JETIR.ORG ISSN: 2349-5162 | ESTD Year : 2014 | Monthly Issue

JOURNAL OF EMERGING TECHNOLOGIES AND INNOVATIVE RESEARCH (JETIR)

An International Scholarly Open Access, Peer-reviewed, Refereed Journal

REVIEW ON CYBER SECURITY IN BUSINESS

Rashmi Dagde
(Assistant Professor)
Computer Science And Engineering
Priyadarshini Bhagwati College Of Engineering
Nagpur, India

Utkarsha M. Wanjari
(Research Scholar)
Computer Science And Engineering
Priyadarshini Bhagwati College Of Engineering
Nagpur, India

Tanishka R. Dubey
(Research Scholar)
Computer Science And Engineering
Priyadarshini Bhagwati College Of Engineering
Nagpur, India

Arya R. Amgaonkar
(Research Scholar)
Computer Science And Engineering
Priyadarshini Bhagwati College Of Engineering
Nagpur, India

Abhijeet . Somkuwar
(Research Scholar)
Computer Science And Engineering
Priyadarshini Bhagwati College Of Engineering
Nagpur, India

Abstract: Businesses play a significant role in the economies of many nations, but the literature indicates that they are not adequately implementing cyber security, making them vulnerable to attacks. In this essay, we review current research on business cyber security with a particular emphasis on how well it adheres to the well-liked NIST Cyber Security Framework (CSF). We also summarise the major obstacles that companies must overcome in order to implement effective cyber security, and we end with important suggestions for doing so. Future research in SMB cyber security should be more evenly distributed, researchers should adopt powerful, well-established quantitative research methodologies to refine and test research, and governments and academia are urged to make investments in providing incentives for researchers to broaden their research focus.

***Index* Terms:** Cyber security, business, security posture, cyber security threats, cyber security frameworks, security.

- **Introduction**

At the international level, businesses account for more than 90% of the business economy. Businesses account for 98% of all businesses in Australia, producing one-third of the nation's GDP and employing 4.7 million people, in contrast to 99.9% ofall businesses in the UK. We are using the definition of the Australian Bureau ofStatistics, which classifies businesses as organisations that employ between 5 and 199 people, because there are different definitions of businesses or small-to-medium enterprises.A growing field, cybersecurity research has a wide range of topics for which authors like Suryotrisongko and Musashi have attempted to create taxonomies. The discovery that there was very little literature available regardingthe cyber security of businesses, both in Australia and globally, made our study necessary. To our knowledge, only two

surveys of a similar nature have been conducted; we go into more detail on these two surveys in Section IV. None of the current surveys have examined the geographic distribution of the surveyed research or aligned theirresearch to a well-known security framework.Attackers are now focusing on companies because they are an easy target and many ofthem lack the resources to protect their networks and information resources. Businesses continue to fall victim to cyberattacks despite widespread precautions taken to protect them. According to statistics, 62% of Australian businesses said they had experienced cyberattacks.

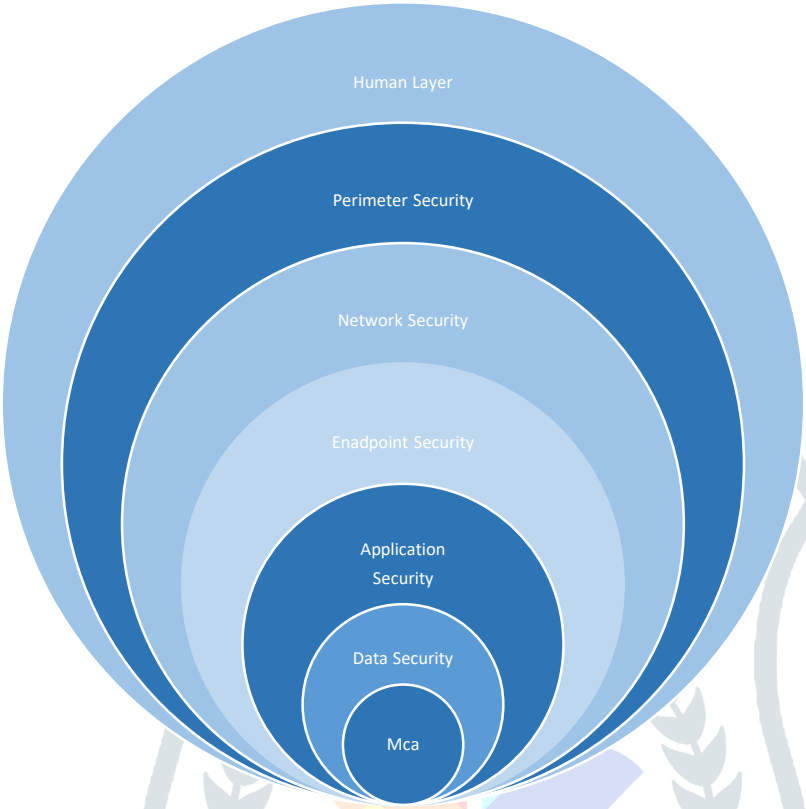

Fig1: 7 Layers Of Cyber-Security

- **Cyber Security Situation for Business**

In this section, we discuss the differences between businesses and large organizations when it comes to cyber security. We continue to discuss current cyberattacks against businesses and their cost implications

2.1 Business VS Large Enterprises

Businesses are vulnerable to the same threats as large organisations because cyber threats do not differentiate between different sizes of organisations. The majorityof the time, larger organisations also have the human and financial resources to implement controls, despite the fact that they generally have a largerattack surface due to their increased employee and device counts. Larger organisations typically employ specialised cybersecurity personnel with the necessary levels of education. Businesses put less money into cyber security, but when it comes to the costs associated with successful cyberattacks, they bear a higher proportional burden than large corporations.

However, businesses may benefitfrom being small and agile and from having more adaptable IT setups.Despite the fact that cyber risk has become a higher priority for larger organisations over thepast few years, industry research showed that many organisations still lack the ability to articulate, approach, and take action in response to cyber risk despite having the necessary human and financial resources. They were also discovered to behaving difficulties with a problem that is common in businesses: teaching and training their staff about cyber security.

2.2 Businesses Under Attack

Businesses are being targeted by online threats more frequently, according to Hayesand Bodhani, because they are thought to be inherently more vulnerable. Cybercriminals who are inexperienced or newer frequently target businesses because they are simple targets. According to the authors, businesses that planned their ITsecurity under the assumption that their networks and data were already secure are to blame for this lax

security.According to a 2020 Verizon report, the attacks are widespread and affect all organisations, regardless of their size, industry, orsector.

However, it should benoted that businesses involved in finance and health care are the most frequently targeted worldwide. The most frequent cyber-attack types that businesses encounter are social engineering (such as phishing), hacking (such as stolen credentials, data theft), malware (such as ransomware), misuse (such as malicious insider behaviour), web-based attacks, and supply chain attacks for e-commerce, according to academic and industry reports. According to the findings of the Ponemon Institute's 2018 study, phishing and social engineering attacks were the most common types of attacks faced by business respondents

2.3 Cost Of Poor Cyber Security For Business

In terms of damaging effects, such as financial ones, cyberattacks are getting worse. The Australian Criminal Intelligence Commission (ACIC) estimates that the direct costs associated with cybercrime alone account for up to $1 billion in annual economic losses for Australia. The effects of cybercrime can be extensive, with additional indirect costs including harm to one's identity, lost business or employment opportunities, and a significant impact on one's psychological and emotional health.

According to reports, 60% of small businesses that were the targets of cyberattacks closed their doors within six months. This shows that smallbusinesses must have cyber defences in place because they stand to lose a lot if cyber threats materialise.The cost of lost business, along with financial loss, legal fees, victim compensation, fines, and internal investigations, was one of thebiggest expenses for small businesses. The expense of compliance checks, training, research, and infrastructure upgrades may be high after a data breach. Additionally, given that hackers are likely to return, businesses are vulnerable torepeated attacks. According to research, 28% of non-compliant victims will likely experience another breach two years after the first one.

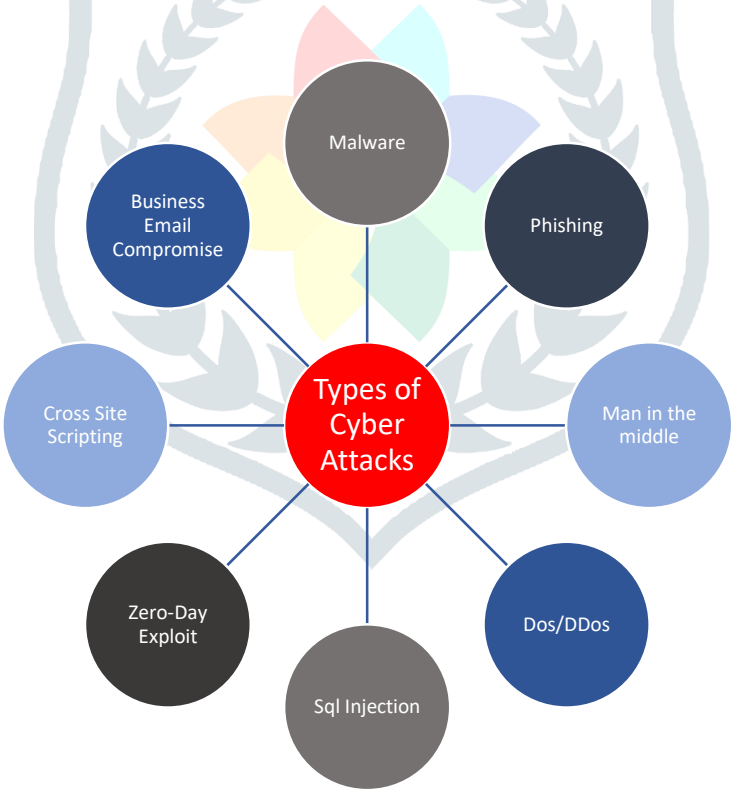

Fig2: Types Of Cyber-Attacks

- **METHODOLOGY**

A methodical approach to researching and comprehending various cyber threats, vulnerabilities, and safeguards for organisational information systems and data areall part of business cybersecurity. The general process for conducting research on business cyber security is outlined below:Definition of the research issue: The research issue or questions you want to address should be clearly stated. For instance, you might want to look into the different kinds of cyber threats that businesses must deal with, the efficacy of the security measures in place, or the effects of cyber incidents on business operations.Research Design: Choose an appropriate research design based on the nature of your research questions. Common research designs in cyber security include:

- Surveys: Collect data from companies using written or online questionnaires to learn about their cyber security procedures, difficulties, and experiences.
- Case Studies: Examine actual cyber security incidents in businesses to comprehend the reasons behind them, theireffects, and how to respond.
- Interviews: To gain in-depth knowledge about particularfacets of cyber security, interview IT specialists, business executives, and experts in the field of cyber security.To assess the efficacy of particular security measures or strategies, conduct controlled experiments.

Data Collection: Compile data using the research design you've selected. Make sure the information is true, pertinent, and reflects the business environment you are researching.

Data analysis: To process and interpret the data, use the appropriate statistical and qualitative analysis techniques. Find the relationships, patterns, and trends in the data that answer your research questions.

Ethics: Make sure your research complies with ethical standards, especially when working with sensitive data. Obtain participants' informed consent, anonymize data as needed, and uphold confidentiality and privacy.Provide actionable advice for businesses on how to strengthen their cyber security procedures and increase their resilience to online threats based on your research'sfindings.

Limitations: Recognise the limitations of your research. Discuss any limitations or difficulties encountered during the studythat may have had an impact on the findings.

- **LITERATURE SURVEY**

- This technical study assesses the level of responsible behaviour exhibited by small and medium-sized businesses and suggests ways to strengthen and encourage CSR in SMEs. The term "corporate social responsibility" has expanded to include efforts done by businesses to conduct their operations in a way that respects the environment, the community, and their workers while also offering opportunity to improve them.
- The study used to determine whether or not this is the case is reported in this publication. The main conclusion is that while the majority of SMEs are aware of the problem, relatively few of them even take a cursory look at the security measures that are available. The confusion resulting from the abundance of contradictory and unclear internet information provided by government and industry entities seems to be one contributing reason. SMEs appeared to be more hampered than helped by this, leaving them unsure of how to strengthen their resilience..
- All societal levels are affected by cyber security, and new risks are emerging in this space as a result of the Internet of Things. When technology advances, so do expenditures in security. New demands for SMEs in terms of cyber-security are brought about by changes in technology, globalisation, and business structures that favour networking and subcontracting. This paper examines the security issues faced by SMEs in the manufacturing sector and offers cyber-security management strategies to address these issues.
- These models help SMEs identify and address risks and weaknesses in their assets. The conceptual framework under investigation represents security concerns in terms of owners, vulnerabilities, threat agents, threats, countermeasures, risks, and assets, as well as their interrelationships. In contrast, the threat classification model is based on attack timeline, and the asset classification model is based on values..

- **CONCLUSION**

To support the creation of cybersecurity solutions for businesses, ongoing researchis necessary. Despite accounting for a sizable portion of businesses, research on cyber security rarely focuses on businesses. It makes a significant contribution tothe world economy, and in Australia in particular, where they account for 98% of all businesses and one-third of GDP. Our study demonstrates thatresearch in business cyber security is rather constrained and narrowly focused, despite their substantial number and significance. This agrees with earlier discoveries made by other researchers.

We also discovered that the majority of business cyber security research is conducted in the United States, despite the fact that other countries have high proportions of businesses and face comparable threats but in different environments. This may be in part because our study only included English-language publications, but it also suggests that many countries are not paying enough attention to business cyber security despite the fact that businesses are the foundation of both national economies and the global economy.Ourresearch discovered that, when taking into account the well-known NIST CSF, research pertaining to business cyber security is concentrated on elements of information security policies and operational security.

The detection, response, and recovery of cyber security incidents are hardly ever discussed in previous or current research. 62% of small businesses in Australia have experienced a cyberattack. Researchers need to concentrate more on cyber resilience given that previous research has mainly been focused on prevention paradigms in order to ensure a more balanced approach to cyber prevention, response, and recovery. Governments should make investments in research and projects that encourage business resilience worldwide. Although cyberattacks are unavoidable, businesses should be prepared to respond to them and recover.

- **References**

- A. Vives, ‘‘Social and environmental responsibility in small and medium enterprises in Latin America,’’ (in English) *J. Corporate Citizenship*, vol. 2006, no.21, pp. 39–50, Mar. 2006, doi:10.9774/GLEAF.4700. HYPERLINK "http://dx.doi.org/10.9774/GLEAF.4700.2006.sp.00006"2006.sp.HYPERLINK"http://dx.doi.org/10.9774/GLEAF.4700.2006.sp.00006"00006.

- K. Renaud and G. R. S. Weir, ‘‘Cybersecurity and the unbearability of uncertainty,’’in*Proc.CybersecurityCyberforensicsConf.(CCC)*,Amman, Jordan, Aug. 2016, pp. 137–143, doi: 10.1109/CCC.2016.29.

- M. Heikkila, A. Rattya, S. Pieska, and J. Jamsa, ‘‘Security challenges in small- and medium-sized manufacturing enterprises,’’ in *Proc. Int. Symp. Small-Scale Intell. Manuf. Syst. (SIMS)*, Narvik, Norway, Jun. 2016, pp. 25–30, doi: 10.1109/SIMS.2016.7802895.

- C. Onwubiko and A. P. Lenaghan, ‘‘Managing security threats and vulnerabilities for small to medium enterprises,’’ in *Proc. IEEE Intell. Secur.Informat.*, New Brunswick, NJ, USA, May 2007, pp. 244–249, doi:10.1109/ISI.2007.379479.

- H. Suryotrisongko and Y. Musashi, ‘‘Review of cybersecurity research topics, taxonomy and challenges: Interdisciplinary perspective,’’ in *Proc. IEEE 12th Conf. Service-Oriented Comput. Appl. (SOCA)*, Kaohsiung, Taiwan, Nov. 2019, pp. 162–167, doi:10.1109/SOCA.2019. HYPERLINK "http://dx.doi.org/10.1109/SOCA.2019.00031" HYPERLINK"http://dx.doi.org/10.1109/SOCA.2019.00031" HYPERLINK "http://dx.doi.org/10.1109/SOCA.2019.00031"00031.

- T. Tam, A. Rao, and J. Hall, ‘‘The good, the bad and the missing: A narrative review of cyber-security implications for Australian small businesses,’’ (in English) *Comput. Secur.*, vol. 109, Oct. 2021, Art. no. 102385, doi: 10.1016/j.cose.2021.102385.

- A. Alahmari and B. Duncan, ‘‘Cybersecurity risk management in small and medium-sized enterprises: A systematic review of recent evidence,’’ in *Proc. Int. Conf. Cyber Situational Awareness, Data Anal. Assessment (CyberSA)*, Dublin, Ireland, Jun. 2020, pp. 1–5, doi: 10.1109/CyberSA49311.2020.9139638.

- J. F. Carias, M. R. S. Borges, L. Labaka, S. Arrizabalaga, and J. Hernantes, ‘‘Systematic approach to cyber resilience operationalization in SMEs,’’ (in English) *IEEE Access*, vol. 8, pp. 174200–174221, 2020, doi: 10.1109/ACCESS.2020.3026063.

- S. Widup, D. Hylender, G. Bassett, P. Langlois, and A. Pinto, ‘‘Verizon: Data breach investigations report 2020,’’ (in English) *Comput. Fraud Secur.*, vol. 2020, no. 6, p. 4, 2020, doi: 10.1016/S1361-3723(20)30059- HYPERLINK "http://dx.doi.org/10.1016/S1361-3723(20)30059-2" HYPERLINK "http://dx.doi.org/10.1016/S1361-3723(20)30059-2" HYPERLINK "http://dx.doi.org/10.1016/S1361-3723(20)30059-2"2.

- M. Heidt, J. P. Gerlach, and P. Buxmann, ‘‘Investigating the security divide between SME and large companies: How SME characteristics influence organizational IT security investments,’’ (in English) *Inf. Syst. Frontiers*, vol. 21, no. 6, pp. 1285–1305, Dec. 2019, doi: 10.1007/s10796-019-09959- HYPERLINK"http://dx.doi.org/10.1007/s10796-019-09959"HYPERLINK"http://dx.doi.org/10.1007/s10796-019-09959-1" HYPERLINK "http://dx.doi.org/10.1007/s10796-019-09959-1"1.

- T. Tam, A. Rao, and J. Hall, ‘‘The invisible COVID-19 small business risks: Dealing with the cyber-security aftermath,’’ *Digit. Government, Res. Pract.*, vol. 2, no. 2, pp. 1–8, Apr. 2021, doi: 10.1145/3436807.

- M. Bada and J. R. C. Nurse, ‘‘Developing cybersecurity education and awareness programmes for small- and medium-sized enterprises (SMEs),’’ (in English) *Inf. Comput. Secur.*, vol. 27, no. 3, pp. 393–410, Jul. 2019, doi: 10.1108/ICS-07-2018-0080.

- J. Hayes and A. Bodhani, ‘‘Cyber security: Small firms under fire,’’ *Eng. Technol.*, vol. 8, no. 6, pp. 80–83, Jul. 2013, doi: 10.1049/et.2013.0614.