ISSN: 0976-3031

*Available Online at http://www.recentscientific.com*

**CODEN: IJRSFP (USA)**

*International Journal of Recent Scientific Research*
*Vol. 9, Issue, 5(I), pp. 27101-27107, May, 2018*

**International Journal of Recent Scientific Research**

**DOI: 10.24327/IJRSR**

**Research Article**

# THE IMPORTANCE OF WELL-PREPARED CYBER RISK INSURANCE AND OPEN SOURCE INTELLIGENCE (OSINT)

**Baris CELIKTAS[1]*., Mevlut Serkan TOK[2] and Nafiz UNLU[3]**

[1]Applied Informatics Department, Institute of Informatics, ITU, Istanbul, Turkey
[2]Cyber Security Department, Institute of Engineering and Science, TOBB ETU, Ankara, Turkey
[3]Cyber Security Engineering and Cryptography Department, Institute of Informatics, ITU, Istanbul, Turkey

**DOI: http://dx.doi.org/10.24327/ijrsr.2018.0905.2188**

**ARTICLE INFO**

***Article History:***
Received 24th February, 2018
Received in revised form 19th March, 2018
Accepted 16th April, 2018
Published online 28th May, 2018

***Key Words:***
Cyber Threat, Transfer of Risk, Risk Removal, Cyber Risk Score, Cyber Risk Insurance

**ABSTRACT**

In recent years, as a result of increased internet dependence, individuals and organizations are exposed to much more cyber attacks. A provision of internet security has become important for individuals, organizations, and even states. Transfer of risk which is one of the approaches to the risk removal phase based on a licensed insurance company takes risks under the scope of cyber risk insurance for a certain fee. Through cyber risk insurance, risk evaluation and management processes can be performed with predictable and regular payments instead of financial losses and uncertain cyber threats. In this study, it will be focused on why the cyber risk insurance should be done and its importance. For insurance companies, the calculation of the cyber risk score of organization or individual is very important for determining the criteria and value of the policy to be signed. The insurance company, who will calculate the risk score, makes an accurate calculation by using the open source intelligence method and vulnerability analysis. The cyber risk score should be checked by repeating these processes at regular intervals after the signing of the policy by calculating the cyber risk score and corrective measures should be taken if necessary. As an example, the contents of individual cyber risk insurance policies of three international insurance companies have been presented and the differences among these companies have been evaluated. As a result, we consider that this study will be a guide for future academic studies on cyber risk insurance and score.



## INTRODUCTION

The internet which has developed rapidly since the early 1990s has become an indispensable element for human beings with the concept of the "Internet of Things". According to statistical data, 8 billion machines have communicated on the internet in 2017, it is predicted that this number will be 20 billion by 2020 (Gartner, 2017). Namely, almost all machines will be in constant communication with each other in the future.

Internet, information and communication technologies that irreversibly affect people's lives have also affected the means of governing the states. Increased internet dependence, information and communication technologies in the critical infrastructure sectors such as healthcare, transportation, energy, communications, agriculture and food, water management and dams, banking and finance, production facilities, culture, and tourism make these sectors the target of cyber threats (Celiktas *et al*, 2018). This has led governments to include the topics of developing defense mechanisms against cyber threats and taking an active role in cyberspace in their survival measures.

The internet, which is effectively used by individuals, organizations, and governments, becomes a part of economic activities, and so providing security, confidentiality, integrity, accessibility of the data which has personal and commercial value is very important. Because too much data is used, it is necessary to store and preserve them safely in storage devices (Bayraktar, 2015).

Online shopping and the volume of money transfer have also increased substantially in recent years. When the global e-commerce sector is considered to be around 3 trillion dollars, a sector where such a large amount of money is circulated also make attacker's mouths water (Statista, 2017).

In recent years, there has been an increase in the number of cyber threats to individuals and organizations, and as a result, an increase in material and reputational losses have occurred.

**Corresponding author:* **Baris CELIKTAS**
Applied Informatics Department, Institute of Informatics, ITU, Istanbul, Turkey

Individuals with low levels of education and awareness, carelessness and insensitivity, lack of necessary cybersecurity measures, especially small-scale organizations, are at much greater risk in cybersecurity. Large-scale organizations are at lesser risk due to their large budgets and more professional teams that take the necessary precautions. But the loss of material and reputation will be much higher when the organization is exposed to cyber threats as the scale of organizations grows compared to small-scale organizations.

Individuals, on the other hand, are particularly vulnerable to a wide variety of cyber frauds such as phone frauds, online frauds in online shopping, credit cards, identity card theft, demanding ransom etc.

Thus, cybersecurity, cyber risk, risk management, and risk removal should be considered under a wider coverage from large-scale organizations to individuals. In particular, sophisticated risk management and risk removal processes should reduce financial and reputational losses. One of the most important approaches in the risk removal phase is the transfer of risk and one of the most important options of the risk transfer approach is to have cyber risk insurance. Cyber risk insurance should be considered within a wide range of large-scale organizations to individuals.

Against cyber threats that have a negative impact on information and communication infrastructures, insurance companies are preparing cyber risk insurance packages that will minimize the effects of cyber attacks so that threats no longer cause a problem for organizations and individuals and thereby contribute to risk management process.

In this study, it will be focused on cyber threats and risks, the risk removal approaches, cyber threats to organizations and individuals, and the importance of cyber risk insurance. We will also outline what should be taken into consideration when taking out cyber risk insurance and how to determine the cyber risk score.

***Cyber Threats and Risks***

Cyber threats are events or conditions that are likely to cause harm if they occur. Cyber risk is the possibility of harm to institutions, organizations or individuals as a result of cyber threats occurred during processing and transmission of data (CRO Forum, 2014). As a result of constantly increasing cyber threats in cyberspace, the possibility of cybercrime risks is also increasing linearly with the development of the internet and information communication technologies.

At the beginning, non-profit motivated, done solely for fun or challenge, but with the increasing popularity of e-commerce, the rapid increase in the need for employees to access corporate data, ease of use, seeing cyberspace as a fifth battlefield area and using it for own interests and benefits, has resulted in cyber threats becoming more complex and destructive (Hallam-Baker, 2008).

In 2017, out of the 3.1 billion people in 20 countries, 1.8 billion are online, and 978 million have experienced cybercrime. As a result of these cybercrimes, 172 billion USD (average 142 USD per capita) financial losses have occurred (Symantec, 2018).

***Risk Removal Approaches***

For individuals and organizations, there are four basic approaches to risk removal stage in risk management process. These are avoidance of risk, risk acceptance, risk mitigation and transfer of risk (Majuca *et al*, 2006).

In the avoidance of risk approach, zero or minimal level of interaction with information communication technologies is taken as a basis in order to avoid exposure to cyber threats (Borghesi *et al*, 2013). Although this is a viable option for some individuals, today it is almost impossible to give up the benefits provided by information and communication technologies.

In the risk acceptance approach, bearing in mind the loss arising from the realization of the risk, and as a result of the cost analysis to be carried out during the risk management process, risks are accepted without undertaking risk precautions (Crouhy *et al*, 2006).

The approach in risk mitigation is based on the reduction of the possibility of the risk with the help of various technical and administrative processes. Investing in people and devices and constantly evolving security measures are some of them (Wheeler, 2011).

The transfer of risk, based on a licensed insurance company takes risks under the scope of cyber risk insurance for a certain fee is the last approach to risk removal stage.

With cyber risk insurance, individuals and organizations can carry out risk management processes with predictable and regular payments instead of financial losses and uncertain cyber threats (Romanosky *et al*., 2017).

***Cyber Threats to Organizations and Individuals***

Due to the increasing use of the Internet, a high increase in cyber threats has taken place towards organizations and individuals.

Cyber threats to organizations are divided into two groups according to the source of the attack: insider and outsider attacks (Kumar *et al*, 2005). Samples of insider cyber threats are financial fraud performed by employees of the organization; data theft; attacks on data integrity and identity theft. Outsider cyber threats are theft of money or trade secrets; rendering information systems unserviceable by rival organizations; weaknesses against network fluctuations and power failures (Brockett *et al*, 2012).

As a result of these cyber threats, organizations, aside from experiencing high levels of material loss, also occur a loss of reputation in the sector they are in. Loss of reputation also involves a great deal of importance in the critical infrastructure sectors, especially in banking and finance.

Many people consider that they will not be a cybercrime target. They also do not realize that the machines used in cyberspace can be used as means for carrying out cybercrime. In general, individuals also consider that people over a certain age with little ability to use technology are more desirable targets for cyber attackers (James *et al*., 2013), (H.M. Government, 2016). However, studies in the UK have shown that the probability of a cybercrime target of persons 75 years old or over is less than all other age groups, and an individual's chances of being a

cybercrime target is 11 times higher than the probability of extortion (UK Office for National Statistics, 2017), (Department for Culture, Media, and Sport, 2017). Thus, individuals have to take the necessary security precautions to protect their personal information and devices against cyber threats (Marsh & McLennan Co., 2018).

The cyber threats that individuals exposed can be summed up in two categories. These are threats originating from privacy breach and traditional network-based threats (Gharibi *et al*, 2012). Threats originating from privacy breach encompasses obtaining the individuals birth date, home address, telephone number etc., obtaining sensitive information and the use of social engineering techniques by malevolent people to benefit (Best *et al*, 2017). Traditional network-based threats target users and stored data. This category includes spam e-mails, phishing, fraud, identity theft and harmful attacks as well as attacks on personal rights through social engineering techniques, cyberbullying, and insults (Mishra *et al*, 2015).

***Cyber Risk Insurance and Its Importance***

Recommendations on the use of cyber risk insurance to provide Internet security took place in 1994 (Lai *et al*, 1994). In 1997, Steve Haase, employed at a US-based insurance company, wrote the first cyber policy, even if it was a simple third-party liability policy (Wells, 2018). The risk management approach, especially used in the financial sector, could also be used for internet based risks was first voiced by Dan Geer in 1998. (Geer, 1998). In 2001, Bruce Schneier turned the concept of cyber insurance into an academic debate, and the basic outline accepted currently in the risk management of cyber security was outlined by him (Schneier, 2001).

Although the history of academic studies on cyber risk insurance has been in existence for twenty years, cyber insurance products still have not reached the level of other insurance products. It has been found that 25% of companies in Europe are not even aware of the existence of such insurance, and only 10% have purchased a cyber risk insurance policy (Tøndel *et al*, 2015). Nevertheless, it is predicted that global cyber risk insurance market will reach 5 billion USD by the end of 2018 and 7.7 billion USD by 2020 (PwC, 2015).

Raising awareness and taking technical measures for organization and individuals against cyber risk will significantly reduce the risks encountered, but will never provide full protection. Moreover, small organizations often do not have the large budgets to invest in high-cost security devices such as next-generation firewalls; intrusion detection and prevention systems, and email security solutions. At this point, the importance of cyber risk insurance for small organizations emerges.

Why is cyber risk insurance important for organizations? The answer to the question is explained below.

- Data are among our most important assets and results in financial losses if it is stolen or lost.
- Information and communication technologies are critical in daily operations. The interruption of the system will cause a lot of financial loss.
- The obligation to protect data of third parties is stipulated in laws and if they are lost or stolen, are exposed to serious penal and punitive sanctions.
- All of these cyber attacks which are occurred lead to material losses as well as the loss of reputation of the organization in the sector (Sloan, 2017).

Why is cyber risk insurance important for individuals? In order to answer this question, it is necessary to know the moral losses, as well as the financial losses resulting from the threats are generated by cyber threats. The moral losses that individuals exposed are listed below.

- Psychological breakdown and embarrassment.
- Spending time to make exploited or damaged equipment operational.
- Spending time to reach financial institutions like banks etc.
- Spending time in reporting the cybercrime occurred to law enforcement officers.
- Loss of personal and sensitive data such as videos, photos.
- Spending time to warn other individuals to be careful.
- Exposure to the effects of blackmail, threat or extortion (Home Office, 2018).

The psychological and reputational losses mentioned above sometimes overtake financial losses and can cause very damaging consequences for the individual. The financial loss caused by cyber attacks to organizations and individuals can be quite high, and a loss of brand value can negatively affect the organization's revenues for many years, and excessive resources may need to be spent to repair it.

Although organizations and individuals have taken a number of measures to ensure safety in cyberspace, they can still be affected by cyber threats. When they are affected by these cyber threats, there is a cyber risk insurance to cover permanent damages. The resulting risk will be transferred to the cyber risk insurance and the financial and moral losses mentioned above will be totally or partially acceptable.

***Measuring Cyber Risk Score and Its Importance***

Cyber risk insurance companies are the main starting point for the preparation of policies in which customers understand their cybersecurity situation. Cyber risk scores are generated after completing a long checklist by the experts; the security devices used, applications; the penetration test report done for the organizations and sharing these results with the insurance company. Fees are also charged considering the cyber risk score. However, today the rapid development of the information and communication industry and the constant change of the security situation of organizations prove that this detection method is no longer usable. For example, the weakness and vulnerability of a new device added to the network infrastructure can make the entire system insecure.

Surveillance data should be used consistently when measuring the cyber risk scores of organizations and individuals. This will allow the customer to evaluate the cybersecurity situation in real time.

Where the ecosystems of the organizations are considered to have a constantly changing dynamic structure, a system that has weaknesses within a certain period during a year, may not be vulnerable in other time periods. In addition, taking measures to ensure the security of the organization's internal

network and web applications is the first measure to be taken, but the measures are not limited to these. There is a lot of confidential information about the organization and the individual on the internet; social media, the dark web, and in other platforms. In summary, there are numerous factors in the internet environment that can threaten your company even if it is not related to your internal network or your web applications. The analysis of how organizations and individuals are seen by the attacker within cyberspace, and the existence of a control mechanism that constantly controls assets, is crucial for organizations and individuals who have cyber risk insurance.

Data such as hacked e-mail addresses, passwords for organization employees, and customer accounts obtained by scanning system has included detrimental information for organization or individual. In addition, fake websites, mobile applications, and other products are being constantly scanned by cyber attackers to deceive customers. This data, which is provided by many different individuals and organizations, is called Open Source Intelligence (OSINT).

As shown in Figure 1, the Cyber Risk Score Calculation Cycle has consisted of three basic phases. As a result of these phases, the cyber risk insurance policy fee should be determined.

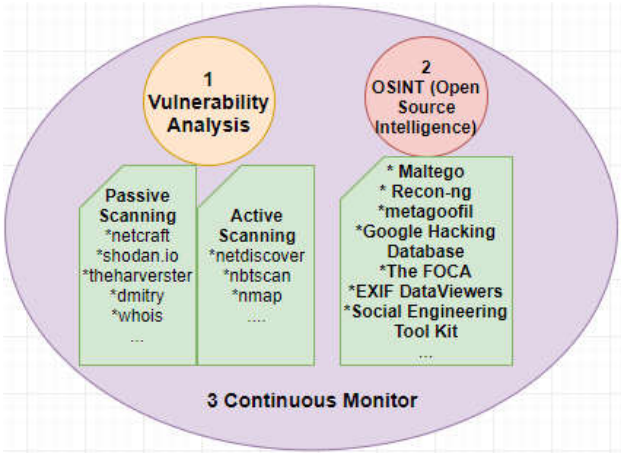


**Figure 1** Cyber Risk Score Calculation Cycle

During the Vulnerability Analysis phase, vulnerabilities of the system should be defined. At this stage, the passive and active scanning methods shown in Figure 1 must be used and information about system vulnerabilities must be obtained. Through this phase, the identified vulnerabilities must be hardened by the cybersecurity team before it is exploited and effort should be exerted to improve the existing system.

The OSINT phase is the basic data source of the Cyber Risk Score Calculation Cycle and some of the data source tools used are shown in Figure 1. The most notable data source tool is Maltego, interface of which is shown in Figure 2. A scoring should be done as a result of analysis made by OSINT tools.

During the Continuous Monitoring phase, a vulnerability analysis to be carried out at a certain frequency, and an assessment of the outcome of the OSINT phase should be conducted where the organization or individual should be continuously consulted in order to improve the cyber risk score. As a result of the Cyber Risk Score Calculation Cycle, a clear and detailed report should be prepared on the cyber risk score of the organization or the individual.

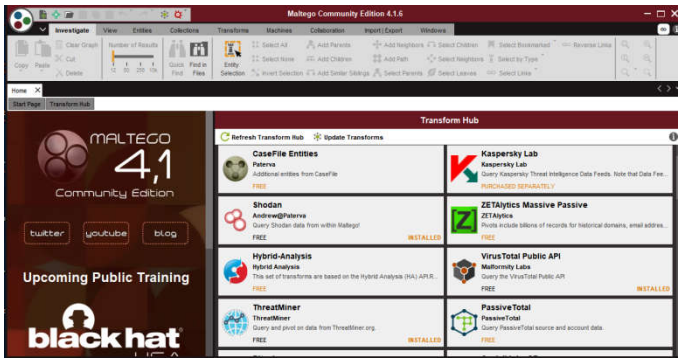


**Figure 2** Maltego OSINT Tool

This report will help identify possible security risks that an organization or an individual may encounter and will assist in taking the necessary steps to mitigate those risks.

Thus, a more accurate cyber risk score and cyber insurance policy fee can be calculated, and as a result of prior notification to organizations and individuals of a cyber attack, the cyber attack and damage will have been prevented and the cyber risk insurance company will not have to pay any fee to victims.

### *Current Individual Cyber Risk Insurance Policy Examples*

In this section, examples of policies provided by three international cyber risk insurance company for the individual will be mentioned.

### *C-1 Insurance Company*

The C-1 insurance company is a large-scale, multinational company with various insurance products. The company provides individual cybersecurity insurance products annually as a package.

Guarantees provided under the policy:

1. Legal Counseling Coverage: In the event of disagreement, a team of lawyers appointed by the insurer shall explain the rights and obligations of the insured.
2. Identity Theft Coverage: Exemptions, non-judicial solutions, and legal solutions are available.
3. Online Reputation Damage Coverage: Solutions for non-judicial and judicial proceedings are available.
4. Online Shopping Disputes Coverage: Solutions for non-judicial disputes and legal proceedings are available.
5. Theft or Fraudulent Usage of Payment Instruments Coverage: Non-judicial solutions, as well as legal proceedings, are available.
6. Personal Password Theft Coverage: Payment is made if the damage is not covered by the relevant bank or the financial institution. Solutions are available on demand and throughout the policy period.

The insured can benefit from each of the mentioned types of coverage once within the policy period. In addition, personal computer technical support services are provided for the insured to solve technical problems they experience in their personal computers. During the policy period, the insured's identification number, bank account number, telephone number, email address etc. and other information determined by the insured is provided with a “continuous monitor” service

on the internet to detect the malicious use of the information provided.

***C-2 Insurance Company***

The C-2 insurance company is a medium-sized company with various insurance products in its internationally active portfolio. The company provides individual cybersecurity insurance products as an annual package.

***Guarantees provided under the policy***

1. Password Protection Coverage is available.
2. Identity Protection Coverage: There are solutions available for annual legal costs, revenue losses and other costs.
3. ATM Snatching Coverage is available.

In addition to the main guarantees, support is provided with the monitoring of safe shopping; transactions and information sharing of identified individual information with the computer, tablet and mobile devices and reporting of suspicious activities as well as complimentary antivirus programming support are available.

***C-3 Insurance Company***

The C-3 insurance company is a large scale international company operating in the USA, Europe, and Asia and has various insurance products in its portfolio. Customers are recommended private, individualized cybersecurity policy that offers low-limit as well as high-limit options in coverage amounts.

***Guarantees provided under the policy***

1. Cyber Sniffing Damage Coverage: There are a normal limit and high limit options for repairing and renewing computer, hardware, and software of the customer and for recovering personal data.
2. Cyber Theft Coverage: In the event, the attacker steals money from the customer's personal account, personal documents or title deed are stolen, there are options for normal limit and high limit payment, including coverage of communication invoices to be issued.
3. Social Engineering Coverage: As a result of a phishing attack, if an account balance is transferred from the personal account of the insurer to the account of the fraudster, there are options for normal limit and high limit payment.
4. Cyber Blackmail Coverage: In the event, cybercrime is followed by a ransom demand from the insured, there are a normal limit and high limit payment options.
5. Cyber Environment Responsibility Coverage: In the event of financial losses resulting from the stealing of the insured's personal account, there are the options of normal limit and high limit payments after cybercriminals are found guilty of infringement of intellectual property rights, computer virus transmission or insulting/ defamatory actions.

The company evaluates its customers according to their own criteria and decides on the basis of the assessment to be made whether the customer will benefit from this insurance product. Company's assessment criteria are cited below:

1. The policy can only be sold to customers who use or will use home and family insurance products of the same company.
2. Customers should not have suffered a loss in the last five years within the scope of this policy.
3. Customers should be aware of the actions and events that will lead to an adverse effect within the scope of this policy.
4. Customers should have updated antivirus software and a firewall to protect their personal computer, laptop, tablet, mobile device and computer network in their home.
5. Customers must update within 90 days their Android, Apple, etc. devices, with an operating system, if an update patch for these devices is released.

With the policy, the insured is provided with a license for a cyber risk assessment and management software developed by expert staff. This software identifies the insured individual's cyber risk score and learns how to improve vulnerability and online safety. Data breaches, including e-mail accounts, are identified with the software and protection of the insured against phishing and guidance on basic computer usage are provided. Cyber victim consultants will be appointed to provide the insured expert opinion and guidance after cyber attacks.

***Assessment of Individual Cyber Risk Insurance Policies***

Basically, C1 and C2 companies:

1. Have an individual cyber insurance product with uniform and standard package contents,
2. The annual cost of the insurance product is at a reasonable and affordable level which corresponds to 8%-9% of the current monthly minimum wage in the countries served,
3. Legal and technical support is available within the scope of the insurance policy,
4. Network monitoring service and antivirus software are provided free of charge under the policy,
5. Identity theft and the stealing of personal passwords have the same coverage with different limit guarantees.

***Compared with the C1 and C2 companies***

1. C3 company addresses a broader customer segment with personal products that have low and high limit options.
2. The guarantees provided by the C3 company are closer to the threats that individuals may be exposed to in cyberspace.
3. The C3 company ensures and makes it compulsory that the customer should comply with the safety criteria of any device to be used in cyberspace.
4. The C3 company provides support to customers in raising cyber security awareness and in realizing personal cyber risk management.
5. The C3 company provides expert opinion and guidance services to customers after they have been exposed to a cyber attack.
6. The C3 company pays customers at higher limits when exposed to a cyber attack.

7. The C3 company makes a pre-insurance risk analysis that is more comprehensive than the other companies and so the insurer determines the personal cyber risk score, learns how to improve vulnerability and online safety and as a result of this process, a cyber risk insurance policy is signed with the customer.

## CONCLUSION

In our study, the policies of three international cyber risk insurance companies have been examined. In order to make cyber risk insurance sector more widespread in the future, the following items have to be included in the content of the cyber risk insurance policies prepared for organizations and individuals.

1. Prior to the signing of the cyber risk insurance policy between the cyber insurance company and the customer, the cyber risk assessment and the customer's risk score developed by experts with the help of OSINT tools, must be calculated and according to this score, the insurance fee must be identified.
2. System vulnerabilities and how online security measures should be taken by the customer must be put forth.
3. Data breaches, including software and e-mail accounts, should be identified.
4. Guidelines should be provided for protection against phishing attacks and basic computer usage instructions should be given to the customer.
5. Within the coverage of the cyber insurance company's cyber risk insurance policy, training should be provided during certain intervals that increase the level of consciousness and awareness of the customer, and, if necessary, an online exam should be carried out as a condition of renewal of the insurance policy.
6. The cyber insurance company must have insurance policies and guarantees with various packages that are appropriate for different organizations and individuals. This will expand the target customer base. These coverages are:
    - Legal Counseling Coverage
    - Identity Theft Coverage
    - Online Reputation Damage Coverage
    - Online Shopping Disputes Coverage
    - Payment Instruments Theft or Fraudulent Usage Coverage
    - Income Loss Coverage
    - Travel and Communication Charges Coverage
    - Social Engineering Coverage
    - ATM Snatching Coverage
    - Personal Password Theft Coverage
    - Ransomware and Malware Coverage
    - Cyber Environment Responsibility Coverage
    - Cyber Sniffing Damage Coverage
7. The insurance company's cyber risk insurance policy must be at a reasonable and affordable level for the organization and individual.
8. The cyber insurance company should be required to provide legal and technical support to the organizations or individuals under the scope of the cyber risk insurance policy.
9. As a part of the cyber risk insurance policy, security measures such as an intrusion detection system, antivirus and firewall for protection of personal computer, laptop, tablet, mobile device and the home computer should be provided free of charge and kept updated.
10. The company should evaluate its customers according to certain criteria and decide on the basis of the assessment to be made as to whether the customer can be benefited from this insurance product.
11. Within the coverage of the cyber risk insurance policy, cyber victim consultants should be appointed to provide customer expert opinion and guidance during or after cyber attacks occurred.
12. Compulsory housing insurance for individuals who will take out cyber risk insurance will provide an integrated security protection by ensuring the physical security of the devices.

## References


Bayraktar G. Cyber Warfare and National Security Strategy. Yeniyüzyıl: İstanbul; 2015: 23-51.

Best DM, Bhatia J, Peterson ES *et al*., Improved Cyber Threat Indicator Sharing by Scoring Privacy

Risk. 2017 [cited 2018 May 05] Available from URL: https://ieeexplore.ieee.org/ document/7943482/

Borghesi A. and Gaudenzi B. Risk Management: How To Assess, Transfer and Communicate Critical Risks. Springer-Verlag: Milan; 2013: 89-91.

Brockett PL., Golden, Ll and Wolman W. "Enterprise Cyber Risk Management". In Emblemsvag J (ed.). Risk Management For The Future- Theory, and Cases. 1st. ed. InTechOpen Ltd: Rijeka; 2012: 319-340.

Celiktas B. and Unlu N. A Research on Cyber Power and Capacities of Various States. The Journal of Academic Social Science Studies. 2018; 67; 469-488.

CRO Forum. The Cyber Risk Challenge and the Role of Insurance [online]. 2014 [cited 2018 Apr 08]. Available from: URL: http://www.thecroforum.org/cyber-resilience-cyber-risk-challenge-role-insurance/

Crouhy M, Galai D, and Mark R. The Essentials of Risk Management. 1st edition. McGraw-Hill: New York; 2006: 83-109.

Department for Culture, Media, and Sport. Cyber Security Breaches Survey 2017 [online]. 2017 [cited 2018 Apr 30]. Available from: URL:https://assets.publishing. service.gov.uk/government/uploads/system/uploads/ attachment_data/file/609186/Cyber_Security_Breaches_ Survey_2017_main_report_ PUBLIC.pdf

Gartner Media Relations, Gartner Says 8.4 Billion Connected "Things" Will Be in Use in 2017, Up 31 Percent From 2016 [online]. 2017 [cited 2018 May 10]. Available from: URL: https://www.gartner.com/newsroom/id/ 3598917

Geer D. Risk Management is Where the Money Is, Talk Before Digital Commerce Society of Boston [online]. 1998 [cited 2018 May 15]. Available from: URL: http://catless.ncl.ac.uk/Risks/20.06.html #subj1

Gharibi W and Shaabi M. Cyber Threats in Social Networking Websites. *International Journal of Distributed and Parallel Systems (IJDPS)*. 2012; 3(1): 119-126.

Hallam-Baker P. Famous for Fifteen Minutes: A History of Hacking Culture [online]. 2008 [cited 2018 May 02]. Available from: URL: http://www.csoonline.com/ article/217058/ famous-for-fifteen-minutes-a-historyof-hacking-culture

Home Office. A Call To Action: The Cyber Aware Perception Gap Report [online]. 2018 [cited 2018 May 04] Available from: URL: https://www.cyberaware. gov.uk/sites/cyberstreetwise/files/ thecyberawareperceptions gapreport.pdf

HM Government. National Cyber Security Strategy 2016-2021 [online]. 2016 [cited 2018 Apr 15]. Available from: URL: https://assets.publishing.service.gov.uk/ government/uploads/system/uploads/attachment_ data/file/567242/national_cyber_security_strategy_ 2016.pdf

James BD, Boyle PA, and Bennett DA. Correlates of Susceptibility to Scams in Older Adults Without Dementia. *Journal of Elder Abuse & Neglect*. 2013; 26(2): 107-122.

Kumar V., Srivastava J. and Lazarevic A." Intrusion Detection: A Survey". In: Kumar V., Srivastava J. and Lazarevic A. (eds.). Managing Cyber Threats: Issues, Approaches, and Challenges. Springer: New York; 2005:19-78.

Lai C, Medvinsky G, Neuman BC. Endorsements, Licensing, and Insurance for Distributed System Services, 2nd ACM Conference on Computer and Communications Security (CCS), 1994.

Majuca RP, Yurcik W and Kesan JP. The Evolution of Cyber insurance [online]. 2006 [cited 2018 Apr 28]. Available from: URL: https://arxiv.org/ftp/cs/papers/0601/ 0601020.pdf

Marsh&McLennan Companies Global Risk Center. MMC Cyber Handbook 2018: Perspectives On The Next Wave Of Center [online]. 2017 [cited 2018 May 03]. Available from: URL: https://www.mmc.com/content/dam/mmc-web/Global-Risk-Center/Files/mmc-cyber-handbook-2018.pdf

Mishra MK, Kumar S, Vaish A, Prakash S, Quantifying Degree of Cyber Bullying Using Level of Information Shared and Associated Trust [online]. 2015 [cited 2018 Apr 22] Available from URL: https://ieeexplore.ieee.org/document/7443773/

Office for National Statistics. Crime Survey for England and Wales [online]. 2017 [cited 2018 Apr 15]. Available from: URL: https://www.ons.gov.uk/peoplepopulation andcommunity/crimeandjustice/datasets/crimeinengland andwalesexperimentaltables

PwC. Cyber insurance market set to reach $7.5 billion by 2020- PwC Report [online]. 2015 [cited 2018 May 18] Available from: URL: https://preview.thenewsmarket. com/Previews/PWC/DocumentAssets/ 400106.pdf

Romanosky S., Ablon L., Kuehn A. and Jones T. (2017). Content Analysis of Cyber Insurance Policies: How do carriers write policies and price cyber risk? [online]. 2017 [cited 2018 May 02]. Available from: URL: https://www.rand.org/pubs/working_papers/WR1208. html

Schneier B. Insurance and the Computer Industry. Communications of the ACM. 2001; 44(3): 114-115.

Sloan R. Cyber Matters: The Importance of Cyber insurance for SMEs. [online]. 2017 [cited 2018 May 10] Available from URL: https://www.cybersecurityjournal.org/cyber-matters-the-importance-of-cyberinsurance-for-smes/

Statista. Retail e-commerce sales worldwide from 2014 to 2021 (in billion U.S. dollars) [online]. 2017 [cited 2018 Apr 12]. Available from: URL: https://www.statista.com /statistics/379046/worldwide-retail-e-commerce-sales/

Symantec. Norton Cyber Security Insights Report Global Results [online]. 2018 [cited 2018 May 18]. Available from: URL: https://www.symantec.com/content/dam/ symantec/docs/about/2017-ncsir-global-results-en.pdf

Tøndel IA, Meland PH, Omerovic A, Gjære EA, Solhaug B. Using Cyber-Insurance as a Risk Management Strategy: Knowledge Gaps and Recommendations for Further Research [online]. 2015 [cited 2018 May 09]. Available from: URL: https://www.sintef.no/en/ publications/publication/ ?pubid=CRIStin+1306136

Wells A. What Agent Who Wrote First Cyber Policy Thinks About Cyber Insurance Now [online] 2018. [cited 2018 Apr 29] Available from URL: https://www. insurancejournal.com/news/national/2018/03/01/ 481886.html

Wheeler E. Security Risk Management: Building an Information Security Risk Management Program from the Ground Up. 1st edition. Elsevier: Amsterdam; 2011; 147-162.

**How to cite this article:**

Baris CELIKTAS *et al*.2018, The Importance of Well-Prepared Cyber Risk Insurance And Open Source Intelligence (Osint). *Int J Recent Sci Res.* 9(5), pp. 27101-27107. DOI: http://dx.doi.org/10.24327/ijrsr.2018.0905.2188

*******