Journal Homepage: - www.journalijar.com

INTERNATIONAL JOURNAL OF ADVANCED RESEARCH (IJAR)

Article DOI: 10.21474/IJAR01/15730
DOI URL: http://dx.doi.org/10.21474/IJAR01/15730

RESEARCH ARTICLE

INFORMATION SECURITY POLICIES AND STRATEGIES AND PRACTICES ADOPTED IN IT: THE IMPORTANCE OF CONSULTANCY IN SMALL AND MEDIUM-SIZED COMPANIES

Gabriel Matheus Da Silva Noronha, Alessandro Andrade Da Silva and Jaqueline Silva De Souza Pinheiro

Manuscript Info

Manuscript History
Received: 20 September 2022
Final Accepted: 24 October 2022
Published: November 2022

Key words:-
Cybersecurity, Information system, Security Strategies

Abstract

Objective: Companies in the cybersecurity consulting market are expanding their services in periodic training to business stakeholders and enforcement of security policies. The objective of this work is to demonstrate the importance of consulting in information security policies aimed at small and medium-sized companies.
Methods: It is characterized as a narrative literature review with a qualitative approach, which does not use explicit and systematic criteria for the search and critical analysis of the selected literature.
Results: Tools needed for cybersecurity include endpoint detection and response (EDR), antivirus software, next-generation firewalls, Domain Name System (DNS) protection, email gateway security, intrusion detection and prevention, logging and log monitoring, endpoint protection, authentication and virtual private network (VPN) services, cloud-based security, web application firewalls (WAFs), software-defined wide area networks (SD-WAN), enterprise password management , privileged access management (GAP), vulnerability and threat management, and threat detection.
Conclusions: In summary, SMBs seem to implement some of the basic cybersecurity measures only as part of their overall IT implementation. However, it appears that unless cybersecurity controls are included as part of an IT solution, many SMBs do not realize the resulting potential risks to their business.

Introduction:-

Living and working in a connected environment has greatly improved business efficiency and accelerated communication. But it also opened the door to lurking threats that can wreak havoc on small and medium-sized businesses unless they are prepared. Chief among these dangers are attacks against your company's infrastructure, including personnel, computers, mobile devices, and networks.

Information security policies (PSIs) play an important role in information security (DHILLON, 2017). They guide end users, i.e., employees and contractors, to specific work tasks or to specific technology, thus defining acceptable procedures that end users must comply with (SIPONEN AND VANCE, 2010). However, information security breaches caused by end users' non-compliance with PSIs are a serious problem (HAYSTAX, 2019; PONEMON, 2020; VERIZON, 2019). These breaches can have dire consequences for organizations, negatively impacting their revenue streams (CISCO, 2018), reputation (SON E KIM, 2009) and trust (CAVUSOGLU et al., 2004).

Corresponding Author:- Gabriel Matheus Da Silva Noronha

Consequently, it is not surprising that end-user non-compliance with PSIs has received significant research attention (CRAM et al., 2017).

Researchers have increased our knowledge of factors that explain end-user non-compliance with PSIs (eg, BULGURCU et al. 2010, IFINEDO 2016, SOMMESTAD et al. 2019). Researchers have also recognized that different rationales (e.g. productivity and quality goals) come into play in relation to information security (KARLSSON et al., 2018). Kirlappos et al. (2013) argue that when the prioritization of different rationales is left to end users, there are risks of breaches in information security. Thus, for information security managers to align information security with organizations' core work practices, they need to understand the competing rationales within their organizations.

Statistically speaking, 85% of cybersecurity breaches are caused by human error (Master's Guide, 2021); 94% of all malware is delivered via email (OSC, 2021); ransomware attacks happen every 10 seconds (INFOSECURITY, 2021); 71% of all cyber attacks are financially motivated, followed by intellectual property theft and espionage (GUIA DO MESTRE, 2021); More than 80% of cybersecurity events involve phishing attacks (OSC, 2021); 42% of all cyberattacks target small businesses; 77% of organizations do not have a response plan (VARONIS, 2021); 20% of small businesses have enabled remote work without having a cybersecurity plan (ALLIANT CIBERSECURITY, 2021); 43% of SMBs have yet to adopt cybersecurity assessment and mitigation plans; 37% of businesses were hit by ransomware in 2020; 32% of companies paid the ransom to recover their data, with an average ransom of $170,404 (GREY, 2022)

Companies in the cybersecurity consulting market are expanding their services in periodic training to business stakeholders and application of security policies , this is because an increasing number of cybersecurity incidents are related to COVID-19. Thus, companies in the cybersecurity consulting market have taken advantage of this opportunity to offer their services to vulnerable companies. On the other hand, the increasing digitization of business is creating future value capture opportunities for market stakeholders.

Therefore, the objective of this work is to demonstrate the importance of consulting on information security policies aimed at small and medium-sized companies . Specifically, it seeks to identify and fill gaps in companies' cybersecurity strategy; show the efficiency of cyber consulting for small and medium-sized companies and; suggest software that can contribute to the information security of small and medium-sized companies.

Cyber Security Strategy In Small And Medium Businesses

The COVID19 crisis has shown the importance of the Internet and computers in general for SMEs to maintain their business. To survive the pandemic and stay in business, many SMBs have had to take business continuity measures such as adopting cloud services, upgrading their internet services, improving their websites and allowing employees to work remotely. This report highlights how many of the existing cybersecurity challenges have been further exasperated by the impact of the COVID19 pandemic and are now more critical to mitigate.

A survey carried out by SEBRAE (2020), 99% of them have more than 7 million businesses spread across the five regions of the federation, which operate in different types of markets, whether services, commerce and industry. This index is also reflected in the generation of employment and income, which provided 541.7 thousand, a number higher than that registered by medium and large companies. They also represent more than half of Brazil's GDP and play a key role in adding value to all sectors of the country's economy. They serve as facilitators of digital transformation and as a central element of Brazil's social fabric (SEBRAE, 2020).

Many companies urged employees to work remotely using online collaboration platforms, e-commerce, e-banking and e-government services were improved, education activities moved to e - learning and its use became part of the reality of many citizens. Additionally, traditional businesses have had to implement changes to avoid contact or crowded places and implement technologies such as QR codes, contactless payments, and direct-to-consumer models such as home delivery, click-and-pick-up services, and remote assistance via chat or phone (ALMEIDA, 2018).

The recent crisis caused by COVID-19 also showed the importance of digitizing processes for maintaining business operations. The promotion and implementation of digitalization across all industries, not just e-commerce, has accelerated and is expanding. SMEs need to adopt business continuity measures and improve online processes and

related infrastructure to ensure their safe operation . They also have the opportunity to join forces within their industry associations and cooperate with partners and collaborators to ensure the cybersecurity of their industries (KAPLAN, 2018).

Criminals are taking advantage of the fear and uncertainty that many citizens have faced because of the pandemic. We are witnessing a sharp increase in malicious emails, phishing attacks , scams and malware related to the COVID-19 crisis. In addition, there is an increase in the number of cyber-attacks targeting specific sectors already under pressure, such as hospitals, healthcare providers and medical research facilities. Criminals are also targeting SMEs, as they are aware that many SMEs now have employees working remotely, have quickly and insecurely deployed systems to continue serving their customers, and many lack adequate cybersecurity defenses (MARTI, 2015).

Small business owners need to adopt a robust cybersecurity system with multifaceted and integrated security solutions (PAN et.al, 2016). Small and medium business owners need a comprehensive security plan that addresses a wide range of vulnerabilities and internet-based attacks. This comprehensive security plan can also be modified to periodically address ever-changing internet-based attacks.

Cybersecurity is a proactive approach that can be used to protect systems, including software, hardware and data, from cyberattacks. From this point of view, cybersecurity is linked to an organization's practices, policies and physical infrastructure. Cyber security is considered a challenge for any organization that must deal with cyber threats (ALBUQUERQUE et al, 2016).

A holistic cybersecurity strategy encompasses preparations and precautions against cyber breaches (CERIC, 2016). Holistic cybersecurity strategies include corrective actions and preventive measures that some small business owners used to protect sensitive company data from cyberattacks. A cybersecurity strategy is an essential technology element that organizations are using to protect their system from an imminent attack. Good cybersecurity practices ensure the integrity, confidentiality and availability of data security, by becoming proactive in cybersecurity issues, small business owners are essentially protecting their organization's security system (ABEL, 2018).

Watad et.al (2018) noted that the adoption of information security tools is not consistent across all small businesses. These are due to inconsistency, lack of awareness of information security, and lack of skills and knowledge needed to select and implement security solutions. These factors have made it difficult for small businesses to implement a consistent and proactive cybersecurity strategy.

Information security strategies must be able to deal with the continuous growth of threats and risks. However, to be effective, small business owners must align strategies closely with business goals. Entrepreneurs need to determine the vulnerability level of the system and develop an appropriate holistic plan to deal with vulnerabilities. Some small business owners have incorporated holistic strategies that can detect, protect, and respond to today's cyberattack issues (JONES, 2017).

The holistic approach incorporates human, technical and physical factors relevant to detecting, preventing and correcting current cybersecurity vulnerabilities (BREGAR, 2017). Entrepreneurs can defend against cybersecurity by installing security systems, security awareness, education, employee training, and intrusion detection to prevent targeted attacks. Some small business owners have installed computer protection like firewalls , antivirus, intrusion detection systems, two-factor authentication, phishing filters and many other security products to combat internet-based attacks (HUANG et.al, 2018).

Firewalls are a vital strategy for small business network security as they are a set of related layers against threats and prevent outsiders from accessing data on the corporate network. Internal firewalls are being used to strengthen the computer system by some entrepreneurs and can also be used to prevent pop-ups, cookies, malware and email viruses from infecting the business network (ALMEIDA et al., 2018).

As cybersecurity is a complex issue related to technical solutions and measures, it is often perceived as only concerning IT people. This, however, is not the case. Cybersecurity must be part of the organization's culture. Every person should have at least a basic awareness of cybersecurity and how their attitude can affect the cybersecurity posture across an organization. What is really needed is a transition from initial awareness to internal cybersecurity

culture. For example, workers must know and understand how spear attacks work.phishing and social engineering, rules for using your own devices to access the company's ICT environment and other basic cybersecurity precautionary measures (ALBUQUERQUE, 2016).

Not having a specific backup policy, endpoint anti - malware solutionimplemented on all types of devices and kept up-to-date, using obsolete or just unpatched software that doesn't auto-update, can seriously compromise the company's critical and confidential information, making the small business an easy target for cyber-attacks. With that in mind, the next section discusses how information security consulting can be effective in preventing cyber threats.

Efficiency Of Cyber Consulting For Small And Medium Businesses

Cybersecurity is a specialist topic, requiring specialized knowledge, however it is quite common in an SME for individuals to be multitaskers and may have multiple roles assigned to them. As a result, an SME employee may be responsible for cybersecurity as well as other processes. Ideally, an organization would coordinate its security, promote awareness of security-related issues, and establish a resilient cybersecurity culture (FURNELL et al. 2022).

However, SMBs often don't understand the risks, don't have the necessary security knowledge, don't have the financial resources to buy consulting or training, and can rarely prioritize cybersecurity over day-to-day business. Thus, few SMEs have effective procedures, policies and controls to neutralize cyber threats (GUPTA, HAMMOND 2015; SPINELLIS et al. 2019), leaving SMEs vulnerable to attacks from outsiders as well as from insiders with direct access to the company's systems. company. These SMBs are often aware that they should have mitigated a cyber incident after it has happened, or if their peers or the mass media have indicated the need to do so.

SMBs looking to improve cybersecurity are faced with the unfortunate choice of using effort-intensive bespoke advice offered by experts or improving their capabilities on an ad hoc basis . As such, an Information Security Management System (ISMS) is increasingly important for small and medium-sized businesses because it helps them follow a proven framework for protecting their information assets. One of the important areas is identifying risks. In your SME business stage, you need to focus on the business rather than inventing a security framework.

The ISMS provides a systematic approach to managing increasingly complex information security risks, based on widely recognized and time-tested standards such as ISO 27001:2013. ISO 27001 demonstrates to existing and potential customers that the organization has taken the necessary steps to protect its business and is proof of effective internal security practices, giving them a competitive advantage (KRISHNAN, 2020).

As growing organizations, one of the hurdles is establishing credibility with customers or differentiating yourself from larger players. ISO 27001 can help you establish credibility. The ISO 27001 framework will help the organization to protect confidential information and thereby save reputation and costs associated with security incidents. When an organization grows rapidly, it doesn't take long before there is confusion around responsibility for information assets. ISO 27001 helps organizations to establish clear responsibilities regarding information risks (KRISHNAN, 2020).

Consulting firms such as Atlant Security offer services such as password and access management, helping SMBs establish secure access, prevent password reuse and eliminate easy-to-guess passwords. The mitigation control check for 17 types of cyberattacks is also a service that can minimize account compromise, unauthorized access, ransomware , network intrusions, malware infections, sabotage, security policy violations, and more. Cloud security is important as Microsoft 365 has over 280 security settings. Amazon Web Services and Azure also have hundreds of security configuration options.

Gaining access to a corporate account could give a hacker access to all internal systems is a way to secure email and communications where the consultancy protects clients by implementing secure authentication, ensuring the integrity and confidentiality of their communications. Policies and Procedures are the laws that govern even the business of a small company, there is also the possibility of generating security by remote access, using SecureworkFrom Home , whose consulting firms take care of third-party partners and third-party employees, guests and suppliers of small and medium-sized companies.

It is worth noting that each ISMS program built by a consultancy is done differently, from the team to the business objectives. Cybersecurity does n't necessarily have to be expensive for SMBs to implement and maintain. Several

measures can be implemented, as shown here, and the company does not necessarily need to invest in a large amount. Many of these measures focus primarily on ensuring that roles, responsibilities are assigned to the appropriate people, and that employees are aware of cybersecurity risks and how to identify and protect against them. Many of the technical cybersecurity measures are also relatively cost-effective to implement and don't necessarily have to be very sophisticated or complex.

Specific awareness campaigns on cybersecurity issues, which educate SME owners, managers, employees and shareholders , should be created by relevant authorities and, where possible, in partnership with business representative organizations. Such practices will help organizations understand how they can protect their business and what resources such as guidelines, standards and tools they can use. These campaigns must be orchestrated in Brazil, but adjusting their pace and content to specific regional cases.

Software That Can Contribute To The Information Security Of Small And Medium Businesses

There are many types of cybersecurity solutions for SMBs , and getting the right types of security hardware or software can empower your business to maximize its potential without sacrificing security. The key is to choose technology that will keep you one step ahead of attackers and the diverse mix of threats on the scene. The cybersecurity tools that business owners choose will vary based on their network design. But regardless of how their digital infrastructure is set up, they have many options for securing it. The first step is to identify the most valuable digital assets, as well as where the network may be the most vulnerable (FORTINET, 2022).

For many modern companies, the most glaring vulnerabilities are found in the endpoints that connect to the network, as opposed to the assets inside the network. Spending some time analyzing who and what connects to the network and how data flows through it makes it easier to maximize protection. We suggest some tools SMBs can use to protect their business from ransomware , phishing , hackers , and other types of threats.

Endpoint detection and response (EDR) solutions make it easy to detect devices that connect to the network and respond to threats that the system recognizes. For example, if someone connects to the company's network and has malicious intent, the endpoint detection and response system can provide detailed information about the device that connected, as well as data about activity while joining the network. In addition to preventing unwanted users and devices from entering your network, an EDR tool is also a powerful tool for gathering forensic information after a data breach. Entrepreneurs can analyze the logs created by the system to see who connected and determine whether or not they were responsible for the breach (ALMEIDA et al, 2018).

While antivirus software has traditionally been very good at fighting computer viruses, modern antivirus solutions also do a great job of defending against other types of threats. A robust antivirus program can detect a variety of malware attacks by scanning your computer for evidence of known threats. Antivirus software uses existing profiles of attacks that affected users. It checks your system to see if these types of malicious programs are on your computer, informs you about unwanted elements and gets rid of them. Consequently, with the right antivirus software, the company can defend against many of the most dangerous threats in the cyber landscape (ALBUQUERQUE et al, 2016).

Next-generation firewalls provide broad protections against a range of threats while making it easy for external users to access secure connections to your network. They work by inspecting data packets as they are sent to and from your network. If a known threat is detected, Next-Generation Firewall can automatically discard the problematic data packet . Additionally, the right kind of next-generation firewall uses machine learning that can identify malicious behavior. In this way, even zero-day attacks can be stopped because the nature of the malicious code can be detected without the system having to be previously informed of its existence (ASTANI et al, 2016).

Domain Name System (DNS) protection provides an extra layer of defense by preventing employees from accessing dangerous websites. These systems can also filter out content that the company does not want to infiltrate its network, as well as content that it would prefer users not to access (DENSHAM, 2015).

With email gateway security, SMBs can prevent unwanted emails from infiltrating their users' accounts. This includes annoying emails like spam and more direct threats like emails containing malware. With an email gateway security system, while they are using the small business email service, they will not receive the types of messages that are identified as dangerous or unwanted. This keeps threats out of your network, while ensuring email storage space isn't wasted on spam.

Intrusion Detection and Response Systems (IDS/IPS) work by examining the contents of data packets as they attempt to enter the network. This sets it apart from a traditional firewall, which examines information within the headers of data packets. With an intrusion detection and prevention system, the SME can block many different types of threats, especially if its system uses a comprehensive threat intelligence platform to identify malicious code.

With an authentication service, the SMB can prevent unwanted users and hackers from entering its network. This is done by devising a privileged access management (GAP) system that forces users to authenticate their identities before connecting to your system. Using a VPN is a straightforward way to prevent potentially dangerous users from gaining access to your digital assets. With a VPN, not only can the SMB require all users to present login credentials, but it can also encrypt all data that is exchanged between them and their system. In this way, the devices, as well as the network, are protected from external threats (EDDOLS, 2016).

Cloud-based security is a broad term that refers to the technologies and policies used to protect cloud-based assets from cyberattacks. These types of solutions protect cloud resources such as: Data, Forms, Services and Cloud Infrastructure (GALINEC, 2017).

Web application firewalls (WAFs) keep web-based applications safe from hackers who might try to infiltrate them to steal information or exploit a vulnerability in a web application. All traffic going to and from your web service is filtered, and if a threat is detected, the data associated with it can be automatically discarded. Many small and medium-sized businesses use WAFs to protect their web assets from hackers, distributed denial of service (DDoS) attacks, and other Internet threats.

In summary, the tools needed for cybersecurity include endpoint detection and response (EDR), antivirus software, next-generation firewalls, Domain Name System (DNS) protection, email gateway security, intrusion detection and prevention. , logging and monitoring, endpoint protection , authentication and virtual private network (VPN) services, cloud-based security, web application firewalls (WAFs), software-defined wide area networks (SD-WAN), management corporate password management, privileged access management (GAP), vulnerability and threat management, and threat detection .

There is a huge range of patterns, tools, methodologies and techniques that can be used to identify key cybersecurity risks. Risk management frameworks that are practical, easy to understand, easy to translate into business terms, easy to implement without specialist knowledge, and scalable for SMEs need to be designed and promoted. In summary, SMEs seem to implement some of the basic cybersecurity measures only as part of their overall IT implementation. However, it appears that unless cybersecurity controls are included as part of an IT solution, many SMBs do not realize the resulting potential risks to their business.

Cybersecurity has become a significant priority for small businesses looking that adopting a third-party vendor has helped limit their liability in the event of a data breach. protect your business against the enormous cost of data breaches. Cybersecurity IT specialists SB1 responded that “the contract we have with our third-party vendor includes an 86 likely to find solutions more quickly before any damage can occur, as cybersecurity is a significant priority for small businesses looking to protect their business from the huge cost of data breaches.

All of the described strategies, if implemented, can benefit small business owners who want to protect their business data from cyber-attacks. Findings from this study can also be used to build employee knowledge base which may include cyber defense methods and preventive measures used to reinforce cyber security awareness, to provide relevant training and consistent policies across all would include awareness, policies, processes and continuous training of employees for processes.

The findings of this study are in line with the evidence of the reviewed literature and may be relevant to expand the knowledge acquired in previous studies. The findings could and people management, which tends to increase the resilience of small business owners 88 provide small business owners with appropriate strategies to further minimize structuring safer business processes from cyber threats; and also provide your employees with a fundamental understanding of cybersecurity risk .

The results of this study can provide small business owners with how much it would increase customer confidence, business economic growth, and spur effective strategies that successful small business owners have used to protect their

socioeconomic lifecycles, resulting in Employment potentials for residents within the business data from cyber attacks. Positive social change can be achieved through the implementation of this strategy, (b) organizational strategy, (c) consistent security policy, and (d) cybersecurity, risk management strategy. Small business owners can implement and improve management strategy, may be able to provide critical guidance to other owners to reduce consumer exposure to security breaches and improve community engagement. your cybersecurity strategies to eliminate future threats to your business and customer data.

References:-

1. ABEL, I. Minimizing Insider Threat Risk with Behavioral Monitoring. Business Review, 38, 61-73. 2018.
2. ALBUQUERQUE, R; GARCIA VILLALBA, L. J; SANDOVAL OROZCO; DE SOUSA JUNIOR, R. T; KIM, T. Leveraging Information Security and Computational Trust for Cybersecurity. The JournalofSupercomputing , 72, 3729-3763. 2016.
3. ALIANT CIBERSECURITY. Flight for remote work and cybersecurity . 2021 Available at: <https://www.alliantcybersecurity.com/the-flight-to-remote-working-cybersecurity/> Accessed on 27 Sept. 2022.
4. ALMEIDA, F; CARVALHO, I; CRUZ, F. Structure and challenges of a security policy for small and medium-sized companies. KSII Transactionson Internet andInformation Systems, 12, 747–763. 2018.
5. ASTANI, M.; KATHRYN, J. Trends and preventive strategies to mitigate cybersecurity breaches in organizations. Issues in Information Systems Volume 17, Issue II, pp. 208-214, 2016.
6. BREGAR, A. Cybersecurity - Building sustainable protection. DAAAM InternationalScientific Book, 081-090. 2017.
7. BULGURCU, BH CAVUSOGLU, I. BENBASAT. Information security policy compliance: an empirical study of mindsets in information security rationality and awareness. MIS Q., 34(3) (2010), pp. 101-1 523 – 548.
8. CAVUSOGLU, H.; MISHRA, B.; RAGHUNAT.The effect of market value and security companies: capital market reactions to breaching market value and security companies on the Internet. Int. J. Electron . eat . , 9 (1) (2004) , p. 69 - 104
9. CERIC, A. Analysis of interactions between IT and organizational resources in a manufacturing organization using cross-impact analysis. Journalof Enterprise Information Management, 29, 589-611. 2016.
10. CRAM, W.; JG PROUDFOOT.; J D'ARCY. Organizational information security policies: a EUR research and review framework. J.Inf . System , 26 (6) (2017) , p. 605 - 641
11. DENSHAM, B. Three cybersecurity strategies to mitigate the impact of a data breach. Network security. 2015.
12. DHILLON, G. Information Security - Text and Cases (2nd ed.), Prospect Press, Burlington, USA (2017).
13. DRECHSLER, A. An IT strategy development framework for small and medium-sized enterprises. e-Business Information and Management Systems, 16(1), 93–124. 2018.
14. Eddolls , M. Making cybercrime prevention the highest priority. Network Security, 2016.
15. FORTINET. Importance of Cybersecurity for Small and Medium Businesses (SMBs). Available from: <https://www.fortinet.com/resources/cyberglossary/smb-cybersecurity-tools> Access Set 23. 2022.
16. FURNELL, S. Work Experience as a Factor in Awareness of Cybersecurity Risks: A Research Study with College Students . □□ J. Cybersecurity . Priv. 2022.
17. GALINEC, D.; MOZNIK, D.; GUBERINA, B. Cybersecurity and cyber defense: a strategic approach at the national level. Automatika : Journal for Control , Measurement , Electronics , Computing & Communications, 58, 273–286. 2017.
18. MASTER'S GUIDE. DBIR Verizon, 2021. Available at: <https://www.verizon.com/business/resources/reports/dbir/2021/masters-guide/> Accessed 27 Sep. 2022.
19. GUPTA, A.; HAMMOND, R. Small Business Information Systems Security Issues and Decisions: An Empirical Examination. Information Management and Computer Security (13:4). 2015.
20. HAYSTAX. Insider Threat Report. 2019. Retrieved from Haystax : https://haystax.com/wp-content/uploads/2019/07/Haystax-Insider-Threat-Report-2019.pdf. Accessed September 27, 2022.
21. HUANG, K.; SIEGEL, M; MADNIK, S. Systematically Understanding the Business of Cyberattacks: A Survey. ACM ComputingSurveys , 51, 1-36. 2018.
22. IFINEDO, P. Critical times for organizations: what should be done to curb workers' non-compliance with IS security policy guidelines? Inf. Manage System, 33 (1) (2016), pp. 30 – 41.
23. INFOSECURITY. Every 10 seconds there are victims of ransomware in 2020. Available at: <https://www.infosecurity-magazine.com/news/one-ransomware-victim-every-10/> Accessed on 27 Sep. 2022.
24. JONES, J. Ransomware Analysis and Defense : WannaCry and the Win32 Environment. internationalJournalofInformation Security Science, 6, 57-69. 2017.

25. KAPLAN, J. The Board's Role in Cybersecurity Risk Management. MIT Sloan Management Review, 59(2), 12–15. 2018.
26. KARLSSON, M.; T. DENK.; ÅSTRÖM, J. Perceptions of organizational culture and value conflicts in information security management. Inf. Computer. Insurance . , 26 (2), 2018.
27. KRISHNAN, R. Cybersecurity for Small and Medium Enterprises (SMEs). Published 10.2020. Available at: <linkedin.com/pulse/cybersecurity-small-medium-size-companies-smes-raghuvir-krishnan> Accessed 23 Sep. 2022.
28. MARTI, K. Optimal feedback control in stochastic open loop. Stochastic Optimization Methods, 79-118. 2015.
29. MASSACCI, F. Security Events and Vulnerability Data for Cybersecurity Risk Estimation. Risk Analysis, 37, 1606-1627. 2017.
30. THE C. Top cybersecurity statistics , trends and facts. 2021. Available at: <https://www.csoonline.com/article/3634869/top-cybersecurity-statistics-trends-and-facts.html> Accessed 27 Sep. 2022.
31. PAN, Y; WHITE, J; SUN, Y. Assessing the Threat of Distributed Web Worker Attacks . 2016 IEEE Conferenceon Communications and Network Security (CNS), 306–314. 2016.
32. PONEMON. 2020 Global External Threat Cost Report. Retrieved from North Traverse City: 2020.
33. SABILLON, R; CAVALLER, V; CANO, J; SERRA-RUIZ, J. Cybercriminals , cyberattacks and cybercrime. 2016 IEEE InternationalConferenceoncybercrimeand Computer Forensic (ICCCF), 1–9. 2016.
34. SIPONEN, M.; VANCE, A. Burnout: new insights into the problem of security policy violations of employee information systems. MIS Q., 34(3) (2010), pp. 101-1 487 – 502.
35. SOMMESTAD, T.; KARLZEN, H.; HALLBERG. J. The theory of planned behavior and compliance with information security policy. J. Computing. Inf. System, 59 (4) (2019), pp. 344 – 353.
36. SONS.; KIM, S. Protective responses to internet users' information privacy: a taxonomy and a nomological model MIS Q. , 32 (3) (2009) , pp. 101-1 503 – 529.
37. SPINELLIS, D.; DIMITRIS G. Panoptis : Intrusion detection using a domain-specific language. Journalof Computer Security, 10:159–176, 2019.
38. TRAPPE, W; STRAUB. A new open access journal. JournalofCybersecurityandPrivacy , 1(1), 1-3. 2018.
39. MALE. Cybersecurity statistics and trends for 2021. Available at: <https://www.varonis.com/blog/cybersecurity-statistics >Accessed on 27 Sept. 2022.
40. VERIZON. Insider Threat Report - Out of Sight should never be overlooked. 2019. Retrieved from https://enterprise.verizon.com/resources/reports/insider-threat-report.pdf. Accessed September 27, 2022.
41. WATAD, M; WASHHAH, S; PEREZ, C. IT Security Threats and Challenges for Small Businesses: Managers' Perceptions. International Journal of the Business Academic World, 12(1), 23–30. 2018.