UNIUNEA EUROPEANĂ

Instrumente Structurale 2014-2020

BUILDING CYBERSECURITY IN ROMANIAN SMALL AND MID-SIZED BUSINESSES

What Small and Mid-Sized Businesses demand to mitigate Cyber threats

Proposed by: Miruna Iliescu, inquito

SEPTEMBER 2020

White Paper, „Cercetător-antreprenor pe piața muncii în domeniile de specializare inteligentă (CERT-ANTREP)" Cod SMIS 2014+: 124708

Co-financed by the European Social Fund through the Human Capital Operational Program

Școala Națională de Studii Politice și Administrative

uefiscdi

CAMERA DE COMERȚ ȘI INDUSTRIE ROMÂNIA

INTRODUCTION

CONTENTS

This is a proposal written by Miruna Iliescu, PhD student and target group member of CERT-ANTREP, founder of inquito, a Romanian SME. The present paper is addressed to the business communities in Romania.

ABSTRACT

This white paper provides an analysis on the different cybersecurity threats that can be found in SMEs' information technology (IT) environment. This study points out different regulations and best practices that helped build a cybersecurity capacity in different business environments in Europe.

Lastly, this paper provides a perspective on what services are required by Romanian SMEs to mitigate cyber threats and solve different cyber security issues.

ROMANIAN BUSINESS IT STATS

<10%

Romanian companies implement compulsory training courses or viewing compulsory material on ITC security issues (DESI, 2020)

1.2%

is the percentage of female working in ICT field in Romania of the total female employment (DESI, 2020)

CONTEXT

Cyber security was identified by the Global Risk Report 2018 as one of the three risks to global stability over the following 5 years (World Economic Forum, 2018). As of 2017, there were an estimated 3.9 billion Internet users worldwide and this accounts for more than half of the global population. As of 2019, there are 4.57 billion people online and, for the first time in history, more than half of the world's total population, 3.96 billion, now uses social media (We are Social & Hootsuite, 2020).

An important result also highlights that the expectation to work from home more frequently, even after the COVID-19 outbreak ends, is 27%. The Internet has grown and so has the rate of hacker attacks. Statistics show that 4.1 billion records were exposed only in the first 6 months of 2019 (Winder, 2019) and in 2016, 95% of the breached records came only from 3 industries: government, retail and technology (Devon, 2020). The global average of companies experiencing a data breach over a two-year period is 28%, so that makes 1 in 4 companies vulnerable to a cyber threat (IBM Security & Ponemon Institute, 2017).

This probability is much higher than for example, home burglary in the US (1 in 50), being hit by a lightning bolt (1 in 14.600), being attacked by a bear (1 in 2.700.000) or winning the lottery (1 in 175.000.000). But two-thirds of business leaders at SMEs do not believe they can fall victim to a cyber attack (Waldersee, 2019).

CONTEXT

Research shows that smaller organisations (1-250 employees) have the highest targeted malicious email rate, at 1 in 323 (Sobers, 2020). Therefore, employees of smaller organisations were more likely to be hit by email threats rather than those in large companies. In 2015, 43% of cyber attacks in general target small business and this percentage was up 9% over 2014 and in a big contrast with the mere 18% registered in 2011. Security issues come at great costs for companies as the global average cost of a data breach is $3.9 million across SMEs (Ponemon, 2019) and the average cost of a ransomware attack is $133.000 (Bera, 2019).

Even more scary should be the fact that 60% of SMEs close within 6 months of being hacked (Galvin, 2018). Despite this context, according to Digital Economy and Society Index (DESI) 2020 only 24.2% of European enterprises plan compulsory training on security. There are significant disparities across Member States regarding training courses, from Estonia, UK and Denmark (above 35%) to Romania, Greece and Hungary (below 10%).

This "It won't happen to me.. Until it does" approach is common due to lack of education and awareness on cyber security procedures, industry practices and attacks' risks. Since the COVID-19 pandemic started, the US FBI reported a 300% increase in reported cyber crimes and Google has reported a major jump in phishing attacks when 18 million coronavirus email scams per day were added to the 240 million daily spam messages (Google, 2020). According to studies conducted by specialised companies, more than 4000 new sites related to the COVID-19 outbreak were created in the past months, several of them being false (certSIGN, 2020).

EUROPEAN DIRECTIVES AND REGULATIONS

After its democratisation and commercialisation in the 90s, the Internet has become an essential part of our lives, linked to personal life, organisations and politics. The opportunities to access information and benefits start to depend on the possibility to connect to the Internet.

The legislator has the role to create laws and regulations that are necessary on issues such as definition of minimum security levels, definition of harmful activities, punishment of harmful activities, implementation of state policies related to Internet security etc. Enterprise-level metrics (ELMs) address the security level of an organisation. In spite of considerable efforts, there is no universally agreed-upon methodology to address the system security. There are some initiatives aimed at developing new paradigms for identifying measures and metrics: Institute for Defense Analyses (IDA) 2006, Idaho National Laboratory (INL), MIT Lincoln Laboratory etc.

In Europe, the European Commission acknowledged that a large part of the European economy is formed by SMEs and they tend to ignore measures in the domain of cyber security. It is obvious that the low resilience of SMEs in this field can have a negative impact on the European economy so different countries implemented different strategies to solve this issue, starting from European regulations and frameworks. While large companies have the knowledge and budgets to implement security measures, SMEs are not very much aware of possible risks and they lack access to resources that can improve its security under smaller budgets.

EUROPEAN DIRECTIVES AND REGULATIONS

1/ Directive (EU) 2016/1148. NIS Directive
The Directive on security of network and information systems is the first piece of EU-wide legislation on cybersecurity. It provides legal measures to boost the overall level of cybersecurity in the EU. Adopted by the European Parliament on 6 July 2016 and entered into force in August 2016

***2/ Regulation (EU) 2016/679 GDPR** is a regulation on the protection of natural persons with regard to the processing of personal data and on the free movement of such data. It also addresses the transfer of personal data outside the EU and EEA areas*

3/ Other relevant EU Directives
3.1 Directive 2013/40/EU is the Directive on attacks against information systems, published on the 12th of August of 2013.

3.2 Directive 2002/58/EC is focusing on the processing of personal data and the protection of privacy in the digital communications sector, published on the 12th of July of 2002.

3.3 Directive 2009/136/EC is amending Directive 2002/22/EC on universal service and users' rights, relating to electronic communications networks and services.

3.4. Directive 2002/58/EC is focused on the processing of personal data and the protection of privacy in the digital communications sector

3.5. Regulation (EC) No. 2006/2004 concerns the cooperation between national authorities responsible for the enforcement of consumer protection laws, published on the 25th of November of 2009.

EUROPEAN UNION AGENCY FOR NETWORK AND INFORMATION SECURITY RECOMMENDATIONS

Increasing knowledge and engagement

- *Developing information security and privacy standards catalogues*
- *Raising general awareness on the benefits of adopting standards*
- *Increasing SME participation in the development and review process*

Driving adoption and compliance

- *Defining certification schemes*
- *Promoting regulatory compliance through standard adoption*

Facilitating implementation

- *Creating standards specifically targeting SMEs*
- *Developing implementation guidelines*
- *Implementing a phased approach during the adoption process*
- *Promoting security and privacy by design*

Increasing capabilities

- *Creating ownership of the information security function*
- *Providing support for standard adoption*

Fostering cooperation

- *Promoting international, European and national collaboration*

Recommendations to increase the level information security and privacy adoption in SMEs (Manso, Rekleitis, Papazafeiropoulos & Maritsas, 2015)

EUROPEAN BEST PRACTICES

Research showed that there is a gap in supporting SMEs beyond the one-way dissemination of reports and recommendations. A more interactive approach should focus on specific actions to fulfil the goals of enhancing cybersecurity education, awareness and training. Best practices include projects developed by Spain, Luxembourg, Ireland or UK.

INCIBE - THE SPANISH NATIONAL CYBERSECURITY INSTITUTE

The Spanish National Cybersecurity Institute (INCIBE) is a service offered by the Spanish Government to work towards the development of cybersecurity as an instrument for social transformation and for developing new fields of innovation.

Objectives:

- *Raise awareness among employers and employees, mainly from SMEs, microenterprises and freelancers*
- *Develop applications and services that provide better understanding in order to mitigate the cyber threats of SMEs*

Activities:

- *free services to protect SMEs (Awareness Kit, Self-Diagnosis Tools)*
- *Toll-free Help Line*
- *systems review and comprehensive report*

Resources

- *Awareness Kit (focused on employees with the goal to raise a company's level of cybersecurity)*
- *Self-diagnosis tool (evaluation of the state of cybersecurity in the company)*

EUROPEAN BEST PRACTICES

UK - THE LONDON DIGITAL SECURITY CENTRE (LDSC)

LDSC is England's first specialist centre aimed at acting as primary resource for cybersecurity education for London-based SMEs (Bada & Nurse, 2019).

The selection of London as starting city was driven by its large number of SMEs and the heightened appeal to cybercriminals but it is planned to be scaled to different regions.

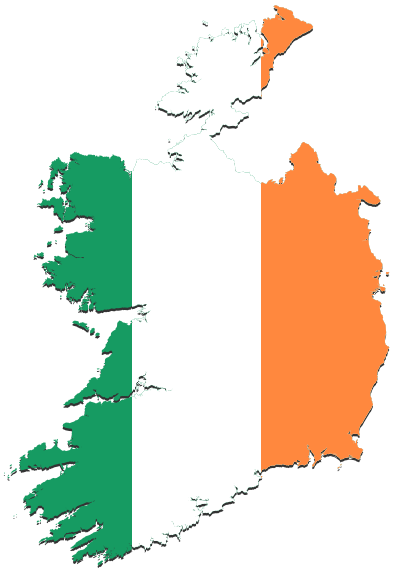
Participants:
- 626 SMEs
- Sectors: *finance, education, communications and technology, health, transport, real estate and manufacturing*

Activities:
- *workshops and lectures*
- *in-person site visits*
- *systems review and comprehensive report*

Resources
- *free services, awareness materials and support*
- *list of trusted third-party resources and services*

EUROPEAN BEST PRACTICES

CYBER IRELAND



Cyber Ireland the national cyber security cluster organisation of Ireland. It aims to facilitate the cyber security ecosystem to capitalise upon this opportunity. Cyber Ireland unites resources between government, academia and industry.

Services:

- *Cyber Ireland Events & Regional Chapter Meetings in order to build a network and make connections*
- *Talent & Skills working group; Cyber Careers Dashboard*
- *Cyber Ireland Schools Academy programme*

Objectives

- *Stronger Promotion & Supporting cross-industry collaboration*
- *Ensuring a sustainable pipeline of Cyber Security Talent*
- *Supporting Irish SMEs and startups to grow and export*
- *Enhancing collaborative R&D between industry and academia*

EUROPEAN BEST PRACTICES

CYBERSECURITY COMPETENCE CENTER C3

C3 (Cybersecurity Competence Center) aims at helping Business to face cyber risks. It works in close cooperation with private sector partners in order to train and empower businesses to better protect themselves. C3 was launched in 2017 and its structure is based on previous governmental initiatives such as CASES (Promotion of Information Security in Businesses) and CIRCL (Computer Incident Response Center Luxembourg)

Services:

- *Startups and SMEs security assessments*
- *Security focused assessments of products for investors*
- *Internal product testing*
- *Cybersecurity trainings using gaming and simulations*

Objectives

- *Increase Luxembourg's competitive advantage in cybersecurity*
- *Contribute to the development of emerging ecosystems (IoT, FinTech)*

ROMANIAN NATIONAL INITIATIVES

According to DESI 2020 there are several projects led by the government that envisage improving digital skills levels around the country, but the results remain limited. Romania has a good performance on connectivity, with high take-up of ultrafast broadband and a wide availability of fixed very high capacity networks. However, in the most recent study published by Eurostat evaluating activities related to internet or software use performed by users aged 16-74 in areas such as information, communication, problem solving and software skills, Romania ranks the lowest in terms of digital skills amongst individuals aged 16-24.

The 'Wi-Fi Campus' project, a national wireless internet platform already in the implementation phase, will provide wireless internet access service for schools (based on wi-fi), with priority on secondary schools.

Strat of 2 major digitalisation projects in the field of education: The school management information system (SIMS -Electronic Catalogue)' and Digital platform with open educational resources (EDULIB -Virtual Library).

Romania has a National Coalition for Digital Skills and Jobs (Skills4IT). This open platform includes several stakeholders, ICT companies, associations, training providers and NGOs involved in the digital transformation.

PROPOSAL

As noticed, Romanian national initiatives include few cybersecurity programmes, lagging behind most European countries in terms of SMEs' access to resources, employee training and learning opportunities. Successfully implemented by the majority of the EU members states, either is an institute, an NGO or a competence center, an entity particularly focused on the education and support of SMEs in terms of cyber security is compulsory.

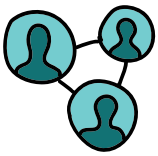
Business environment, in general, and small and mid-sized companies, in particular, require support in cyber security issues and access to services such as:

FREE SYSTEMS ASSESSEMENT

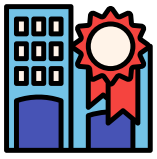
RESOURCES AND MATERIALS

HELP LINES AND SUPPORT

FREE TRAINING AND EDUCATION



CONFERENCES & NETWORKING EVENTS



INDUSTRY STANDARDS AND REGULATION

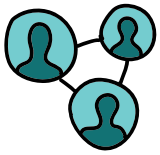
In terms of digitalisation of business and digital skills of the employees, Romanian SMEs lag behind EU member states average scores therefore combined efforts must be done in order to enhance education and skills levels of both individuals and small and mid-sized companies as a whole.

PROPOSAL

Based on other different statistics on the level of digitalisation and digital skills in Romania, the most effective and critical action that Romanian business environment should take is ***building digital skills and strengthen media literacy*** *amongst Romanians of all ages.*

Therefore, we suggest investing in quality research on the present needs and deficiencies. The results might be used in order to develop resources and materials to be used by all small and medium sized companies and to help improve their digital and cyber security skills.

RESOURCES AND MATERIALS



CONFERENCES & NETWORKING EVENTS

FREE TRAINING AND EDUCATION

The results of the studies and the resources and materials developed will be disseminated and promoted in ***conferences on basic cybersecurity topics****. The materials would be presented as well in* ***networking events*** *where they would be improved through feedback from both final users and experts in the field.*

*****Training and education events*** *should be amongst the main actions to be supported and promoted by companies in order to enhance the level of the above basic digital skills. Cyber security cannot be built and understood by the* ***employees without a proper media literacy****. Hence, in order to have better business partners and more secure business environment, a joint effort should be made by private and public organisations.*

CONCLUSION

Previous and actual national initiatives include digitalisation and digital transformation initiatives but they lack an explicit cyber security focus. Different countries across EU implemented and successfully developed several programs and initiatives. Based on their experience and recommendations, the actions that Romanian business environment should take shall have in mind educations as the main objective.

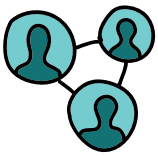
Raising SMEs' owners and their employees' awareness about cyber threats and different digital risks they could face should be the central goal.

The actions identified to be efficient in this context are:

- *free access to resources and materials*
- *conferences and networking events*
- *free training opportunities*

In order for these proposed solutions to be implemented joint efforts should be made by both public and private sector in terms of knowledge transfer, support and promotion amongst targeted SMEs.

FREE TRAINING AND EDUCATION



CONFERENCES & NETWORKING EVENTS

RESOURCES AND MATERIALS

REFERENCES

Bada, M., & Nurse, J. R. (2019). Developing cybersecurity education and awareness programmes for small-and medium-sized enterprises (SMEs). Information & Computer Security.

Bera, Ana. (2019). Ransomware Statistics. SafeAtLast. Retrieved on 18th August, 2020 from https://safeatlast.co/blog/ransomware-statistics

certSIGN. (2020). FEARWARE: Atacuri cibernetice în contextul COVID-19. Care sunt și cum ne ferim de ele?.Retrieved on 18th August, 2020 from https://tinyurl.com/yylhvk9d

Devon, Milkovich. (2020). 15 Alarming Cyber Security Facts and Stats. Cybintsolutions. Retrieved on 18th August, 2020 from https://tinyurl.com/yxsb9y3y

Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications). OJ L 201, 31.7.2002, p. 37–47

Directive 2009/136/EC of the European Parliament and of the Council of 25 November 2009 amending Directive 2002/22/EC on universal service and users' rights relating to electronic communications networks and services

Directive 2013/40/EU of the European Parliament and of the Council of 12 August 2013 on attacks against information systems and replacing Council Framework Decision 2005/222/JHA

REFERENCES

Directive, N. I. S. (2016). Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union. OJ L, 194(19.7)

European Commission. (2020). Digital Economy and Society Index (DESI) 2020. Retrieved on 28th August, 2020 from: https://ec.europa.eu/digital-single-market/en/desi

Galvin, Joe. (2018). 60 Percent of Small Businesses Fold Within 6 Months of a Cyber Attack. Here's How to Protect Yourself. INC. Retrieved on 18th August, 2020 from https://tinyurl.com/y95aw4qd

Global Risks Report 2018. (2018). World Economic Forum. Retrieved on 18th August, 2020 from http://www3.weforum.org/docs/WEF_GRR18_Report.pdf

Huntley, Shane. (2020). Findings on COVID-19 and online security threats. Google. Retrieved on 18th August, 2020 from https://tinyurl.com/y63vc55z

IBM Security & Ponemon Institute. (2017). Cost of Data Breach Study: Global Overview. Retrieved on 18th August, 2020 from https://tinyurl.com/yywyts8d

INCIBE, E. Instituto Nacional de Ciberseguridad. Retrieved on 18th August, 2020 from https://www.incibe.es/

Manso, C. G., Rekleitis, E., Papazafeiropoulos, F., & Maritsas, V. (2015). Information security and privacy standards for SMEs. ENISA: Heraklion, Greece.

REFERENCES

Ponemon, Larry. (2019). What's New in the 2019 Cost of a Data Breach Report. Security Intelligence. Retrieved on 18th August, 2020 from https://tinyurl.com/y2ttogg5

Regulation (EC) No 2006/2004 on cooperation between national authorities responsible for the enforcement of consumer protection lawsRegulation, G. D. P. (2016).

Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46. Official Journal of the European Union (OJ), 59(1-88), 294.

Sobers, Rob (2020). 110 Must-Know Cybersecurity Statistics for 2020. Varonis. Retrieved on 18th August, 2020 from https://www.varonis.com/blog/cybersecurity-statistics/

Waldersee, Victoria. (2019). Businesses find employees scarier than hackers. YouGov. Retrieved on 18th August, 2020 from https://tinyurl.com/yy2w3vbx

We are Social & Hootsuite. (2020). Digital 2020. Global Digital Overview. Retrieved on 18th August, 2020 from https://wearesocial.com/digital-2020

Winder, Davey. (2019). Data Breaches Expose 4.1 Billion Records in First Six Months of 2019. Forbes. Retrieved on 18th August, 2020 from https://tinyurl.com/yamvytu5

Project title: Cercetător-antreprenor pe piața muncii în domeniile de specializare inteligentă (CERT-ANTREP), cod SMIS: 124708

National School of Political and Administrative Studies

Co-financed by the European Social Fund through the Human Capital Operational Program 2014-2020