Security countermeasures in the cyber-world

Andreea Bendovschi
Bucharest University of Economic Studies
Bucharest, Romania
andreea.bendovschi@gmail.com

Ameer Al-Nemrat
University of East London
London, United Kingdom
a.al-nemrat@uel.ac.uk

***Abstract*— Companies and individuals are depending more and more on technology through increasingly automated processes, the use of IoT and daily activities performed through the use of internet, mobile devices and other concepts that the technological evolution deployed. But in the context of the rapid technological progress, the cyber-threats become a serious challenge that requires immediate, continuous action. As cyber-crime poses a permanent, increasing threat, corporate and individual users of the cyber-space are constantly struggling to ensure an acceptable level of security over their assets. Based on the analysis of 4,785 attacks deployed in the recent years all over the world, this paper outlines the correlations and patterns identified, under the final objective of defining security countermeasures that organisations from certain business sectors could implement in order to focus their limited resources and budget on mitigating the right risks.**

Keywords— ***security; controls; cyber-attacks; data analysis; logistic regression***

I. INTRODUCTION

As technology is rapidly evolving, it brings along new risks and challenges. Trying to support businesses and individuals, from the use of information systems in companies' IT-dependent processes to real-time mobile reporting and increasing dependency on IoT devices, technology has never before been so crucial for the daily routines and activities. However, as the importance of IT in our personal and professional lives increases, so does the impact that a potential incident might have. Therefore, just as the role of technology itself, the problem of security has never weighed so much in terms of current priorities.

As cyber-attacks flourished in the recent years to the point that 2014 was universally entitled as "the year of cyber-attacks" [1], companies struggle to ensure an acceptable level of security. However, given the limited financial, material, human and informational resources, it is impossible to reach a level of total security. [2]

The present study commences from the definition of main security concepts, identifies the main international frameworks and standards presenting the best practices in terms of security, and performs a detailed data analysis in order to identify how companies can leverage their limited resources in order to get maximum value from their security enhancing efforts.

II. LITERATURE REVIEW

Numerous authors have approached the security challenges that the cyber-space involve. P. W. Singer and A. Friedman (2014) believe the way an organisation will address vulnerabilities and risks is directly linked to the incentives the organisation perceives. [3] On the same note, Gordon, Loeb, Lucyshyn and Zhou analysed how security decisions are weighing from a cost-benefit analysis. The study outlines the fact that "cyber security underinvestment poses a serious threat to the national security and to the economic prosperity of a nation", and thus incentives should be strengthened in order to increase the companies' investments in cyber security. [4]

William Pelgrin (2014) analyses how our behavior can help improve the level of cyber-security, describing the main actions individuals can perform to improve the cyber-hygiene, and therefore, the security. [5]

Although several international books and papers focus on the design and implementation of general security controls, authors could not identify any previous work directed towards identifying patterns, risks, vulnerabilities and threats specific to certain business sectors. This may be supported by a series of factors. Firstly, the field is relatively new, and has not received much attention until the recent years. Secondly, informational resources regarding security incidents, breaches and cyber-attacks are not always available, even with a few initiatives to collect and analyse data for providing useful insights that would enable preventing attacks. Gordon, Loeb and Sohail studied the reticence of companies in sharing sensitive information regarding cyber-attacks. [4] Hausken also analysed the current data lack issues, outlining the fact that the information sharing could effectively support the timely understanding of cyber-attacks as for all relevant market players could act accordingly. [2]

Purser (2014) describes the main standards and frameworks focusing on cyber-security, concluding that the standards development speed is much slower than the rapid technological evolution, and that a joint effort from governments and organisations is required in order to ensure robust and quick adaptation of standards to the new challenges technology brings along. [6]

While these standards and frameworks have a general applicability, there are also several standards focused on certain processes/systems. For example, PCI DSS focuses on e-payment systems, ensuring trust for customers to perform credit/debit card payments using the certified sites.

Information security is also supported by national laws and regulations (e.g. Data Protection Act in the United Kingdom, Health Information Trust Alliance –HITRUST in the US, etc.). These are usually focusing on the way companies handle private details of individuals, in order to ensure data privacy and protection. However, as the use of internet goes beyond physical boundaries, regulations are closely linked to the geographical delimitation of states, and provisions or coverage may differ from one region to another. As an example, Data Protection Act is only applicable to the United Kingdom, and specifically foresees that information should not be transferred outside the European Economic Area without an adequate protection [7]; however, once the information got outside the United Kingdom, the Data Protection Act is no longer applicable.

Trying to close the gap, the European Network and Information Security Agency (ENISA) developed, in 2012, an international guide for the development and implementation of National Cyber Security Strategies (NCSS) for the EU states. [8] At the same time, the European Commission developed, in 2012, the strategy for "Unleashing the Potential of Cloud Computing in Europe", aiming to increase the awareness and use of cloud computing technology. [9] Sooner or later, most of the EU states developed national strategies that would align with the EU objectives.

However, practice showed that even with all supporting standards, frameworks and regulations, the organisations' limited financial, technological, information al and human resources make it impossible to fully mitigate the cyber-risks, and could thus benefit from knowing how to focus on addressing the right risks.

III. Research Methodology

A. Hypotheses

The main objective of our research was to identify security specific countermeasures that organisations operating in certain business sectors may implement in order to ensure the limited budget and resources are directed towards mitigating the right risks.

The research was based on 3 hypotheses, as follows:

Hp1: A correlation can be found between the type of attacks deployed and the target's business sector.

Testing this hypothesis is aiming to determine which types of attacks are deployed on certain business sectors, in order to support the design and implementation of security controls in the areas they are mostly needed.

Hp2: A correlation can be found between the security breaches and the victim's business sector.

Testing this hypothesis is aiming to identify he main root-causes that allow security breaches in organisations activating in certain business sectors, in order to support focusing the limited resources and budget in mitigating the respective risks.

Hp3: A correlation can be found between the source of attacks and the target's business sector.

Testing this hypothesis is aiming to identify which are the main sources of attacks, in order to support the better management and monitoring of information security controls.

B. Data collection

The hypotheses were tested through statistical analysis of data. The study was based on a population of 4,785 security incidents centralised under VCDB project by Verizon, one of the biggest international security market players. The data set comprises of security breaches collected by Verizon in what is believed to be one of the first initiatives to centralise relevant security incidents data and making it publicly available.

Distribution of attacks per victims' countries is depicted in Fig. 1, showing that although the attacks are spread world-wide, the most frequent targeted regions are USA, Great Britain, Canada, India, Australia, New Zealand, Republic of Korea, Ireland, Japan, Israel, Denmark, China, Turkey and Russia.

The distribution of victims' business sectors is depicted in Fig. 2. Although attacks are targeting all sectors from both private and public areas, the most representative are: Public Administration, Health care and social assistance, Finance and insurance, Information and cultural industries, Educational services, Retail trade, Administration and waste management, Accommodation and food services. These sectors represented the focus of our research, as their models passed the chi-square overall significance test for logistic regression, and the results are thus reliable.

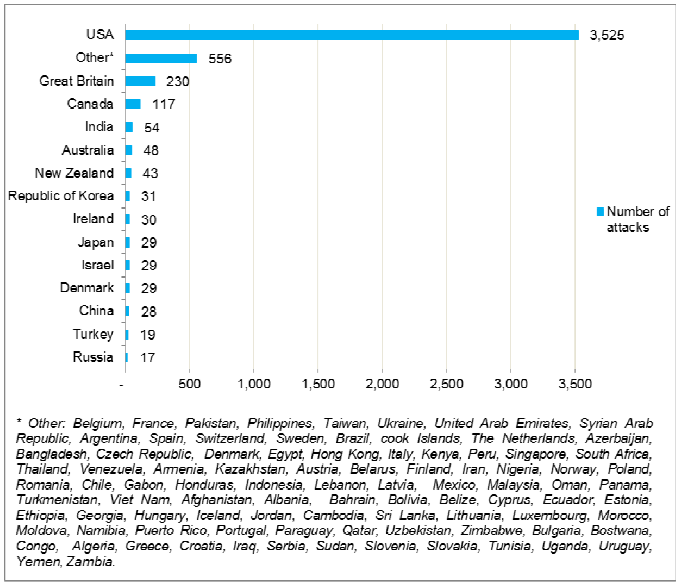

Fig. 1. Distribution of attacks per targeted countries

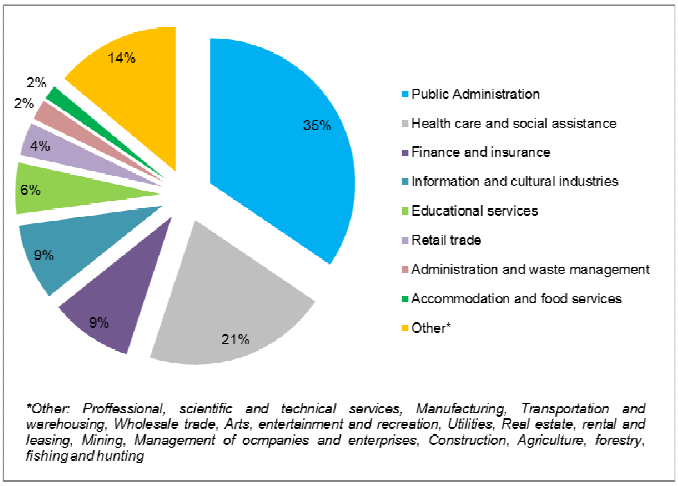

Fig. 2. Distribution of targeted organisations per business sectors

C. Data analysis

The analysis was strongly supported by dedicated software. Using Microsoft Excel, the data was cleansed and arranged in order to ensure completeness and accuracy. Although the database contained detailed information regarding the incident, attacker and victim, only the variables believed to have a statistical relationship with the business sector were included in the analysis: the victim's business sector, the attack pattern and actor, the root cause of the security breach and the discovery method. Only the valid, complete and accurate records were left in the final dataset, adding up to 4,785 incidents.

Data was imported into SAS Studio for statistical analysis. The initial model comprised of all variables authors believed to have a statistical relationship with the business sectors, as in

$$Industry = Pattern + Actor + Root\ cause + Discovery\ method \quad (1)$$

Where:

Industry – the dependent variable (y)

Pattern, Action, Actor, Root cause, Discovery method - independent variables (x).

D. The logistic regression

Defined by Hastie et al. (2008) as "used mostly as a data analysis and inference tool, where the goal is to understand the role of the input variables in explaining the outcome" [10], a logistic regression model was considered the best approach to reach the research's objective.

A stepwise model was deployed, starting from all variables and considering, for each model, only those that are statistically representative. A different model thus resulted for each of the analysed sectors, as presented in Table 1.

TABLE I. RESULTED MODEL FOR EACH BUSINESS SECTOR

Business sector	Category	Parameter	Estimate	Standard Error	Wald: Chi-Square	Pr > Chi Sq	Interpretation
Accommodation and food services	N/A	Intercept	-5.23	0.21	604.86	<.0001	As the confidence level was established to 95% and the *p* value is lower than 5% for all analysed variables, the results are statistically significant. **Resulted model:** *Accommodation and food services = (-5.2310) + Crimeware * 2.0972 + Payment Card Skimming * 1.8056 + Point of Sale * 4.7086 + Privilege Misuse * 1.4227 + External Customer * 1.5356 + External Fraud Detection * 2.61.*
	Pattern	Crimeware	2.10	0.46	20.83	<.0001	
	Pattern	Payment card skimming	1.81	0.52	11.83	0.0006	
	Pattern	Point of Sale	4.71	0.47	100.16	<.0001	
	Pattern	Privilege Misuse	1.42	0.29	23.71	<.0001	
	Discovery method	Customer	1.54	0.34	20.76	<.0001	
	Discovery method	External Fraud detection services	2.61	0.43	36.69	<.0001	
Administration and waste management	N/A	Intercept	-3.78	0.11	1220.34	<.0001	As the confidence level was established to 95% and the p value is lower than 5% for all analysed variables, the results are statistically significant. **Resulted model:** *Administration and waste management = (-3.7802) + Partner * 0.7850 + Carelessness * (-1.4391) + External Fraud Detection * 1.7233 + Internal Infrastructure team * 3.09.*
	Actor	Partner	0.79	0.38	4.32	0.0377	
	Root cause	Carelessness	-1.44	0.51	7.88	0.005	
	Discovery method	External Fraud detection services	1.72	0.45	14.85	0.0001	
	Discovery method	Infrastructure team	3.09	1.23	6.31	0.012	
Educational services	N/A	Intercept	-2.62	0.08	1073.88	<.0001	As the confidence level was established to 95% and the p value is lower than 5% for all analysed variables, the results are statistically significant.
	Pattern	Cyber espionage	-2.74	1.01	7.45	0.0064	

Business sector	Category	Parameter	Estimate	Standard Error	Wald: Chi-Square	Pr > Chi Sq	Interpretation
	Pattern	Privilege Misuse	-1.27	0.24	27.65	<.0001	**Resulted model:** *Educational Services = (-2.6249) +Cyber Espionage * (-2.7439) + Privilege Misuse * -1.2687 + Internal staff * 0.4113 + Carelessness * (-2.2019) + IT Review * 1.5569.*
	Actor	Internal staff	0.41	0.15	7.30	0.0069	
	Root cause	Carelessness	-2.20	0.38	34.17	<.0001	
	Discovery method	IT review	1.56	0.52	9.08	0.0026	
Health and social assistance	N/A	Intercept	-1.65	0.07	590.16	<.0001	As the confidence level was established to 95% and the p value is lower than 5% for all analysed variables, the results are statistically significant. **Resulted model:** *Health and social assistance = (-1.6529) + Cyber Espionage * (-3.6982) + Denial Of Service * -2.4580 + Lost And Stolen Assets * 1.7518 + Privilege Misuse * 0.2923 + Web Applications * (-1.9329) + Carelessness * (-0.9427).*
	Pattern	Cyber espionage	-3.70	1.00	13.56	0.0002	
	Pattern	Denial of Service	-2.46	0.72	11.78	0.0006	
	Pattern	Lost and stolen assets	1.75	0.09	365.51	<.0001	
	Pattern	Privilege Misuse	0.29	0.11	6.96	0.0083	
	Pattern	Web application	-1.93	0.26	57.41	<.0001	
	Root cause	Carelessness	-0.94	0.13	51.00	<.0001	
Finance and insurance	N/A	Intercept	-1.48	0.15	103.33	<.0001	As the confidence level was established to 95% and the p value is lower than 5% for all analysed variables, the results are statistically significant. **Resulted model:** *Finance and insurance = (-1.4819) + Cyber Espionage * (-3.2751) + Lost And Stolen Assets * (-0.3645) + Payment Card Skimming * 1.7492 + External * -0.5871 + Internal * (-0.9125) + Carelessness * (-1.1455) + Actor Disclosure * (-0.9674) + Customer * 0.6067 +Internal Fraud Detection * 1.7175.*
	Pattern	Cyber espionage	-3.28	1.01	10.59	0.0011	
	Pattern	Lost and stolen assets	-0.36	0.14	6.35	0.0117	
	Pattern	Payment card skimming	1.75	0.24	54.59	<.0001	
	Actor	External	-0.59	0.16	13.03	0.0003	
	Actor	Internal staff	-0.91	0.17	30.16	<.0001	
	Root cause	Carelessness	-1.15	0.24	21.99	<.0001	
	Discovery method	Actor disclosure	-0.97	0.23	16.98	<.0001	
	Discovery method	Customer	0.61	0.18	11.55	0.0007	
	Discovery method	Internals fraud detection team	1.72	0.74	5.45	0.0196	
Information	N/A	Intercept	-3.56	0.14	691.02	<.0001	As the confidence level was established to 95% and the p value is lower than 5% for all analysed variables, the results are statistically significant. **Resulted model:** *Information = (-3.5649_ + Denial Of Service * 1.0130 + Lost And Stolen Assets * (-2.2984) + Web Applications * 0.8010 + External * 1.6580.*
	Pattern	Denial of Service	1.01	0.22	21.62	<.0001	
	Pattern	Lost and stolen assets	-2.30	0.32	53.15	<.0001	
	Pattern	Web application	0.80	0.13	38.13	<.0001	
	Actor	External	1.66	0.16	104.51	<.0001	
Public administration	N/A	Intercept	-1.76	0.07	635.46	<.0001	As the confidence level was established to 95% and the p value is lower than 5% for all analysed variables, the results are statistically significant. **Resulted model:** *Public Administration = (-1.7626) + Lost And Stolen Assets * (-0.5695) + Internal * 1.4133 + Carelessness * 2.0112 + Actor Disclosure * 0.7020 + Customer * (-0.8052) + Suspicious Traffic Monitoring.*
	Pattern	Lost and stolen assets	-0.57	0.11	28.30	<.0001	
	Actor	Internal staff	1.41	0.08	283.40	<.0001	
	Root cause	Carelessness	2.01	0.11	327.21	<.0001	
	Discovery method	Actor disclosure	0.70	0.12	33.25	<.0001	
	Discovery method	Customer	-0.81	0.18	19.50	<.0001	
	Discovery method	Suspicious traffic monitoring	3.48	0.24	215.46	<.0001	
Retail trade	N/A	Intercept	-3.54	0.14	652.85	<.0001	As the confidence level was established to 95% and the p value is lower than 5% for all analysed variables, the results are statistically significant. **Resulted model:**
	Pattern	Crimeware	1.44	0.34	17.60	<.0001	
	Pattern	Payment card skimming	2.46	0.29	73.99	<.0001	
	Pattern	Point of Sale	2.70	0.44	37.09	<.0001	

Business sector	Category	Parameter	Estimate	Standard Error	Wald: Chi-Square	Pr > Chi Sq	Interpretation
	Pattern	Privilege Misuse	1.01	0.32	10.13	0.0015	*Retail trade = (-3.5387) + Crimeware * 1.4378 + Payment Card Skimming * 2.4608 + Point Of Sale * 2.7010 + Privilege Misuse * 1.0068 + Web Application * 1.5008 + Internal * (-1.2738) + Random Error * 2.6461 + Actor Disclosure * (-2.0562) + Fraud Detection * 1.5508.*
	Pattern	Web application	1.50	0.22	46.09	<.0001	
	Actor	Internal staff	-1.27	0.29	19.89	<.0001	
	Root cause	Random error	2.65	0.83	10.21	0.0014	
	Discovery method	Actor disclosure	-2.06	0.44	21.87	<.0001	
	Discovery method	External Fraud detection services	1.55	0.37	17.99	<.0001	

IV. Main results and recommendations

A different model resulted for each business sector. Therefore, each of them was separately analysed.

A. Accommodation and food services

Results showed that payment card skimming is the most likely type of attack deployed, with a probability of over 88%. On the other hand, privilege misuse is fairly unlikely to occur, with a probability of 9.34%.

Therefore, the focus of accommodation and food services companies should be on protecting their customers' data from both external and internal attackers. For example, restaurants could avoid card skimming from staff through enforcing a customer personal payment policy, through which the customer's card is not passed to the waiter/server, but the payment procedure is performed by the customer itself. Also, close monitoring of the payment devices (e.g. Point-of-Sale devices) is required to ensure the security and authenticity of devices.

At the same time, keeping staff and customers aware of this specific risk and encouraging them to inform the relevant team in case any suspicious activity/devices are spotted could also help increase the security of payment devices and processes.

B. Finance and insurance

As for other industries using card payments, finance and insurance companies are often victims of payment skimming attacks, with a probability of over 87% for the attack to be spotted by the internal fraud detection service. However, the attack is unlikely to be deployed internally, but most likely performed by external attackers using the ATMs. Closely monitoring the ATMs and increasing customers' awareness in terms of card skimming risks may help increase the security of payment card operations, the privacy and protection of customer data.

As this comes with a cost, incentives may be required to make companies' decision factors improve the security of their processes and used devices. For example, placing responsibility and liability for customer-related fraud and theft on the company, which would thus suffer financial penalties, will change the way risks are perceived by the decision factors, and thus support increasing investments in the security controls.

C. Retail trade

Results showed that if an attack targeted a Retail company, it would be deployed on the Point of sales with a probability greater than 90%. Although this may also include card skimming, the mostly used procedure is through POS malware. Also known as memory-scraping malware, it takes the form of a piece of software designed to search the machine's memory for card data, and store it into a dedicated location from which the attacker can easily retrieve it. The malware takes advantage of the fact that data is only encrypted during authorisation process, but not during the card swiping/reading procedure.

Retail companies may reduce this risk through the implementation of more advanced and secure systems, such as EMV technology. While the magnetic-stripe cards are easily duplicable once data is obtained, an EMV card generates a unique transaction code each time it is used, thus its duplication would be useless as the same code could not be used twice.

Part of the solution is also in the hands of the payment systems producers, who should permanently strive to ensure advanced and secure technologies are deployed, as well as in the hands of customers, who should keep pace with the latest trends in terms of secure payments.

D. Public sector

Although no single pattern is predominantly deployed on the public sector organisations (Public Administration, Educational services, Health and social assistance, Administrative and waste management), results show that the most likely root-cause is carelessness of internal staff, with a probability greater than 80%. Therefore, a series of recommendations may be raised in order to address this issue.

Firstly, each organisation should have clearly documented policies regarding the information security. These could include, but not limit to: the use the software and hardware, internet and email, password management, data privacy and protection, etc.

On the same note, all staff should be aware of the policies and procedures in place, and should formally sign-off their commitment to respecting the organisation's values, processes and policies. Adequate measures should be taken in case of data security breaches.

Lastly, resources should be invested in the continuous awareness and training sessions addressing to all staff, in order

to ensure an adequate level of understanding and commitment to the organisation's policies and values.

V. General level recommendations

Although the study shows a clear distinction over the main risks and security breaches each business sector faces, security is not solely a matter of controls implementation. Authors believe that there are certain steps that could help improve the general level of security, regardless of the organisations' business sector.

A. Risk management framework

One essential step in ensuring information security is the implementation and maintenance of a risk management framework. NIST SP 800-39, Managing Information Security Risk, defines risk management as "the program and supporting processes to manage information security risk to organizational operations (including mission, functions, and reputation), organizational assets, individuals, other organizations, and the Nation".[11]

One framework companies could adopt is the NIST model for risk management, described in NIST special publication 800-37 Revision 1, Guide for Applying the Risk Management Framework to Federal Information Systems: a Security Life Cycle Approach. The framework designs the risk management process based on a 6 steps approach, as below: [12]

- Classify information systems;
- Select security controls to be implemented;
- Implement security controls;
- Assess security controls;
- Authorise information systems;
- Monitor security controls.

Risk identification and assessment is the first step towards improving the information security. However, if the process is a one-time activity, the changing risks of the dynamic and rapidly developing technological environment may determine organisations to ignore critical risks or overinvest in risks not worth addressing. Therefore, each entity needs to perform regular review of its risk assessment, in order to identify all new arising risks and update the understanding and weight of previously known risks. The frequency may vary from monthly to annually, depending on the entity's resources, dependency of information technology, risk profile and level and nature of changes.

B. Standards and legislation

The previous sections showed how standards and legislation are not always successfully managing to stay aligned to the rapid technological development. One practical example is Amazon, who suffered major security incidents in the recent years although it was SAS 70 certified. [13] One other example is outlined by Scott J. Shackelford (2014), who describes the international law supporting the information technology as often proving to be "ambiguous and nonbinding". [14] Authors believe that a joint effort between authorities (at national and EU level) and IT and security professionals will support the alignment of standards and legislations with the technological progress, thus supporting the secure use of information systems.

C. Incentives for information sharing

Understanding the threat is the first step towards facing the risk. The fact that the data analysis supporting this research allowed authors to define patterns and correlations between attacks characteristics and targeted business sectors outlines how useful information sharing can be. However, the experience only shows how reticent organisations are in sharing sensitive information. As P. W. Singer and A. Friedman state in their book, Cyber security and cyber war – what everyone needs to know, that most organisations would never risk affecting their reputation by publicly admitting their information security was breached, which could affect their reputation and customers' trust. [3]

One example of such incentive is HITECH Act, which requires organisations falling under the Health Insurance Portability and Accountability Act of 1996 (HIPPA) to report any data breach that affects at least 500 persons to the affected individuals, media channels and to the United States Department of Health and Human Services. [15]

Incentives do not necessarily have to take the form of legislative requirements, but can also be dictated, for example, from customers. P. W. Singer and A. Friedman give the example of Mandiant, who was the first company to publish the analysis of security breaches detected at its clients. Although the act was then considered outrageous and expected to generate a drop in the company's credibility among potential customers, the entity's reputation actually boosted, and in the following years many companies used its example as a marketing practice. [3]

D. General awareness

As previously mentioned, companies' perspective of cyber-security is a matter of cost and benefit. As long as the cost to address the risk is higher than the benefits control implementation would bring, most organisations will decide to ignore the risk. Thus, authors believe that a change in the perspective is required in order for actions to be taken. For example, if the information security would be the subject of customer requirements (e.g. individual customers or business partners would include the security controls as a mandatory requirement for the business relationship to develop), the organisations' investment in security would increase as a normal reaction to the market demand.

However, that requires a general level of awareness. Regarding the current level of individual awareness, M. Uma and G. Padmavathi (2013) point out a lack of knowledge regarding cyber-attacks, risks and threats. [16] This aspect is crucial not only in developing security requirements, but also in ensuring the individual cyber-hygiene. For example, if all individual users of the internet would be trained in security measures, the theft of credentials, personal data and even more complex cyber-attacks (for example botnet attacks, in which

the attacker takes control of multiple individual workstations and uses them to achieve a greater goal even without the consent of the compromised devices' owners) would significantly drop in number and impact.

In recent years, more and more initiatives to increase public awareness have been developed. In UK, the government launched in 2014 a National Cyber Security campaign entitled "Cyber Streetwise", providing security advice every technology user should take for ensuring a basic level of security. [17]

Future research will focus on supporting the increase of general awareness in terms of the threats that the cyber-world brings along for both organisations and individuals, aiming to increase the understanding of cyber-risks, attacks that could be deployed and how to ensure the confidentiality, integrity and availability of information are not compromised.

REFERENCES

[1] [1] Lawrence A. Gordon, Martin P. Loeb, William Lucyshyn, Lei Zhou (2015), Externalities and the Magnitude of Cyber security Underinvestment by Private Sector Firms: A Modification of the Gordon-Loeb Model, Journal of Information Security, Vol.06 No.01(2015), Article ID:52952, available online at: http://file.scirp.org/Html/3-7800247_52952.htm, accessed 25 September 2015.

[2] [2] Hausken, K. (2007) Information Sharing among Firms and Cyber Attacks, Journal of Accounting and Public Policy, 26, 639-688. http://dx.doi.org/10.1016/j.jaccpubpol.2007.10.001 (accessed 24 June 2015).

[3] [3] Singer, P. W. and Friedman, A. (2014). Cyber security and cyber war – what everyone needs to know. Oxford University, 35-197.

[4] [4] Gordon, L.A., Loeb, M.P. and Sohail, T. (2010) Market Value of Voluntary Disclosures Concerning Information Security. MIS Quarterly, 34, pp. 567-594.

[5] [5] William Pelgrin (2014), book chapter – A model for positive change: influencing positive change in cyber security strategy, human factor, and leadership, Best practices in computer network defense: incident detection and response, IOS Press, ISBN 978-1-61499-371-8, pp. 107-110.

[6] [6] Steve Purser (2014),book chapter – Standards for Cyber Security ,Best practices in computer network defense: incident detection and response, IOS Press, ISBN 978-1-61499-371-8, pp. 97-106.

[7] [7] Data Protection Act 1998 (2015), available online at: http://www.legislation.gov.uk/ukpga/1998/29/data.pdf, (accessed on 15 September 2015).

[8] [8] European Network and Information Security Agency (ENISA) (2012), National Cyber Security Strategies – Practical Guide on Development and Execution, available online at: https://www.enisa.europa.eu/activities/Resilience-and-CIIP/national-cyber-security-strategies-ncsss, (accessed on 12 September 2015).

[9] [9] Bendovschi, A., Tinca, A., Ionescu, B., Plescan, D. (2014), Cloud computing – enabling drivers and adoption issues, Proceedings of the 9th International Conference Accounting and Management Information Systems AMIS 2014, ASE, ISSN 2247-6245, pp. 264-265.

[10] [10] Hastie, T., Tibshirani, R. and Frienman, J. (2008), The Elements of Statistical Learning: Data Mining, Inference, and Prediction, Springer, pp. 115 – 128.

[11] [11] Dempsey, K., Witte, G., Rike, D. (2014), Summary of NIST SP 800-53 Revision 4, Security and Privacy Controls for Federal Information systems and Organizations, National Institute of Standards and Technology, US Department of Commerce, available online at: http://csrc.nist.gov/publications/nistpubs/800-53-rev4/sp800-53r4_summary.pdf, (accessed on 28 July 2015).

[12] [12] NIST (National Institute of Standards and Technology), US Department of Commerce (2008), NIST Special Publication 800-53A – Guide for Assessing the Security Controls in Federal Information Systems, pp.13-26.

[13] [13] Bendovschi, A., Ionescu, B. (2015), The Gap between Cloud Computing Technology and the Audit and Information Security Supporting Standards and Regulations, Audit financiar, XIII, Nr. 5(125)/2015, ISSN: 1583-5812, pp. 115-121.

[14] [14] Scott J. Shackelford (2014), Managing cyber attacks in international law, business and relationships, Cambridge University Press, ISBN: 978-1-107-00437-5, pp. 5-10.

[15] [15] Health Information Technology for Economic and Clinical Health (HITECH) Act of 2009,available online at: https://www.healthit.gov/sites/default/files/hitech_act_excerpt_from_arra_with_index.pdf (accessed 19 December 2015).

[16] [16] Uma, M., Padmavathi, G. (2013) A survey on various cyber-attacks and their classification, International Journal of Network Security, 15, 5, pp. 390-396.

[17] Cyber Streetwise official website, available online at: https://www.cyberstreetwise.com/, (accessed on 28 September 2015).