has to call the bluff – and these confident players better have a good hand. Probing security questions could come either from a potential customer (a less risky scenario), or an attacker who might actually try to hack your shiny toys in order to get the answers (far worse if he succeeds). In the first case, you lose one security-conscious customer, while in the other real money is on the line. In this article, I will demonstrate why you shouldn't rely on Your gut feeling, but rather go for hard evidence.

Customer on it Data Leaks?

Think of what could happen if you leaked your customer data? Adobe has recently been fined 1 million dollars to settle a lawsuit regarding a data breach affecting over 38 million people[1]. Sounds scary? The EU isn't any safer either, but the General Data Protection Regulation will soon come into force and regulate data breaches, imposing fines on those guilty of non-compliance[2]. The consequences of security incidents for businesses can be disastrous. In the past, some companies, including those operating in the security field, had to file for bankruptcy after security failures had been revealed[3].

Operational Failure

Security issues don't have to be related to applications only, but they may affect the development process as well. Recently it has come to light that backup files stored on Capgemini's web server for the international recruitment company Michael Page were exposed to the whole world due to enabled directory listing[4]. This only shows that no one is immune to failures, not even global players such as Capgemini.

The Inside Job

One individual can cause significant damage, let alone bring down an entire company. There have been incidents where this happened accidentally – for example, in the case of an "rm–rf" command in some bash script, without a properly set directory, which wiped out everything it found, including customer-related data and even

[1] | https://krebsonsecurity.com/2016/11/adobe-fined-1m-in-multi-state-suit-over-2013-breach-no-jail-for-spamhaus-attacker.

[2] | http://venomit.com/scary-facts-about-gdpr.

[3] | www.bloomberg.com/news/articles/2015-02-09/altegrity-files-for-bankruptcy-after-losing-vetting-contracts.

[4] | www.troyhunt.com/the-capgemini-leak-of-michael-page-data-via-publicly-facing-database-backup.

backups[5]. But what if such an act is malicious? Do you know and control who can access a given resource and who should not? What about that disgruntled employee with too much security clearance[6]?

Us? Who Would Want To Hack Us?

You might also be thinking: "I'm not the target". Well, maybe not. But what if the situation changes as your company grows? What if you're not the target, but just a means to attack one of your customers? This is what happened when a heating system of a building in Finland was disabled in winter due to a DDoS attack[7]. This incident might seem innocuous, but there are much worse examples of such attacks.

Third Party Components

Do you monitor if the libraries that you use are up to date and do not contain any known security issues? How often do you do this? Do you run automated checks? One of Polish banks probably chose to ignore these questions and their negligence cost them serious money[8]. If you do not monitor your third party components on a regular basis, try OWASP Dependency Check[9] or Retire.js[10]. It's a free utility worth having a look at.

Keeping Up Appearances Vs. Stark Reality

Sometimes the way we perceive the security of our system and how secure it actually is are two completely separate realities. In my professional experience I have seen examples where the software architect's view of the application security was very different from the reality known to the programmer. "Yes, we have security requirements in place, and all my programmers are obliged to produce the code with those guidelines in mind." But then the other side says: "Yes, we know about those requirements, but nobody really follows them. They're either incongruous with reality or just too time-consuming. We don't have enough time to focus on the security of our code because the priority is to make it work as expected."

Security Pitfalls In An Agile Environment

Security testing is often done too late. For a product developed in line with the agile approach, where the code changes with a two-week iteration, security or penetration testing done once a year (or even once every two years), without any other security-related activity, is simply not enough.

Fixing security issues only once a year will create a dangerous time window in which vulnerabilities can occur without being detected. Perhaps security issues should also be approached with an agile attitude: how about setting aside time for a sprint dedicated solely to security issues, maybe once every quarter? Simple steps can be implemented to not only facilitate learning about security threats, but also to find out how to handle their prevention, detection, and even automation.

5 | https://krebsonsecurity.com/2016/11/adobe-fined-1m-in-multi-state-suit-over-2013-breach-no-jail-for-spamhaus-attacker.

6 | https://krebsonsecurity.com/2016/11/adobe-fined-1m-in-multi-state-suit-over-2013-breach-no-jail-for-spamhaus-attacker.

7 | http://metropolitan.fi/entry/ddos-attack-halts-heating-in-finland-amidst-winter.

8 | https://badcyber.com/errors-threats-and-extortion-history-of-a-bank-hack-part-one.

9 | www.owasp.org/index.php/OWASP_Dependency_Check.

10 | https://retirejs.github.io/retire.js.

What Did You Do To Cover Your (S)aaS?

So, what about you? Is your SaaS truly secure, or do you just think it is? Are you 100 percent certain it is absolutely bulletproof? If I managed to get you start challenging the reality behind the security of your SaaS, go a step further and see the questions listed below. They should help you assess how secure your SaaS really is. So let's gather some hard facts together.

TESTING

- Do you independently verify the security of your applications?
- Do your customers flag and report on security vulnerabilities?
- Do you have any security requirements in place that you have to comply with?
- Do you use automated tools dedicated to security (vulnerability scanners, source code scanners)?

EDUCATION

- Do you train your programmers on secure development practices?
- Do you train your Q&A people on detection of application vulnerabilities?
- Are your teams interested in the application security field?
- Do you have secure coding guide?
- Do you gather knowledge related to application security?

MONITORING

- What do you monitor?
- Do you monitor all vital components of your systems?
- What security relevant events do you log?
- Can you distinguish between the log footprint of a scanner and a human being?

INCIDENT RESPONSE

- Can you quickly block selected accounts?
- Can you quickly block given IP addresses?
- Can you disable a selected functionality?
- Are you ready to disable an entire application?
- Are you ready to send a message to your users saying something bad has happened?

www.securing.pl/en

Need help? Should your answers be "No" or "I don't know" remember: as long as you fight, you're a winner. If you need professionals to guide you through the process of integrating appropriate security mechanisms in your source code and at the same time instil a security mindset in your teams,

give us a call.

Who Are We?

We are SecuRing, a Polish security company founded in 2003. Since the outset, we've done over 400 successful security assessments in more than 15 countries. We specialize in the application security area, and most of our clients are big local and international banks, financial institutions, government institutions as well as software houses and SaaS providers.

Following our motto "more than security testing", we always go the extra mile to make sure our customers and applications hit the security mark. With a focus on individual needs, we provide an in-depth analysis of the landscape in which a given application exists to help protect it from real threats.

My colleagues and I are actively sharing our knowledge and research outcomes at various IT security conferences around the world, like AppSec EU, Black Hat USA, DeepSec, and HITB to name just a few. Currently, we are focusing on areas such as Host Card Emulation (HCE) payments security and Bluetooth Low Energy communication security used on various IoT devices and "smart" tools. ■

securing

A REVOLUTIONARY APPROACH TO ANTI-RANSOMWARE SOLUTIONS

INTRODUCTION TO ANTI-RANSOMWARE SOLUTIONS AND THEIR APPLICABILITY BOTH ON-PREMISE AND CLOUD-BASED, IN RESPECT OF EFFICIENCY

BY FERENC FRESZ

FERENC FRÉSZ
is the CEO of Cyber Services, dealing with Information technology and information security related services, special cybersecurity services in homeland and abroad for international markets. Previously, he worked for the Hungarian Ministry of Defense and Ministry of Home Affairs, leading projects respectively related to military cyber capabilities establishment and to Information systems' preventive cyber defense. Ferenc Frész has many years of experience in the cyber defense exercices.

Ransomware, more precisely crypto-ransomware, is a kind of malware aiming to infect IT systems unnoticed, catalogue and encrypt all documents that represent value for the users, and finally demand a payment against decrypting and making the files available again for the users. Ransomware poses threats to individuals as well as to organisations: the main difference is that organisations, beyond the ransom itself, can expect other losses caused indirectly by the ransomware, like expenses due to downtime, data restore from backups, and damaged reputation.

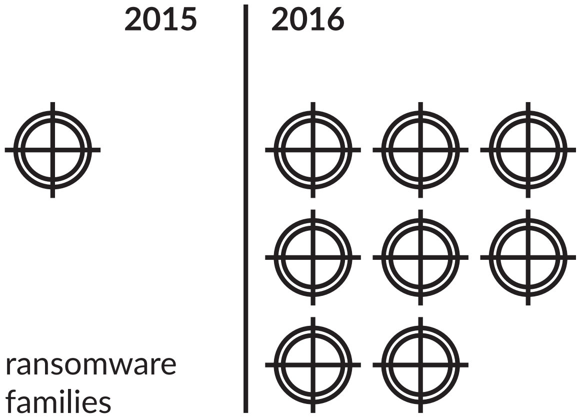
For instance, the Hollywood Presbyterian Medical Center (Los Angeles, USA) paid USD 17k in February 2016[1] as ransom. And the mentioned institute is not a very rare exception: many home users, companies, even police departments decided to pay (a sum of USD 209 mn just in Q1 2016) to the online criminals[2] in order to re-establish their business continuity.

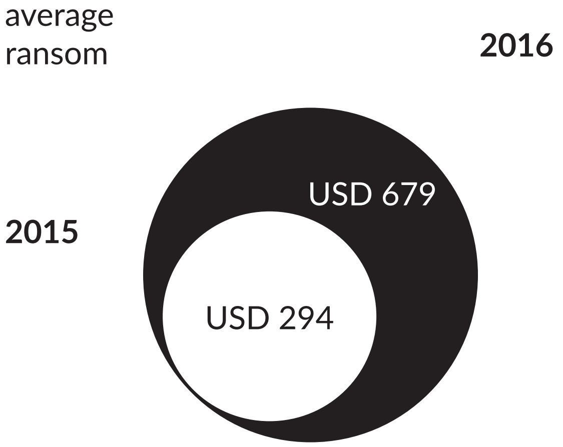
Although the proof of concept of ransomware dates back to the 1990s, it has reached a mature level only in the past couple of years. Besides its quick technical evolution, a dramatic development is also reflected in numbers: only in the course of a single year (from 2015 to 2016) the number of ransomware families has risen 752% (from 29 to 247), and the average

[1] | Polish cyberspace security system www.cert.pl/wp-content/uploads/2015/12/nask_rekomendacja.pdf.

[2] | Polish cyberspace security system www.cert.pl/wp-content/uploads/2015/12/nask_rekomendacja.pdf.

ransom has grown from USD 294 to USD 679[3]. According to the estimates of the US Federal Bureau of Investigation (FBI) the amount of ransom paid in 2016 has reached USD 1 bn[2].





The numbers speak for themselves: ransomware development nowadays is entirely motivated by the possibility of unprecedented financial gain. The possible profits resulting from card data theft fraud are restricted by the countermeasures taken by banks and the awareness of clients. The demand for industrial and government espionage carried out by cybergangs is limited by the annual budget of government agencies and enterprises. Therefore, in contrast to all earlier business models, cybercriminals using ransomware have gained extensive possibilities for potential growth as they encounter the victims they demand the ransom from directly.

The above reasons resulted in a 'gold rush' behaviour among cybercriminals spreading ransomware. The technology of ransomware has developed so much that industrial-scale service providers offering Ransomware-as-a-Service are emerging on the illegal online marketplaces of the darknet.

The most convenient device to let ransomware arrive at a victim's computers has been social engineering. Cybercriminals started to spread e-mails that seemed to come from credible entities and lured users to click on malicious links or attachments. This technique is still responsible for around 60% of infections[4].

After the initial infection vector, spearphishing started to culminate, and attackers began to use more and more sophisticated techniques: drive-by download, watering hole, malvertising and finally targeted attacks. Malvertising and targeted attacks are the hardest to resist, because these methods employ exploit kits that may contain exploitation procedures targeting previously unknown zero-day vulnerabilities.

According to Symantec, the ratio of affected organisations is constantly growing compared to individualsi. Industries more actively using the Internet are more likely to became the subject of a ransomware attack. In case of an enterprise or a renowned organisation, the losses caused by downtime and the damage of reputation can possibly even exceed the ransom itself. Anyway, paying the ransom does not solve anything: there is neither a guarantee that the files will be restored by the perpetrators, nor any assurance that the same attack will not hit the organisation again in the future. Therefore, it is more advisable to focus on prevention by investing in reliable backup and anti- ransomware solutions.

[3] Polish cyberspace security system www.cert.pl/wp-content/uploads/2015/12/nask_rekomendacja.pdf.

[4] Polish cyberspace security system www.cert.pl/wp-content/uploads/2015/12/nask_rekomendacja.pdf.

Some system administrators and most private users have presumed that advanced antivirus software packages would fight ransomware since the threat was categorised as crypto-malware. However, they were bitterly disappointed. Motivated by prospective financial gain, cybercriminals could become very successful by employing differently packaged, obfuscated malware at each wave of the attacks, in order to circumvent the signature-based blacklisting used by most AV packages. Although antivirus software with advanced memory scanning was able to find the known binaries running in the memory, it was often too late: by then, the droppers infecting the systems had already slipped under the radar and the encryption process had already started.

More advanced antivirus producers have started to bring specialised tools to the market, either for free or commercially distributed. Some of these tools are called on-premise protection software. On-premise means that the creators of such software prepared the tools to combat known ransomware families, and the resulting tools are sensitised to specific IOCs (Indicators of Compromise) or even memory signatures of binaries originating from these families. These tools may also be able to deal with future variants of already known ransomware families, but unless they are updated in time by their vendor, they are determined to fail when facing an entirely new breed of ransomware.

As a newer technology, cloud-based solutions mostly rely on artificial intelligence or machine learning, but these powerful methods desperately need resources hosted in the cloud. The weak point of this approach is that these resources are way out of the client's control and so depend on the service provider. As the direct control over security measures is given to the service provider, it cannot be predicted if such a cloud-based solution will not start to block legitimate or even vital functions of the client enterprise. Apart from that, cloud-based solutions cannot be effective when certain subnets have to stay isolated from the Internet.

Unfortunately, the above-listed solutions do not really consider the fact that most ransomware run and encrypt the organisation's most important documents on behalf of the originally trusted but already deceived user. This makes protection against ransomware hard: an effective anti-ransomware system needs to be instructed about the user's legitimate behaviour and block any illegitimate moves. Since most vendors satisfy the market's demand for the comfortable set-and-forget solutions, they avoid the challenge of protecting the user from their own mistakes, or a possible misuse. Teaching a system to recognise desired and undesired user behaviours can never happen in a quick drop-in introduction scenario.

When Cyber Services[5] started to examine the challenge posed by ransomware, a slightly different approach has led to a similar idea. The basic expectation users and enterprises have towards any anti-ransomware solution is no more than to protect intellectual property and vital business-critical documents from undue access of any unwanted actor. This approach is obviously a much broader one than the elimination of the threat originating from known ransomware families. Cyber Services was admittedly looking for a solution against other kinds of malware, like APT (Advanced Persistent Threat) used in espionage campaigns as well.

Data Loss Prevention (DLP) systems can protect users from their own mistakes or a possible misuse by employing reliable and strict file access and applying executable controlling tools. Cyber Services has found a DLP partner and jointly developed the most comprehensive anti-ransomware product on the market. Named Armor, an acronym for Advanced Risk Mitigation of Ransomware, it combines all DLP tools with professional cyberthreat intelligence services, in order for Armor to create and introduce the right behaviour-based protective rules into systems. This combined approach makes it even more effective against ransomware and other malware, while making the product friendly for both users and system administrators.

During the implementation phase, the system behaviour-based rules are completely tailored to the needs

[5] Polish cyberspace security system
www.cert.pl/wp-content/uploads/2015/12/nask_rekomendacja.pdf.

of the protected organisation. The whole system is based on a thorough logging of events. All processes are evaluated and the desired and legitimate processes are expressed in corresponding exception rules, while harmful accesses are blocked. This approach demands a definition of both the allowed, positive activities and the restricted, undesired, harmful actions by the management, system administrators and single users. Users can be informed about the blocking actions. Such regular maintenance makes sure that the anti-ransomware system develops with the organisational needs and stays effective. Integration tasks are performed by the vendor; maintenance tasks can be taught to local system administrators or alternatively carried out regularly by the vendor as well.

One of Armor's user-friendly features is Application Management, where the system administrators can conveniently classify executables on a graphical user interface even by using drag-n-drop, creating whitelists to allow the desired processes. The inventory of executable files is maintained automatically by the client agent modules running on each workstation and server. Besides, by default, Armor blocks the running of all grey-listed applications not listed earlier as allowed.

Apart from the Application Control feature, files and data types can be protected by path or extension effectively by allowing them to be accessed only by given applications or users, at given periods, etc. Special rules can be defined for removable media. Adding the function of encryption protects the data on the move. Host Intrusion Protection rules make sure that any accidentally shared folder is only accessible by a well-defined circle of computers but not by benevolent or malicious guest users.

Configurable alerts make security violations promptly visible to management and system administrators, while syslog compatibility integrates the solution to the enterprise security infrastructure, e.g. to a SIEM. Thus, the solution has 17 levels of control to intervene if a contemporary ransomware employing multi-level droppers and encrypting executable is trying to reach the user's valuable data.

To ensure that no deceit or human error causes unwanted ransomware to run, the related CTI (cyberthreat intelligence) service continuously blacklists all known ransomware binaries. The list of known ransomware executables is updated on a regular basis in the installed software. Such protective functionality is highly effective even in isolated environments. The explanation is simple: a basically protective system is integrated into the client's system that is built on whitelisting and on rules based on legitimate user behaviour.

To close the circle, a valuable anti-ransomware solution provides real-time reporting and alerting functions for the organisation. This significantly improves and helps handle any potential incidents, far beyond ransomware threats. Overall, instead of more traditional antivirus applications, current ransomware threats much rather require a well-designed endpoint protection system with significant DLP (data loss prevention) capabilities. It is an added value when such a new layer in the security of workstations and servers coexists well with existing antivirus systems and authentication schemes, and integrates fully with Active Directory.

In summary, let us take a different path to minimise current ransomware threats, as data loss prevention may lead to revolutionary approaches and effective protection. Since the new approach is based on low-level logging and access control, even the most sophisticated processes can be described and allowed while all unwanted moves can be blocked via rules and policies. The keywords to remember are: logging, whitelisting, and technical education. Additionally, apart from the technical measures, the introduction of such processes raises the data security awareness in any organisation. ■

CyberServices

Academic Models For R&D Results Commercialisation in the IT sector in Poland

by Krzysztof Oleksy

Large IT companies contract to carry out such projects out to academic teams, or establish new startups with them using their own funds.

Public grants for development work are largely conditional upon contracting the development work from research entities. Disappointingly, however, according to the NASK (Research and Academic Computer Network) report "Polish cyberspace security system[1]" , quoting the document "National Smart Specialisation[2]" , ICT and IT security domain is not considered a priority of the Polish research and innovation policy until 2020, and therefore projects from this domain that are important for Poland are not eligible for funding under operational programmes. Notwith-standing, large IT companies contract to carry out such projects out to academic teams, or establish new startups with them using their own funds.

What are the figures? Statistics of the Central Statistical Office of Poland reveal[3] that only 10.6% of service

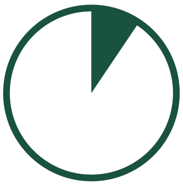
[1] | Polish cyberspace security system www.cert.pl/wp-content/uploads/2015/12/nask_rekomendacja.pdf.

[2] | National Smart Specialisation (KIS) www.mr.gov.pl/strony/zadania/wsparcie-przedsiebiorczosci/innowacyjnosc/krajowe-inteligentne-specjalizacje.

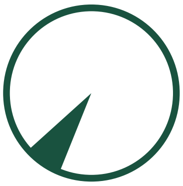
[3] | Innovative activities of enterprises in Poland in 2013-2015 http://stat.gov.pl/download/gfx/portalinformacyjny/pl/defaultaktualnosci/5496/14/3/1/dzialaln_innowacyjna_przedsiebio_w_polsce_w_latach_2013-2015.pdf.

enterprises were involved in innovative activities in 2013-2015, while new or markedly improved product or process innovations were introduced by 9.8% of service businesses. According to surveys on innovative activities of small and medium-sized enterprises in the period from June 2011 to May 2012[4], collaboration with research sector entities was among the least frequent, and applied only to 2% of the surveyed entities.

What are the underlying reasons? Disappointingly, the expectations of business and research entities regarding their mutual cooperation are sometimes rather divergent. The needs of businesses in this respect are quite clear. They require new solutions to be quicker, less expensive and better. Ideally, all three in one.



10,6%
of Polish service companies involved in innovative activities



new or markedly improved products in 9,8% of them

The cost of maintaining an in-house research and development department is often too high, and not every entity is capable of establishing a separate company for the purpose, and hence their interest in collaboration with universities. Researchers, on the other hand, do not want cost cutting at their expense, and need to ensure the results of their research these needs, if both attitudes appear reasonnable? Let us take a closer look at what the process essentially is.

1. University Offering and Business Expectations

Let us first try and locate the offering of universities relative to the expectations of the IT sector.

The Cracow University of Technology is a leading Polish research institution active in IT security projects. Research units and teams from as many as four university faculties deal with cybersecurity-related matters[5]:

Faculty of Electrical and Computer Engineering

The E-13 IT unit is dedicated to failure-proof system research, design and validation, while the E-3 Chair of Automation Technology and Information Technologies deals with issues like developing artificial intelligence-based system.

Faculty of Mechanical Engineering

The Network Technology Laboratory (M-76) is primarily specialised in the operation of modern computer networks, enabling integrated data, voice and multimedia services transmission, network administration and security, and in operating systems for network servers.

Faculty of Physics, Mathematics and IT

The Information and Communication Technologies Institute (F-5) conducts research and development work on e.g.[6]:

- signal processing and analysis (1D, 2D, 3D),
- research on context awareness of mobile devices,
- design of computer network, security, monitoring and network traffic analysis systems,
- computer system virtualisation

[4] Science and business collaboration www.parp.gov.pl/images/PARP_publications/pdf/18863.pdf.

[5] Source:Cracow University of Technology website.

[6] The institute's offering is published in the database of the project company INTECH PK http://www.s2b.pk.edu.pl/#show?id=86.

Cybersecurity-related implementations of the Information and Communication Technologies Institute include:

1) Architecture analysis and research for cloud services based on context-awareness methodology [for Orange]
2) PATHFINDER – an integrated platform for the financial sector based on the concept of neural networks, comprising three modules: loan, insurance, and debt recovery [for VSOFT S.A.]
3) STREAMLINER – a tool and maintenance platform comprising four prototypical components: update server, mechanism for reporting incidents directly from the application, modelling and delivery of independently operating update packages [for VSOFT S.A.]

A detailed offering and mutual expectations are best exemplified by statements from representatives of universities and small businesses interested in research and development collaboration.

dr hab. Zbisław Tabor prof. PK – head of the ICT Institute at the Faculty of Physics, Mathematics and IT of the Cracow University of Technology

Our offering for cybersec businesses includes research work related to computer system security (network security and monitoring system, and network traffic analysis), and computer system virtualisation, including programming for hypervisors, productivity isolation, cloud processing, cloud service models (SaaS, PaaS, IaaS), industrial network services.

Cooperation with cybersec businesses embodies the mission of the university as regards the transfer of knowledge to the business, and allows us to adapt the research profile of the institute to the actual technology problems and challenges faced by companies from the sector.

Ewelina Kurzeja – expert of Exnit Sp. z o.o., independent service provider on the data security market:

So far, we have not had a lot of experience in collaborating with universities.

We are interested in developing projects with industry experts, who are well-versed in the current state of technology to help us verify the technical aspect of our business concepts and to jointly develop prototypical business ideas. What is crucial for us is not the academic achievements, but rather genuine experience of translating technology into services.

2. Potential Areas of Cooperation

Collaboration between businesses and universities may adopt various forms, depending on its scope or nature. Employers are usually interested in the following project types:

- contracted work funded with the company's own funds, to work out and transfer rights to know-how or a prototype,
- projects developed by consortia or partnerships, focusing on research grants awarded to companies for the implementation of new products or services by research institutions,
- smaller expert and consultancy services, to provide a better direction for the company in terms of its work to gain a competitive advantage,
- cluster-type permanent cooperation structures and industry-specific or sector-specific associations,
- spin-off companies.

In the case of single, small or pilot projects, the optimum cooperation model is science to business (S2B). If the scale of the project is greater and requires a more detailed regulatory framework (e.g. in terms of responsibilities, rights to results and mutual liability), a consortium, that is an entity without legal personality, is formed. However, if the joint product or service implementation and sale requires not only permanent cooperation, but also the commitment of resources contributed by the participating entity and the sharing of risk, it may be necessary to establish a separate legal entity. Universities in Poland use their special purpose vehicles companies (INTECH PK sp. z o.o. in the case of the Cracow University of Technology) for such projects (requiring capital or in-kind contribution, such as technology, equipment, or real property).

Establishing a spin-off company with the university is an opportunity to share the investment risk at an early stage of technology development, and a guarantee of higher motivation and commitment on both sides. For large companies, it also constitutes an opportunity to obtain public funding for technology development, and does not require them to incur expenses relating to permanent, in-house research staff. On the other hand, it should be considered that the company incurs fixed costs of its operation, and there is a number of legal, accounting, and tax doubts in particular with respect to public funding of business operations.

The project was a follow-up on a contract delivered one year earlier in cooperation with the Cracow University of Technology, and was a consequence of achieving the objectives assumed by both parties to the contract.

Another factor in the choice of a cooperation model is the pool of funds and equipment available, team make-up and personal motivations of the persons involved in the cooperation. Key success factors for spin-off companies are:

- appropriate documenting and protection of know-how, as well as regulated ownership rights
- operating focus on market products and services, as well as global aspect of the business
- motivated team, open to cooperation

3. How to Manage R&D Projects on Cooperation With A University

An example of successful cooperation between the academia and business was a research and development project concerning context data management solutions, developed together with Orange in the years 2012-2013.

The research involved in the project included examination of the state of technology in context awareness (in particular semantic technologies, query language standards and data descriptions), on the basis of which a model and prototype of an engine for context data querying with approximation mechanism was proposed.

The solution considered the information that we can receive from the querying service, including certain factors and elements that ensure an appropriate level of data reliability, returning, in response to the query, data that most approximate the desired data.

The project was a follow-up on a contract delivered one year earlier in cooperation with the Cracow University of Technology, and was a consequence of achieving the objectives assumed by both parties to the contract. Results of the work (a prototype of system management, including a database, engine, interface, and query rules) provide opportunities for development and improvement of services and projects at Orange.

Key factors in the success of this case were the clear setting of the rules of communication and splitting the workload within the team. Most of the tasks were carried out remotely, and the achievement of milestones and their determination was agreed on during teleconferences between Warsaw and Cracow. On the university's end, all works related to the substance of the subject matter were carried out by the staff of the ICT Institute, whereas business and formal support of the contract was handled by the university's experts on commercialisation. PhD and MSc students were also included in the project and played active roles.

4. Confidentiality

A key aspect for all institutions dealing with cybersecurity is to ensure security of the processed data. This requirement results from the nature of IT-related projects (intellectual property is a strategic resource here), and the availability of protection tools for software-embedded knowledge (patenting options on the European market are significantly limited). How to ensure confidentiality of the developed know-how, then?

There are no one-size-fits-all remedies. Each institution typically has its own developed information-confidentiality policy. There are however a few golden rules, the application of which was proven in practice during the projects developed by the Cracow University of Technology.

RULE 1: drawing up a thorough "opening balance" determining, before the beginning of cooperation, the extent of the contribution of both the contractor and the employer. We should remember that, next to the knowledge and technology delivered by the contractor, the object of confidentiality also includes business data supplied by the employer.

RULE 2: specifying what "new" knowledge that will be generated in the project (in particular, the separation between what is open and what is confidential), and who will have access to it on the contractor's side. Confidential know-how is understood here as information that is: Written either in paper documentation or computer files, described (in a way which is comprehensible to an average expert), not available publicly, secured, not patented, with operation proven in practice, useful for business, having a tangible value.

RULE 3: signing a precise and enforceable confidentiality agreement. The document should take into account the following aspects:

- scope of information (e.g. on a specific technology or company) and its type (e.g. technical, process, economic, financial, commercial, legal, and corporate)
- form of materialisation (e.g. verbal or written information, electronic record)
- form of transfer (i.e. whether the information must be explicitly marked as confidential or not)
- scope of confidentiality (i.e. what activities are prohibited)
- term (duration) of the confidentiality provisions
- rules of providing information required to perform the contract to employees and collaborators (so that not to tie the contractor's hands)
- penalties for wilful and inadvertent breach of confidentiality (typically expressed in amounts, or based on the value of damage so inflicted)
- exclusions (e.g. information in the public domain, provided by a different source, information which confidentiality was repealed by courts).

We should remember that there are two conflicting trends in terms of confidentiality. For businesses, it is key to retain information monopoly, while it is the essence of research to share the knowledge developed in its process. What is more, researchers usually want to ensure they can use the knowledge developed for businesses for academic purposes, such as publishing papers or speaking at conferences. Therefore, we should consider that it will not always be possible to obtain the consent to keep confidential even the mere fact of cooperation, names of entities involved, or its scope.

RULE 4: establishing clear terms of acceptance and transfer of the developed knowledge, in particular the form of the transfer (electronic recording or hard-copy documentation, file format, if any, confirmation that the remaining carriers were destroyed by the contractor, etc.).

RULE 5: ensuring the transfer of e-rights to results to the employer (if so agreed in the contract), in particular if subcontractors performed their work under civil-law contracts.

The practice shows that errors in the confidentiality domain (both in relations with external entities and own personnel) may cost us dearly and adversely affect the image of our institution.

5. Example of B2B Model of Cooperation With the University: INTECH PK

Where direct cooperation between the business and the research institutions is not possible, or that formula is not sufficiently productive for both parties, the Cracow University of Technology offers the option of business to business (B2B) cooperation. For that purpose, the university established a company INTECH PK, operating on the market since 2014. Its core market activity is to generate revenue from services based on the university's intellectual resources, in particular through commercialisation of results of research and development work carried out at the Cracow University of Technology. INTECH PK establishes spin-off companies, delivers expert studies, training and business consultancy, as well as provides agency for contracted work and implementation projects. INTECH PK has an agreement in place with the university which governs the rules of access to the university's resources (experts, research equipment, infrastructure, logo).

A benchmark example of cooperation with businesses as regards new product and service launches are innovation vouchers. Companies such as INTECH PK are authorised contractors for such projects in the Małopolskie province.

The role of the company is to carry out research work where its peculiar features require multidisciplinary teams, in particular from various research institutions, or experts without an official academic affiliation. The company has therefore much more freedom in selecting contractors and acquiring materials and services necessary for its work. The company is also capable of effectively conducting all business activities involved with R&D work (legal aspects, intellectual property, contracts, billing, negotiations, submission of proposals) as it employs and cooperates with business practitioners, specialising in new technology implementation.

Time will tell whether the implementation of innovations in the cybersec area in collaboration with universities is an artificial spin, a temporary fad, or the future for those wishing to compete on the market with new products and services.

Collaboration with universities on innovation in your business growth strategy is nevertheless worth considering. Try it with the Cracow University of Technology! Contact INTECH PK – we know-how! ■

PK

INTECH PK

ABOUT THE AUTHOR

Krzysztof Oleksy is responsible for the commercialisation of knowledge developed at the Cracow University of Technology. He has extensive experience of managing projects involving cooperation with the industry and academic entrepreneurship. Next to raising funds for those projects and their coordination, he provided consultancy services for young entrepreneurs. Participant in the "Top 500 Innovators Science-Management Commercialization" programme of the Ministry of Science and Higher Education carried out at the Stanford University, US (2013).
Now Vice-President of the Management Board of INTECH PK (a project company of the Cracow University of Technology), he is involved in the establishment of high-tech companies and management of the university's intellectual property. Co-author of the company's organisational concept and member of the project team funded under the SPIN-TECH programme.

A SILVER BULLET?

BY MAREK OSTAFIL

Many industry sectors are looking for the best access control methods. Financial, military, national security services, and industry IT experts all want to make sure that the right person has access to the right account, sensitive data or technological processes.

Passwords are the most popular method of access control, but the ubiquitous user login method is widely known to be the weakest link in cybersecurity today. Stolen passwords mean stolen identities. Other user authentication/login methods, such as PIN codes, smart cards, and SMS have all been compromised. Their vulnerabilities generated efforts to search for more secure user authentication techniques. Biometric technology is becoming increasingly popular and at first glance appears to be the most secure. In its original concept only the physical presence of the authorized person would grant access to restricted accounts or other resources.

What is biometrics?

"Biometrics refers to the automatic identification of a person based on his or her physiological or behavioral characteristics. (...) Biometric recognition technology relies upon the physical characteristics of an individual, such as fingerprints, voiceprint, pattern of the iris of the eye and facial pattern. (...) Examples of physiological biometric features include height, weight, body odor, the shape of the hand, the pattern of veins, retina or iris, the face and the patterns on the skin of thumbs or fingers (fingerprints).[1]"

Biometric technologies appear as a great opportunity for authorization and access management systems.

[1] | http://biometrics.pbworks.com/w/page/14811351/Authentication%20technologies#WhatIsBiometrics, http://biometrics.pbworks.com.
https://www.ukessays.com/dissertation/examples/information-systems/advantages-and-disadvantages-of-biometrics.php.
http://www.cse.wustl.edu/~jain/cse571-11/ftp/biomet/#sec5.1.
"Face & Voice Biometrics Market Examined by Global Industry Analysts in Insightful Study Available at MarketPublishers.com", PR Newswire US. 02/17/2016

Fascinating cutting-edge technology is very appealing and seems to be a silver bullet that would replace all other user authentication systems. The bad news is that biometric systems, which are starting to replace the password-based ones, come with some serious security risks of their own.

A Great New Danger

Biometrics has been announced as the most secure and accurate user authentication technology, but what seems to be its greatest strength, i.e. the identification of a physical person using permanent and highly personal biometrics, is also one its greatest weaknesses. Why? Because a person's biometric characteristics do not change over time. That includes the pattern of one's iris, retina or palm vein. They remain the same throughout the whole life. It also means that once stolen or compromised, biometric data is unfortunately compromised forever. Every human being has only a limited number of biometric features (face, fingers, eyes). In case of authentication systems based on hardware elements (such as keys, badges), a compromised token can be revoked and replaced. Also, user IDs and passwords can be changed or reset when needed.

However, when biometric data becomes compromised, this "reset" is not possible. In the event of biometric record leak or theft, users will have their permanent and most private personal data end up in unwanted hands. The user will have permanently lost control of that form of identification.

With traditional methods of user authentication—even if they are not secure or easy to use—when credentials are stolen, they can be changed, but this is not the case with one's iris. "You can always get a new credit card. You can always create a new password. [It's] really hard to get new fingers. You only have ten of them and once that information leaks, it's out and there's nothing you can do," said Marc Goodman, an advisor to Interpol and the FBI in an interview with NBC News[2].

The same characteristics that make biometrics seemingly secure are also what makes them so intrusive. When our passwords are stolen, we can simply change

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 Elctroacoustic 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

[2] | http://www.biometricnewsportal.com/biometrics_issues.asp.

them. But we are not able to change our fingerprints or our faces, at least not without a huge effort. In this case, the disadvantages of using biometrics outweigh the profits. Recent experience shows that storing any kind of personal data might be tempting to cybercriminals and hackers. Jennifer Lynch, a senior staff attorney at the Electronic Frontier Foundation warns that "data breaches are very common. If biometric information is stored on a mass scale, it can be hacked into and stolen and we may lose control of it.[3]"

Billions of usernames and passwords have already been stolen, and biometric data is not immune to this problem: in September 2015, biometric data of 5.6 million US federal employees was stolen when the Office of Personnel Management was hacked. That means 5.6 million people's biometric data was compromised. This included biometric data of secret agents. For these high security employees the result is that they are not able to work anymore. Changing their official identity will not help[4].

Biometric data is not immune to the traditional techniques of cyberattacks and data theft. But there also other dangers related to biometric technologies.

Biometric data is not immune to the traditional techniques of cyberattacks and data theft. But there also other dangers related to biometric technologies. Some examples show how easy it may be to steal biometric data and misuse it. In his article "False sense of security spreading on a gigantic scale," Hitoshi Kokumai makes a very interesting and important statement. He points out that fingerprint authentication in our smart phones is not used to make them more secure, but rather as a form of convenience. What is even worse is the fact that biometric data is stored on those devices, and they can simply be hacked. It looks that user authentication will widely relay upon biometrics and therefore this kind of data will be the target for attacks. It will be compromised. Cybercriminals are likely already working on finding a way around protection systems[5].

Researchers from mobile security company Vkansee were able to break into Apple's Touch ID system with a small piece of Play Doh in 2016 at one of the biggest events of the technological world: Mobile World Congress in Barcelona. This (unfortunately successful) experiment was similar to what security researcher Tsutomu Matsumoto did with a gummy bear a few years earlier to compromise another fingerprint sensor[6]. A group of researchers at Michigan State University have published a paper in which they describe a method for spoofing a fingerprint reader in less than fifteen minutes with the use of conductive ink printed with an ink jet printer. Even if some biometric systems are harder to crack than others, experience shows that no security system is impermeable. Biometric hackers from Germany's Chaos Computer Club bypassed Apple's Touch ID just days after its launch. They simply took a photo of a fingerprint on a glass surface, and then used it to create a fake fingerprint that could unlock a smart phone.

A year later, a member of the same hacking group, Jan Krissler, cloned the thumbprint of the German defence minister Ursula von der Leyen, after photographing her hand from a distance at a press conference[7].

Not only fingerprints can be spoofed. Some facial recognition tools can also be fooled just by using high quality photos or videos. A team of researchers in Spain

[3] | https://www.theguardian.com/technology/2015/dec/08/the-end-of-passwords-biometrics-risks-benefits, https://www.scientificamerican.com/article/biometric-security-poses-huge-privacy-risks.

[4] | https://blog.digicert.com/biometric-authentication-methods.

[5] | https://www.scmagazineuk.com/false-sense-of-security-spreading-on-a-gigantic-scale/article/531496.

[6] | http://www.dailymail.co.uk/sciencetech/article-3471718/Can-iPhone-s-fingerprint-sensor-hacked-using-PLAY-DOH-Researchers-claim-toy-bypass-Apple-s-security.html.

[7] | http://www.dawn.com/news/1154284.

managed to trick eye-scanners with reverse-engineered fake irises.

And this is only the tip of the iceberg.

There are also other dangers associated with biometrics. In addition to data theft, there are seven main points of attacks that expose vulnerabilities in biometric systems[8]:

- Presenting fake biometrics or a copy at the sensor, for instance a fake finger or a face mask. It is also possible to try and resubmit previously stored digitized biometrics signals, such as a copy of a fingerprint image or a voice recording.
- Producing feature sets preselected by the intruder by overriding the feature extraction process.
- Tampering with the biometric feature representa tion: The features extracted from the input signal are replaced with a fraudulent feature set.
- Attacking the channel between the stored templates and the matcher: The stored templates are sent to the matcher through a communication channel. Thedata traveling through this channel could be intercepted and modified, so there is a real danger, if the biometric feature set is transmitted over the Internet.
- Corrupting the matcher: The matcher is attacked and corrupted so that it produces pre-selected match scores.
- Tampering with stored templates, either locally or remotely.
- Overriding the match result.

This list shows how many points of weakness the biometric technologies have. These are all additional vectors of attacks. And it requires additional resources, research and development to create an appropriate level of security. Especially taking into account that the stake in this game is extremely high. If we are going to widely use biometric data to identify users in all areas of our life, they must be perfectly protected by all agents that possess and process biometric data. Corporations and government agencies roll out new systems that use biometric data to log into systems or services. They seem to be attractive for users and apparently easy to use: just one touch of a finger or even a selfie, and the user is logged in.

However, serious questions arise as to whether those methods can also guarantee security to the users. Biometric technologies are being presented to us as the universal solution that will enable us to securely access different services, both commercial and governmental. Biometric technologies seem to offer us the best possible way. Many corporations go for biometrics, as it seems that it offers the best user experience, thus guaranteeing customer satisfaction. And we, the customers, seem to believe that this is really the best solution. But is it really the greatest user experience? Is it really so easy to use? How often does a fingerprint sensor not recognize our fingerprint and we have to use our code to access the phone? Are we really ready to log into our bank account or confirm a transaction in a public place using voice recognition? Do they really work in such environmental conditions? Is it really a secure solution to use a selfie as a transaction confirmation? How high is the security threshold set to recognize us from a low quality image?

And as we are so fascinated by the apparent ease of use, and seem to be convinced that it is also a secure solution, do we stop to think about who has access to our most personal data? How is it really protected? What are the threats? Have we ever thought of what may happen to us if unauthorized parties have access to our biometric data? Do we really think of that?

The security issues mentioned above are not the only ones that need to be considered in the case of using biometric data. Another serious issue is the legal aspect.

Legal Issues

Another problem is the legal status of most types of biometric data. Regulations are inconsistent and lagging behind today's technological capabilities. That also concerns the issue whether government agencies are allowed to collect biometric data without a person's

[8] | http://www.nbcnews.com/mach/technology/biometric-scanning-use-grows-so-do-security-risks-n593161.

knowledge. Recent EU regulations, such as GDPR, start mentioning biometric data in the legal context but they are very generic. That is a big problem from the point of view of privacy. Unfortunately, in most cases, legal regulations come much later than any technology solution appearing on the market. That creates a time gap between who and how handles available data and regulations that also include security measures.

Let us remember that both corporations and government agencies are gathering our biometric data. The questions remain: Are they really prepared to protect it?

As was pointed out in a report by Pricewaterhouse-Coopers, even if the new GDPR introduces the concept of biometrics into the legal field, many EU countries still have very different regulations regarding the collection and transfer of biometric data. And it will continue to be so for at least the next few years. A company that holds such data—either on its own or through a third-party provider in the case of cloud computing systems—will face serious regulatory problems in case the biometric data is stolen or misused[9].

Once a user's fingerprints, face, iris or DNA profile becomes digital data, it will be difficult to protect. People are becoming increasingly aware of the very thin and porous boundary between the commercial gathering and use of biometric data and government's access to it. And the line is indeed very thin. Let us remember that both corporations and government agencies are gathering our biometric data. The questions remain: Are they really prepared to protect it? Who and under what conditions may have legal access to our biometric data? Right now this is still not a strictly regulated field.

On the other hand, there is a growing concern of users regarding the technical and legal aspects of gathering biometric data. And this is a good sign. There seems to be a higher and higher awareness of the security issues connected with biometric data. We should be aware of them and make an informed decision whether the apparently great user experience is worth giving away our most personal data. Of course, there is also another element involved: money.

Market

We cannot forget that the biometric technologies industry is a large and fast-growing market, with billions of dollars-worth of investments in research and development every year. Analysts forecast the global biometrics market in the retail sector to grow at a CAGR of 21.30% during the period 2016–2020. There are plenty of companies that offer different kinds of biometric technologies. The market is divided into segments based on biometric technology: fingerprint identification, facial recognition, hand geometry, vein recognition. There is a lot of money, including public funds, involved and invested in research on biometric technologies and development programs.

The global face and voice biometric technologies market is expected to be valued at nearly USD 3bn by the end of 2018. Geographically, the United States still accounts for the largest share of the global face and voice biometrics market. Nevertheless, most of the market growth is expected to come from the emerging economies, with the Asia-Pacific taking the lead.

As we can see, it is already a fairly developed industry. An industry that attracts investments and the attention of government agencies as well as companies that want to participate in the profits. It has already gone too far and nobody really wants to admit that it may not

[9] | http://fortune.com/2016/05/12/biometrics-passwords.

be the most secure solution. It seems like many people do not want to see the weak points of the biometric technologies, and that the money invested in their development caused more and more money to follow. There have been more and more complex systems being rolled out recently, some of them created thanks to public funds. One of them requires scanning all biometric data—such as fingerprints, iris, voice, and signature—to open a bank account. This is a huge project. But we should ask ourselves the following questions: Is it really making the life of the users easier and more secure? Is the organization ready to protect such massive amounts of the most personal data? And finally, is the development equally focused on security measures?

Conclusion

We cannot stop technological progress. However, we need to be very careful: relying only on biometrics is a bad idea, no matter how good the technology might be today or in the future. In fact, one could argue that

the better the technology, the more dangerous and invasive it is for everyone's right to privacy and ability to control who has access to our private and permanent information.

As a user identity tool, biometrics can be a convenient and accurate way to identify a person; but just as any other tool, it can be used for good or for bad. As Oz Mischli has pointed out in Adrian Bridgewater's article, biometric features are very difficult if not impossible to change, should they be stolen. If a password is compromised, it can be changed and reset; if a Client Certificate is stolen, it can be revoked and a new one issued; if an OTP device is stolen, it simply needs to be cancelled and reconfigured[10].

The advance of biometrics should be welcomed, but with caution. People should not be forced to use biometrics to identify themselves, as this may pose a great danger to their personal privacy.

Many people refer to biometrics as the silver bullet of user authentication: easy to use and highly secure. It is not. We are a long way from either, and as the use of biometrics grows, personal privacy and data security issues must be resolved. And one more thing: the system should be designed to serve people and not to control them.

Biometric only Login: Why isn't it just as good or better? A number of articles mention that the voice ID is slow and use of biometrics other than built in fingerprint sensors is cumbersome.

CYBERUS KEY vs Biometrics

The problems with using biometrics only are:

1. The user experience is poor.
2. A false negative result, which has plagued this industry, will lock users out of their accounts.
3. It is a credential just like a password and just like a password it can be stolen. Phishing attacks to get user biometrics are possible. Millions of fingerprints had been stolen from the US government last year, which makes all those users vulnerable to biometric hacks. Our system does not use any user credentials so there is nothing to steal, no phishing attacks and no ID theft.
4. If a user biometric record is stolen, it cannot be changed like a password can, so the user is now permanently at risk…forever. Unless they get their voice or face or fingerprint changed.

[10] http://www.nbcnews.com/tech/sec urity/opm-5-6-million-fingerprints-not-1-1-million-were-n432281, http://fortune.co m/2016/05/12/biometrics-passwords/

Biometrics have a problem with false negative and false positive identification failures. False negatives can render a biometric system unusable.

Using biometrics integrated with the Cyberus Key allows the biometric scan to be biased for no false negatives. This creates more false positives, but these are rendered harmless by the additional certification afforded by the Cyberus Key.

The Cyberus Key system uses one-time transaction codes to verify users, with no user credentials being transmitted or stored. One-time transaction codes have been shown to be an unbreakable cipher. The sonic handshake used by the Cyberus Key guarantees user proximity to website or device being logged on to. This means that stolen user credentials, like biometrics, cannot be used remotely by cyber criminals.

Cyberus Key identifies the user by identifying their cell phone and our unique app ID, which is tied to the user identity and validates the process with a one-time Password. Biometrics can provide additional confirmation that the user is holding the phone during the Cyberus Key logon, though the likelihood of anyone else holding it is very low. Nonetheless, in most phones, PIN or fingerprint are already in use to assure that the user is holding the phone. Using additional biometrics becomes superfluous. Still, more biometrics, like voice or iris scan or face recognition can be used in addition to provide more authentication factors.

Using Cyberus Key is much quicker and easier than any biometric. Cyberus Key identifies both sides of the transaction making sure both actors: user and website, are legitimate. This stops the most common ID theft attack: phishing. Biometrics only identify the user so they cannot stop phishing attacks.

Recent ransomware attacks direct users to download software from an attack website. Cyberus Key website identification would prevent a user from ever accessing such a website. Biometrics do nothing to prevent ransomware attacks.

In conclusion: Cyberus Key easily adds biometrics for additional authentication factors, but the use of biometrics alone, without Cyberus Key is a poor UX, can fail catastrophically, is dangerous, as credentials can be stolen and only validates one side of the transaction making phishing and ransomware attacks possible. ■

BACKUP SYSTEMS AS PART OF THE CYBERSECURITY STRATEGY

ERNEST ŁOJAN
Co-Founder and Technology Consultant in EXnIT Sp z o.o. He has almost 10 years experience working with storage, backup & recovery technologies. Participates in IT projects as technology consultant advising and designing protection policy for client's core infrastructure and applications. During these projects, he works with the industry leaders in data protection and storage like: IBM, Dell, EMC, Netapp, Veritas, CommVault to deliver the best suited solution to the client's specific requirements. He provided services to dozens of clients from different industry sectors: Telecommunications, Financials, Health Care and many Government Administration Offices.

It is an undeniable fact that we nowadays live in cyber reality. This means that almost all aspects of our business and private activities are mirrored in the electronic world. And with electronic data being generated at almost every step, it has become crucial to raise awareness about different aspects of security in the cyber world. A comprehensive cyber security strategy for organisations and firms should not only consider different domains like network access control, security systems, software development security, identity management, etc. but also Business Continuity and Disaster Recovery Planning. Businesses of any size, be they small start-ups or big enterprises, ought to have an emergency plan in case a 'disaster' happens to the IT systems on which their business relies. The fundamental element of the Business Continuity policy is a stable and reliable mechanism, a Backup and Replication System, which automates the process of copying digital data. Someone could ask:

Why should we include a backup policy in a cybersecurity strategy?

The answer can be found in some risk management concepts: we have to consider that the elements of the cybersecurity strategy at an 'access control' level could theoretically be defeated by someone 'unfriendly', thus resulting in a company's data being deleted or its IT system made inaccessible. In such cases, the ability to recover a previous version of data is the only way to bring back applications to a stable state. A good example of such critical incidents is a ransomware attack on IT systems (web, filesystems, etc.). Ransomware is a type of malware that encrypts user files in infected systems, blackmailing users for money in return for a decryption key. According to a Symantec Report, *"Ransomware has quickly emerged as one of the most dangerous cyberthreats facing both organizations and consumers, with global losses now likely running to hundreds of millions of dollars.*[1]*"*

The ability to recover an IT system after outage gets a special meaning, particularly nowadays, when a majority of firms have their services available through online applications 24 hours a day, 7 days a week. What is more, they are very often integrated with different social media, so if downtime occurs, it immediately affects existing and potential customers, having a highly detrimental effect on the company's public image and, in consequence, on the company's competitiveness.

Challenges for modern backup and replication systems

Over the last few years, the IT world has evolved significantly, forcing backup systems to address new challenges. One of the most important factors is the exponential growth of data volumes and the ability to provide near real-time data protection. For most companies, producing one backup in a day is now unacceptable. On the other hand, the pressure to speed up data recovery is also growing. All this makes backup companies put a lot of effort to develop new technologies and approaches to their systems. The truth is that the importance of backups has been known since time immemorial. We have to aware, however, that the usefulness of backup systems is dependent upon their integration with protected IT systems in terms of technologies used. Generally speaking, our backup engine has to match our applications, i.e. their APIs and architecture we wish to protect. Currently, the most desirable features include:

Support for on-premises and cloud solutions

The important factor is the place where the original data is generated and written on a mass storage device. For example, when we consider an e-mail and collaboration system, there is a huge difference between a classic approach, like on-premises Microsoft Exchange or IBM Lotus Domino systems, and cloud solutions, such as MS Office 365 or Gmail. Even if a company does not use a cloud e-mail service now, a backup system feature which guarantees tight integration and support backup and restore of cloud service elements is rather mandatory – a growing utilization of cloud infrastructure and applications is one the most certain trends in IT. A backup solution for public cloud apps and those maintained by the client but installed on public infrastructure in an IaaS (Infrastructure as a Service) model could be protected by an internal mechanism of a cloud provider. For many clients, however, it is important to keep their data in at least two independent localizations and with two different providers. In this scenario, there are solutions that offer data deduplication at source and send only modified data through a secure WAN link to other localizations: public cloud, local data centre or a private server room.

Optimization of space needed for backup storing

I mentioned deduplication as a solution for efficient data transfer across WAN, but this term has a much broader meaning. In fact, different kinds of algorithms eliminating redundant data in a backup stream have been developed and implemented in both backup software and storage. The enormous growth of data volumes used by applications and IT systems require legacy backup systems with a classic backup policy, for example daily copies with a two-week retention and weekly copies with a four-week retention, to have a backup volume which is significantly higher than the production data volume. The purpose of storing backup data on a device with deduplication enabled is to reduce written data and eliminate redundant data. We have examples from real-life implementations where the amount of data transferred during a backup task was reduced by 98 percent, while

[1] | http://www.symantec.com/content/en/us/enterprise/media/security_response/whitepapers/ISTR2016_Ransomware_and_Businesses.pdf.

in some cases only 0.05 percent of production data volume was identified as unique in a single backup task.

Efficient backup mechanism for mobile, laptop, and desktop devices

For the last few years, we have observed a noticeable acceleration of the bring-your-own-device (BYOD) trend, and its popularity is still growing in most companies. Therefore, backing up data from mobile devices is now posing an issue. The BYOD movement means that a lot of employees can use their private mobile devices, such as laptops, tablets, or smartphones, to do some activities for company they work for. The point is that in many situations they are not only just reading documents, but they are also creating content and generating data, so it is quite obvious that mobile devices can store data that is crucial for company's business operations and thus have to be protected with backups. From the perspective of an IT department, protecting data on phones and tablets present a bigger challenge. Incorporating them into legacy backup systems is not as easy as it is for laptops because their operating systems are almost always supported by backup agents software. If we check backup application compatibility tables, there are only a few which have an option for both iOS and Android. More often, we can come across alternatives such as sync and backup to cloud services, but this may not meet the company's requirements regarding the protection and control of its data. Using mobile devices to do work brings a few considerations in terms of data protection. Doing regular backups is necessary in case a device should be lost or stolen. There is also a potential risk of the company's infrastructure being penetrated by someone who can easily crack basic passwords and use the device as a gateway to access the company's IT infrastructure. This, of course, is rather a security concern than a backup strategy. However, it is important to know that many security functions dedicated to portable devices, including Data Loss Prevention (DLP), device management (MDM), and remote wiping could be provided in combination with backup by a single, centrally managed system. It seems to be the best method to guard company's assets on portable devices.

> Note: Data loss prevention (DLP) is the strategy used to ensure that sensitive data is not lost, misused, or accessed by unauthorized users. Generally, DLP software products classify and protect confidential and critical information to prevent end users from accidentally or maliciously sharing data that could put the organization at risk. Data loss prevention software and tools monitor and control endpoint activities, plus filter data streams on corporate networks and protect data as it moves. (source: https://digitalguardian.com)

Support for virtualized infrastructure backup

Currently server virtualization technologies like Vmware vShpere, Microsoft Hyper-V, and Citrix Xen have become a standard, being incorporated into almost every IT environment, even into applications which at the beginning of the virtualization era were claimed not to be working well within such architecture, i.e. transaction-oriented applications. In terms of data protection, most backup applications had to become virtualization aware and IT staff responsible for data protection had to understand how virtual environments differed from physical sever backups. Nowadays such backups are created by integrating the hypervisor layer with backup applications. Virtualization awareness means that even if there is no backup agent installed on a computer running any operating system, a backup application is able to trigger a snapshot on an up-and-running object and use it as a source to access production data (image level backup). As always, the most important are the details regarding the support for online and application-consistent backup for e.g. Microsoft SQL, Exchange, SharePoint, and Oracle databases. A backup administrator should pay a lot of attention to checking how their backup system could handle the backup of an application that may be spread across multiple virtual machines, especially those running on clustered configuration. Unfortunately, not every backup system do it at the same high-quality level.

The best way to ensure backup security and recovery is through the evaluation process, which demonstrates the effectiveness at an acceptable level. The process can include:

- General performance of both storage space utilization as well as backup and recovery times
- Support for granular restore for virtualized applications, for instance a recovery of a single file or an SQL table from a backup image
- Instant recovery feature which is a modern approach to extremely shortened time of recovery (RTO) for large virtual machines
- Support for virtualization features like vMotion/ Live Migration. One of the most appreciated advantages of server virtualization is the ability to move machines between physical hosts. At the same time, a modern backup system should be able to track those changes between backup periods.

The above points offer some general guidance for the backup system evaluation. The specific details should be identified for each IT environment.

Replication vs. Backup

Companies should be conscious of how the technical features of a backup system can influence their business. Recently it has turned out the RPO and RTO parameters offered by classic backup systems are becoming increasingly unsatisfactory. Defined for every organisational function or service, RPO/RTO parameters are identified during the Business Impact Analysis that is part of the Business Continuity Planning. Respectively, data protection systems have to offer appropriate features to accomplish the lowest RPO/RTO. For an organisation's service whose availability is critical, RPO offered by backup (generally 24 hours) is not enough; in such an environment, the replication feature is essential. Only a properly designed and functioning replication system can offer RPO on single minutes or even seconds. Unfortunately, complexity makes these systems expensive, and the IT infrastructure has to meet many requirements, such as network connection between replicated sites, hardware compatibility, additional server and storage just for disaster recovery purposes, software licences, know-how, etc. For companies which require very short RPO/RTO only for a limited number of services, it is common that ROI for the replication system is not reasonable. Luckily, the current IT market is adapting many services to cloud infrastructure. One of them is the replication feature for single IT systems, so that companies can protect the most important services without investing in the implementation of an entire spare IT infrastructure.

Disaster Recovery as a Service

Disaster-Recovery-as-a-Service (DRaaS) providers mostly built their offering on the virtualization and capability of cloud platforms to recover workloads, although some of them support replication for both virtual and physical servers. According to Gartner Inc.:

"Disaster recovery as a service is now a mainstream offering that is supported by more than 250 providers. Data center managers should use this Magic Quadrant to help them evaluate DRaaS providers. From 2016 through 2020, the use of either DRaaS or IaaS to support the failover of production applications will grow by more than 200%[2]".

Strong competition and a multitude of Infrastructure-as-a-Service offerings cause the DRaaS price policy to be very aggressive, so for many organisations this could be a good point to start their adventure with the 'cloud'. From a technical perspective, DRaaS services could be divided into those working at an OS, hypervisor, and storage level. Because of some independence from OS and hardware, services based on hypervisor level replication, especially when it is hypervisor agnostic, provide quite an interesting example. The other thing is the technique used to transfer data across WAN links. In terms of performance and RPO/RTO, Continuous Data Protection (CDP) technology, which works in an asynchronous mode, seems to be most effective. Data changes on a protected application site are monitored, with modified blocks being 'caught' in real time, compressed, and

[2] | https://www.gartner.com/doc/reprints?ct=160617&id=1-39NNEX-2&st=sb.

sent to a DR site. Therefore, the system can produce and keep many points of recovery, which is crucial when a disaster occurs; in some circumstances, it is possible that the last point of replication may also be damaged, so it is good to have the option to roll back previous versions of data. Another issue is to guarantee that the system is able to track and send changes in a correct sequence designed for IT systems consisting of more than one virtual machine. This is a necessary condition to ensure consistency when recovering such a system. DRaaS is often not a purely replication service, but it has many additional features like:

- **Testing environments.** Useful feature for the application development process or offloaded data analysis
- **Offload, long-term backup service.** When data is transferred in a reliable way, the next logical step is to keep different versions of data for longer term purposes.
- **File-level recoveries.** In some scenarios, the recovery of a single file resource without the failover of a whole system is very useful.
- **Self-service portal.** Ease of use is often underestimated, but in stressful situations an intuitive and easily accessible administration panel is essential.

What do we do in EXnIT ?

Data storage

We plan, design, and implement advanced architectures for data storing and processing. We think about information as a process that needs to be protected and managed.

Backup

Do you have a backup policy? Do you test and verify your backup regularly? Do you spend hours and days on managing and enhancing backup solutions?

We can help you by:

- providing advanced consultancy services helping customers to implement best backup solutions, archiving plans and policies;
- taking care of existing backup environments by enhancing and modernizing backup;
- providing BaaS (Backup as a Service).

Business Continuity

We think about a Disaster Recovery plan as the insurance for your information. We can help you design a high availability solution that best fits your needs and value of your data. Depending on your company's profile, we can implement DR on premise, in a Cloud, or as a Service.

Security

Our advanced consultancy services can help you to pinpoint the most vulnerable areas and design a consistent data security policy.

Education

Continuous learning is the best way to stay up to date with the dynamic technology growth as well as threats expansion. We provide a broad portfolio of proprietary courses that help IT professionals to develop their knowledge and competences.

**WE KNOW YOU CARE ABOUT YOUR INFORMATION.
THE QUESTION IS HOW YOU PROVIDE THIS CARE.
USE OUR EXPERIENCE TO DO IT RIGHT.** ■

PROMOTING EUROPEAN CYBERSECURITY INNOVATION IN THE SILICON VALLEY

CYBERSEC HUB has been the proud partner of the Global Venture Forum 2017, hosted by the Microsoft Ventures in San Francisco on 23 March. Startups, investors and corporate representatives were debating international investment strategies and the hottest technological breakthroughs in the cybersecurity realm.

During their trade mission to the United States, the CYBERSEC HUB delegates also met with other key stakeholders who drive innovation in the Silicon Valley, including 500 startups, Facebook, IBM, and Mind the Bridge.

1 INTERNATIONAL CONFERENCE

7 START-UPS

15 PITCHES BUSINESS MEETINGS

GLOBAL VENTURE
FORUM
A Perfect Storm:
Distributed Startups, Epic Waves
Create Value & Get Returns
March 23 @ Microsoft Reactor in San Francisco. Invitation-only.

More to come at www.cybersechub.eu

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