AN IMPROVED CYBER SECURITY FRAMEWORK FOR EDUCATION INSTITUTIONS IN INDONESIA

Syarif Hidayatulloh[1], Aedah Abd Rahman[2]
ARS University, bandung, Indonesia[1]
Asia e University, Kuala Lumpur, Malaysia[2]

Abstract

One of the trends in the world of Education is Education technology. The COVID-19 pandemic forces us to accelerate using educational technology to keep the learning process in educational institutions around the world running. However, in adapting and using educational technology, it turns out that there is a factor of concern, namely cyber security. Because almost all educational technology platforms use the internet, cyber security is something that we inevitably have to deal with. Moreover, it turns out that during this covid19 pandemic, cybersecurity attacks have also increased along with the increase in the use of educational technology. Due to the high number of attacks and a large number of security holes in the Education technology platform adopted by educational institutions, So in this study, the authors will evaluate existing standards, models, and frameworks, identify fundamental and critical cybersecurity problems in several educational institutions in Indonesia, and propose a better security framework to address cybersecurity problems in educational technology in institutions.

Keywords: ***cyber security, educational technology, Security Framework***

INTRODUCTION

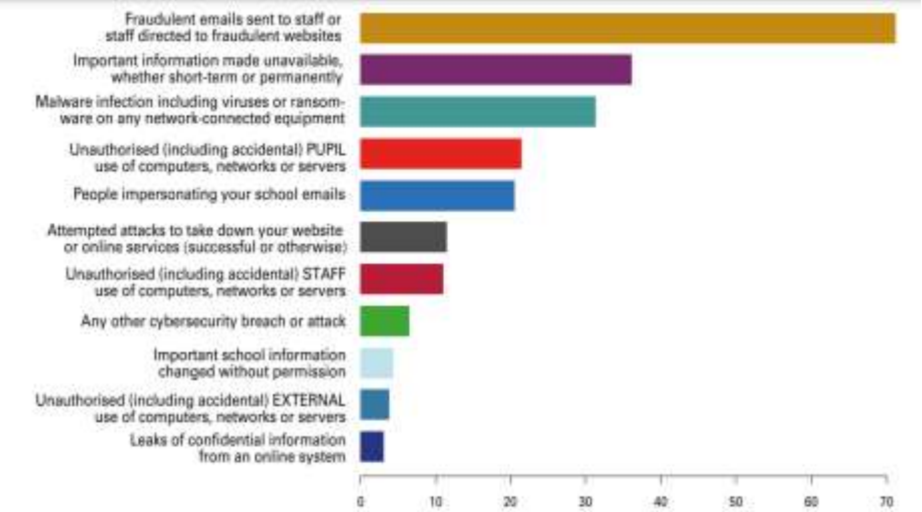
The public and the world of education were shocked by the emergence of the COVID-19 pandemic, which made technological developments change so fast. A tremendous impact was felt in the field of Education, which at the same time gave rise to several trends and issues. For education to continue to run well as it should, the world of education must adapt quickly to various factors that affect learning. Because by understanding trends and issues in the world of education can help educational institutions create learning environments, systems, and tools to support learning effectiveness.

At the beginning of 2020, it was reported that the development of internet use in Indonesia was very rapid. There were recorded active smartphone users connected to the internet, twice the number of internet users, which shows that the average Indonesian has two smartphones. In addition, the number of active social media users is 160 million, with a population increase of 1.1% from the previous year, followed by an increase in the number of internet users, smartphone users, and social media users (Kemp, 2020).

In this year of covid19, internet penetration and the use of information technology have increased compared to the previous year, increasing the potential for cyber-attacks. Educational institutions are one of the targets of cyber attacks because educational institutions contain valuable data that can be exploited. However, many educational institutions are currently not ready to face cyber-attacks because of the lack of awareness of educational institutions on cyber security, such as not understanding the procedures for dealing with various cyber attacks. Several critical issues on cyber security in educational institutions (Wijayanto & Kom, 2020) that is:

1. The high use of information technology and computers in universities increases the risk of cybercrime occurring in educational institutions.
2. Lack of knowledge of the importance of information data security and digital forensics in educational institutions.
3. Many educational institutions have not implemented Cyber Security Management Standards.

2017 to 2018 Joint Information Systems Committee (JISC) survey concluded that staff and students played a significant role in various cybercrime incidents (Goud, 2018). This happens because staff and students are direct users of technology in their respective educational institutions. In addition, Internet users are the most dangerous group in cybersecurity because they have access to various internal services that are less security concern than security from external cyber threats (Centre, 2019).



Source : (Centre, 2019)

LGfL (London Grid for Learning), in collaboration with NCSC (National Cyber Security Center), researched cyber security in 432 schools in the UK and produced several findings, namely (Centre, 2019) :

1. 97 percent of schools stated that losing access to IT services was a significant nuisance.
2. 35 percent of schools train their staff in cybersecurity.
3. 92 percent are aware of and welcome to support their non-IT staff with cybersecurity skills.
4. 83 percent of schools have experienced at least one cybersecurity incident. For example, 69 percent experienced phishing attacks and 35 percent experienced inaccessibility.
5. All schools have some security technology.
6. 98 percent of schools have antivirus and firewall protection.
7. Vigorous use of cybersecurity, such as mobile device management and two-factor authentication, is relatively infrequent.
8. 85 percent of schools have cybersecurity development rules and plans.
9. Less than 49 percent of schools stated that they were ready to accept cyber attacks.

Due to the high number of attacks and a large number of security holes in the Education technology platform adopted by educational institutions, So in this study, the authors will evaluate existing standards, models, and frameworks, identify fundamental and critical cybersecurity problems in several educational institutions in Indonesia, and propose a better framework to address cybersecurity problems in educational technology in institutions.

LITERATURE REVIEW

An essential aspect of the application of information systems is the development of security-related issues in information systems (Chaudhry et al., 2012). Helping network administrators perform their duties efficiently is a constantly researched and investigated problem along with technological developments. In addition, various security issues that need to be known and addressed at the technical and managerial level are a challenge in security issues in information systems (Sadowsky et al., 2003). One of the essential things in information system security is addressing a problem with appropriate precautions as early as possible.

Educational institutions, companies, and government bodies rely heavily on information systems to carry out daily activities in providing their products and services. With the increase in constraints on the information system, it will be a complex problem because it is in the essential system. Thus, the security of information systems is an essential function. This function must be managed and appropriately managed for the maintenance of various services. Good governance is one of them by implementing a proactive system when low costs also accompany problems. Thus, the governance of information system security has its own set of requirements, challenges, activities, and different types of rules (Bowen et al., 2006)

Security becomes a priority when information systems have been tampered with and hacked. Various forms of system destruction, such as spreading viruses, are carried out automatically in the system, while those responsible for information system security must take precautions manually. This is a form of weakness also in security governance (Oriyano, 2017). It all makes the world have to be more focused on securing information systems. Security measures should be taken appropriately to ensure there is no data leak. A comprehensive security framework must be created (Patil, 2008)

In the industrial sector, the blueprint of the company's architecture is a long-term strategy needed to develop information systems. It also serves to balance business and information technology and to add value to the company. One of its essential dimensions is security (Shen et al., 2009)

One example is the modern banking sector is a company increasingly dependent on the internet and information technology to operate its business and interact in its market. Threats, violations, and attacks on the banking world have increased in recent years. Attacks from inside and out have cost trillions of dollars a year to the business. Therefore, a proper framework is needed to organize and secure information systems. Furthermore, it is necessary to examine and compare general and specialized elements to design an optimal and efficient framework (Ula et al., 2011)

Security becomes even more attractive because it is a strategic issue that is even advisable to be removed from the IT domain and aligned with the corporate governance approach with the aim of a security framework designed to be appropriate and following their respective companies (A.A, 2013) IBM's IBM security framework and IBM Security Blueprint explore fears of threats to business systems and information technology. IBM's framework governs risk and cost governance, as well as compliance with business policies. It further demonstrates how these drivers can be translated into security capabilities and needs represented within the framework, enabling better enterprise security. Over the past few decades, industry groups and standards bodies developed frameworks that served as the basis for specific security aspects, and this IBM framework represents many frameworks in detail. To help organizations with their security challenges, IBM created a bridge to address the communication gap between business and security technical perspectives to enable simplification of thoughts and processes (Buecker et al., 2013)

Furthermore, one of the developments in the internet world is an information system based on cloud computing, and this architecture is trendy these days because it has many advantages. Cloud computing architecture is utilized primarily by colleges because, generally, colleges are limited to server resources. In addition, there are already several recommended frameworks for cloud computing such as the European Network and Information Security Agency (ENISA), Cloud Security Alliance (CSA), National Institute of Standards and Technology (NIST) (Negara & Andryani, 2014), Because of the crucial security issues of this information system, in addition to the framework, Intel formed a Security group that is a new business unit that collaborates with McAfee. This Emiratization focuses on accelerating the security of businesses and organizations from various security risks (Framework & Clear, 2014)

Securing sensitive data is becoming increasingly important for educational institutions. Information Security Management System (ISMS) is a systematic approach to establishing, implementing, operating, monitoring, reviewing, maintaining, and improving information security (Haufe et al., 2016). Although ISMS is formed from various existing security standards, it still has many shortcomings because it is considered not mature enough.

NIST and COBIT are commonly used as security references and even become the primary reference for designing new security (Stewart, 2016). In one of its publications, NIST states that organizational risks include many types of risks, such as program management risk, investment risk, legal liability risk, safety risk, inventory risk, supply chain risk, and security risk. Security risks associated with the operation and use of information systems are just one of the many components of an organization's risks handled by those responsible for the management of risks in an organization or company (Calumpang & Dilan, 2016)

The executive order assigns NIST to develop a framework for improving security in critical sectors to produce common standards that can be used by a variety of critical sector organizations and are critical to assessing and managing their security risks. This framework is designed to complement the organization's risk management processes and security programs. This framework applies broadly, regardless of size, industry, or security sophistication (Department of Defense, 2019)

Information security (IS) should be integrated into the governance of institutions and considered a governance challenge that includes adequate reporting, accountability, and risk management. The implementation of good information security governance (ISG) provides strategic alignment, risk management, resource management, performance measurement, and value delivery. Several publications have discussed this area. However, there has been no identified success determinant that ensures improvement across areas of effective governance. We need a framework of best practices across areas of effective IS governance that supports institutions to survive and thrive (Gashgari et al., 2017)

Most organizations recognize that security is essential to information system development, but business costs and performance often take precedence over security. Although security awareness is growing, most organizations focus on implementing security only at the commissioning stage of system development and trying to incorporate system security by force into the final design, resulting in the ineffective implementation of system security (CSA Singapore, 2017)

Research in security approaches, both technical and non-technical, continues. Due to the growing need for security, an alternative approach combines technical and non-technical methods. In this way, it is expected to find new, better ways to use (Koskosas, 2013)

Given the increasing and seriousness of cyberattacks, we must be aware of the need to stay one step ahead. The issuance of security frameworks aims to support regulated entities to have proper security governance and build a robust infrastructure together with the necessary controls and prevention. A framework that articulates proper control and provides guidance on how to assess maturity levels. The adoption and implementation of this framework is expected to enhance security (Saudi Arabian Monetary Authority (SAMA), 2017)

LITERATURE REVIEW

An essential aspect of the application of information systems is the development of security-related issues in information systems (Chaudhry et al., 2012). Helping network administrators perform their duties efficiently is a constantly researched and investigated problem along with technological developments. In addition, various security issues that need to be known and addressed at the technical and managerial level are a challenge in security issues in information systems (Sadowsky et al., 2003). One of the essential things in information system security is addressing a problem with appropriate precautions as early as possible.

Educational institutions, companies, and government bodies rely heavily on information systems to carry out daily activities in providing their products and services. With the increase in constraints on the information system, it will be a complex problem because it is in the essential system. Thus, the security of information systems is an essential function. This function must be managed and appropriately managed for the maintenance of various services. Good governance is one of them by implementing a proactive system when low costs also accompany problems. Thus, the governance of information system security has its own set of requirements, challenges, activities, and different types of rules (Bowen et al., 2006)

Security becomes a priority when information systems have been tampered with and hacked. Various forms of system destruction, such as spreading viruses, are carried out automatically in the system, while those responsible for information system security must take precautions manually. This is a form of weakness also in security governance (Oriyano, 2017). It all makes the world have to be more focused on securing information systems. Security measures should be taken appropriately to ensure there is no data leak. A comprehensive security framework must be created (Patil, 2008)

In the industrial sector, the blueprint of the company's architecture is a long-term strategy needed to develop information systems. It also serves to balance business and information technology and to add value to the company. One of its essential dimensions is security (Shen et al., 2009)

One example is the modern banking sector is a company increasingly dependent on the internet and information technology to operate its business and interact in its market. Threats, violations, and attacks on the banking world have increased in recent years. Attacks from inside and out have cost trillions of dollars a year to the business. Therefore, a proper framework is needed to organize and secure information systems. Furthermore, it is necessary to examine and compare general and specialized elements to design an optimal and efficient framework (Ula et al., 2011)

Security becomes even more attractive because it is a strategic issue that is even advisable to be removed from the IT domain and aligned with the corporate governance approach with the aim of a security framework designed to be appropriate and following their respective companies (A.A, 2013) IBM's IBM security framework and IBM Security Blueprint explore fears of threats to business systems and information technology. IBM's framework governs risk and cost governance, as well as compliance with business policies. It further demonstrates how these drivers can be translated into security capabilities and needs represented within the framework, enabling better enterprise security. Over the past few decades, industry groups and standards bodies developed frameworks that served as the basis for specific security aspects, and this IBM framework represents many frameworks in detail. To help organizations with their security challenges, IBM created a bridge to address the communication gap between business and security technical perspectives to enable simplification of thoughts and processes (Buecker et al., 2013)

Furthermore, one of the developments in the internet world is an information system based on cloud computing, and this architecture is trendy these days because it has many advantages. Cloud computing architecture is utilized primarily by colleges because, generally, colleges are limited to server resources. In addition, there are already several recommended frameworks for cloud computing such as the European Network and Information Security Agency (ENISA), Cloud Security Alliance (CSA), National Institute of Standards and Technology (NIST) (Negara & Andryani, 2014), Because of the crucial security issues of this information system, in addition to the framework, Intel formed a Security group that is a new business unit that collaborates with McAfee. This Emiratization focuses on accelerating the security of businesses and organizations from various security risks (Framework & Clear, 2014)

Securing sensitive data is becoming increasingly important for educational institutions. Information Security Management System (ISMS) is a systematic approach to establishing, implementing, operating, monitoring, reviewing, maintaining, and improving information security (Haufe et al., 2016). Although ISMS is formed from various existing security standards, it still has many shortcomings because it is considered not mature enough.

NIST and COBIT are commonly used as security references and even become the primary reference for designing new security (Stewart, 2016). In one of its publications, NIST states that organizational risks include many types of risks, such as program management risk, investment risk, legal liability risk, safety risk, inventory risk, supply chain risk, and security risk. Security risks associated with the operation and use of information systems are just one of the many components of an organization's risks handled by those responsible for the management of risks in an organization or company (Calumpang & Dilan, 2016)

The executive order assigns NIST to develop a framework for improving security in critical sectors to produce common standards that can be used by a variety of critical sector organizations and are critical to assessing and managing their security risks. This framework is designed to complement the organization's risk management processes and security programs. This framework applies broadly, regardless of size, industry, or security sophistication (Department of Defense, 2019)

Information security (IS) should be integrated into the governance of institutions and considered a governance challenge that includes adequate reporting, accountability, and risk management. The implementation of good information security governance (ISG) provides strategic alignment, risk management, resource management, performance measurement, and value delivery. Several publications have discussed this area. However, there has been no identified success determinant that ensures improvement across areas of effective governance. We need a framework of best practices across areas of effective IS governance that supports institutions to survive and thrive (Gashgari et al., 2017)

Most organizations recognize that security is essential to information system development, but business costs and performance often take precedence over security. Although security awareness is growing, most organizations focus on implementing security only at the commissioning stage of system development and trying to incorporate system security by force into the final design, resulting in the ineffective implementation of system security (CSA Singapore, 2017)

Research in security approaches, both technical and non-technical, continues. Due to the growing need for security, an alternative approach combines technical and non-technical methods. In this way, it is expected to find new, better ways to use (Koskosas, 2013)

Given the increasing and seriousness of cyberattacks, we must be aware of the need to stay one step ahead. The issuance of security frameworks aims to support regulated entities to have proper security governance and build a robust infrastructure together with the necessary controls and prevention. A framework that articulates proper control and provides guidance on how to assess maturity levels. The adoption and implementation of this framework is expected to enhance security (Saudi Arabian Monetary Authority (SAMA), 2017)

METHOD

This chapter describes the design of research in this research for the achievement of research objectives. It starts by identifying the vital variables that affect cybersecurity in educational institutions obtained from previous research. Then the selected variables are made questionnaires containing questions to be given to respondents in educational institutions in Indonesia to find new variables or maybe even eliminate existing variables with quantitative methods, descriptive statistical data analysis. Vital variables are included in the next stage, namely verification, clarification, and validation by experts with qualitative methods to get recommendations in solving cybersecurity problems in educational institutions. The recommendations of these experts become the basis in the formulation of a model of improvement of cybersecurity frameworks in educational institutions to be made.

RESULTS AND DISCUSSION

The increasing access to various digital services in educational institutions will also increase the number of security vulnerabilities (Aldheleai et al., 2015; Salimovna, 2019). Furthermore, because of the COVID-19 pandemic, many educational institutions have just switched to using various technology services for education. However, they do not understand how important the safety factor is in the various technologies they adopt (Shivshankar & Paul, 2016). In addition, the main challenge of cybersecurity in various educational service technologies is the lack of attention to security itself (Adetoba B. T., 2016) and the security factor being something that is often overlooked (Besimi et al., 2009). Furthermore, although this cybersecurity issue is considered very important, the literature and references to research and investigate it are still insufficient (Savulescu et al., 2015). One of the success factors in implementing technology in educational institutions lies in cyber security itself (Abdul Majid et al., 2015). Not to mention that many systems, services, and technology for education are generally powerless when exposed to cyber-attacks (Derawi, 2015). This makes it a unique and significant challenge to research (Bandara et al., 2014; Jianming, 2007). Currently, cybersecurity in educational institutions is highly dependent on the role of humans. In addition, there is no systematic mechanism for testing cybersecurity vulnerabilities (Violettas et al., 2013), so specific techniques or mechanisms are needed to improve cybersecurity in educational institutions (Bhatia et al., 2018). This research will try to find the critical factors in cyber security in educational institutions from various technical and non-technical perspectives to formulate a framework for improving cyber security in educational institutions in Indonesia.

CLOSING

Conclusion

The phenomena in the field and the visible research gaps are very relevant to be explored further. The limitations of previous research on educational technology cybersecurity in educational institutions are the main background of this research. Because at this time, when humanity is preoccupied with handling the COVID-19 pandemic, it turns out that cyber security in educational institutions is one of the objects that are widely exploited for various purposes that are detrimental to educational institutions.

The massive increase in the exploitation of cybersecurity during the COVID-19 pandemic has become an exciting phenomenon. This phenomenon will be observed to obtain several essential factors for designing and formulating a new cybersecurity framework in Educational Institutions.

Research and testing will be carried out in several educational institutions in Indonesia that have adopted various educational technologies in their educational institutions. The initial stage of the research is to identify and validate various cyber security factors from previous research and from the survey results to be conducted. Furthermore, it was followed by conducting a follow-up survey to experts in the field of cyber security.

This research is expected to obtain new findings theoretically and practically, which can be implemented in the framework of proposed improvements, and ends with a brief discussion about the importance of this research to provide input for further research.

The contents of the bibliography are written in Times New Roman 12 font and written with 1.15 spaces. The bibliography is a source of reference/reference which is used as a reference for manuscript writing. Writing a bibliography is a source of reference/reference that is used as material for citations to writing manuscripts. Writing a bibliography uses the rules of The Chicago Manual of Style (CMS). The number of reference sources used as a manuscript bibliography is at least 10 titles of scientific literature (80% primary references, and 20% secondary references). Primary reference sources, such as: journals, research reports, theses, teris, dissertations, and proceeding papers. Secondary reference sources, such as: books and internet sources. We recommend writing citations using the Mandeley reference manager application

REFERENCES

A.A, A. (2013). Information Security Management System: Emerging Issues and Prospect. *IOSR Journal of Computer Engineering*, *12*(3), 96–102. https://doi.org/10.9790/0661-12396102

Abdul Majid, H., Abdul Majid, M., Ibrahim, M. I., Wan Manan, W. N. S., & Ramli, M. R. (2015). Investigation of security awareness on e-learning system among lecturers and students in Higher Education Institution. *I4CT 2015 - 2015 2nd International Conference on Computer, Communications, and Control Technology, Art Proceeding*, *I4ct*, 216–220. https://doi.org/10.1109/I4CT.2015.7219569

Adetoba B. T., A. O. and K. S. O. (2016). E-learning Security Issues and Challenges : A Review. *Journal of Scientific Research and Studies*, *3*(5), 96–100.

Aldheleai, H. F., Bokhari, M. U., & Hamatta, H. S. A. (2015). User security in e-learning system. *Proceedings - 2015 5th International Conference on Communication Systems and Network Technologies, CSNT 2015*, 767–770. https://doi.org/10.1109/CSNT.2015.113

Bandara, I., Ioras, F., & Maher, K. (2014). Cyber Security Concerns in E-Learning Education. *Proceedings of ICERI2014 Conference*, *November*, 728–734.

Besimi, A., Shehu, V., Abazi-Bexheti, L., & Dika, Z. (2009). Managing security in a new learning management system (LMS). *Proceedings of the International Conference on Information Technology Interfaces, ITI*, 337–342. https://doi.org/10.1109/ITI.2009.5196105

Bhatia, M., Assistant Professor, SIES College of Arts, S. and C., Navi Mumbai, I., Meghnabhatia@rediffmail.com, Maitra, D. J. K., Professor, A., CS, D. of M. and, University, R., & Jabalpur, I. (2018). 2018 International Conference on Computational and Characterization Techniques in Engineering & Sciences (CCTES) : Integral University, Lucknow, India, Sep 14-15, 2018. *2018 International Conference on Computational and Characterization Techniques in Engineering & Sciences (CCTES)*, 276–285.

Bowen, P., Hash, J., & Wilson, M. (2006). Information Security Handbook: A Guide for Managers NIST Special Publication 800-100. *NIST Special Publication 800-100*, *October*, 137. https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-100.pdf%0Ahttps://nvlpubs.nist.gov/nistpubs/legacy/sp/nistspecialpublication800-100.pdf

Buecker, A., Arunkumar, S., Blackshaw, B., Borrett, M., Brittenham, P., Flegr, J., Jacobs, J., Jeremic, V., Johnston, M., Mark, C., Marx, G., Daele, S. Van, & Vereecke, S. (2013). *Using the IBM Security Framework and IBM Security Blueprint to Realize Business-Driven Security*. 1–240. http://www.redbooks.ibm.com/redbooks/pdfs/sg248100.pdf

Bustani, B., Khaddafi, M. ., & Nur Ilham, R. (2022). REGIONAL FINANCIAL MANAGEMENT SYSTEM OF REGENCY/CITY REGIONAL ORIGINAL INCOME IN ACEH PROVINCE PERIOD YEAR 2016-2020. *International Journal of Educational Review, Law And Social Sciences (IJERLAS)*, *2*(3), 459–468. https://doi.org/10.54443/ijerlas.v2i3.277

Calumpang, J. C., & Dilan, R. E. (2016). Evaluation Framework on System Security Requirements for Government-Owned Agencies in the Philippines. *International Journal of Information and Education Technology*, *6*(5), 398–403. https://doi.org/10.7763/ijiet.2016.v6.721

Centre, N. C. S. (2019). *Cyber Security Schools Audit 2019*. 18.

Chaudhry, P. E., Chaudhry, S. S., Reese, R., & Jones, D. S. (2012). Enterprise information systems security: A conceptual framework. *Lecture Notes in Business Information Processing*, *105 LNBIP*, 118–128. https://doi.org/10.1007/978-3-642-28827-2_9

CSA Singapore. (2017). *Security-by-Design Framework*. 1–51. https://www.csa.gov.sg/~/media/csa/documents/legislation_supplementary_references/security_by_design_framework.pdf

Department of Defense. (2019). *Defense Industrial Base (DIB) Guide to Implementing the Cybersecurity Framework*.

Derawi, M. (2015). E-learning protection of open access platforms. *2014 International Conference on Web and Open Access to Learning, ICWOAL 2014*. https://doi.org/10.1109/ICWOAL.2014.7009238

Falahuddin, F., Fuadi, . F., Munandar, M., Juanda, R. ., & Nur Ilham, R. . (2022). INCREASING BUSINESS SUPPORTING CAPACITY IN MSMES BUSINESS

GROUP TEMPE BUNGONG NANGGROE KERUPUK IN SYAMTALIRA ARON DISTRICT, UTARA ACEH REGENCY. *IRPITAGE JOURNAL*, *2*(2), 65–68. https://doi.org/10.54443/irpitage.v2i2.313

Framework, T., & Clear, P. (2014). The Cybersecurity Framework in Action : An Intel Use Case. *Intel*, 50. www.nist.

Gashgari, G., Walters, R., & Wills, G. (2017). A proposed best-practice framework for information security governance. *IoTBDS 2017 - Proceedings of the 2nd International Conference on Internet of Things, Big Data and Security*, *IoTBDS*, 295–301. https://doi.org/10.5220/0006303102950301

Geovani, I. ., Nurkhotijah, S. ., Kurniawan, H. ., Milanie, F., & Nur Ilham, R. . (2021). JURIDICAL ANALYSIS OF VICTIMS OF THE ECONOMIC EXPLOITATION OF CHILDREN UNDER THE AGE TO REALIZE LEGAL PROTECTION FROM HUMAN RIGHTS ASPECTS: RESEARCH STUDY AT THE OFFICE OF SOCIAL AND COMMUNITY EMPOWERMENT IN BATAM CITY. *International Journal of Educational Review, Law And Social Sciences (IJERLAS)*, *1*(1), 45–52. https://doi.org/10.54443/ijerlas.v1i1.10

Goud, N. (2018). *Students are responsible for cyber attacks on Universities and Colleges*. Cybersecurity Insiders. https://www.cybersecurity-insiders.com/students-are-responsible-for-cyber-attacks-on-universities-and-colleges/

Haufe, K., Colomo-Palacios, R., Dzombeta, S., Brandis, K., & Stantchev, V. (2016). A process framework for information security management. *International Journal of Information Systems and Project Management*, *4*(4), 27–47. https://doi.org/10.12821/ijispm040402

Ilham, Rico Nur. *et all* (2019). Investigation of the Bitcoin Effects on the Country Revenues via Virtual Tax Transactions for Purchasing Management. International Journal of Suplly Management.Volume 8 No.6 December 2019.

Ilham, Rico Nur. *et all* (2019).. Comparative of the Supply Chain and Block Chains to Increase the Country Revenues via Virtual Tax Transactions and Replacing Future of Money. International Journal of Suplly Management.Volume 8 No.5 August 2019.

Jianming, Y. (2007). Security modelling for e-Learning. *Proceedings of the 2007 1st International Symposium on Information Technologies and Applications in Education, ISITAE 2007*, 1–5. https://doi.org/10.1109/ISITAE.2007.4409226

Kemp, S. (2020). Digital 2020: Global Digital Overview. *Hootsuite*.

Koskosas, I. (2013). A Short Literature Review in Information Systems Security. *Business Excellence and Management*, *3*(2), 5–15.

Lasta Irawan, A. ., Briggs, D. ., Muhammad Azami, T. ., & Nurfaliza, N. (2021). THE EFFECT OF POSITION PROMOTION ON EMPLOYEE SATISFACTION WITH COMPENSATION AS INTERVENING VARIABLES: (Case Study on Harvesting Employees of PT. Karya Hevea Indonesia). International Journal of Social Science, Educational, Economics, Agriculture Research, and Technology (IJSET), 1(1), 11–20. https://doi.org/10.54443/ijset.v1i1.2

likdanawati, likdanawati, Yanita, Y., Hamdiah, H., Nur Ilham, R., & Sinta, I. (2022). EFFECT OF ORGANIZATIONAL COMMITMENT, WORK MOTIVATION AND LEADERSHIP STYLE ON EMPLOYEE PERFORMANCE OF PT. ACEH DISTRIBUS INDO RAYA. International Journal of Social Science, Educational, Economics, Agriculture Research, and Technology (IJSET), 1(8), 377–382. https://doi.org/10.54443/ijset.v1i8.41

Mahfud, M., Yudiana, I. K., & Sariyanto, S. (2022). HISTORY OF BANYUWANGI KALIKLATAK PLANTATION AND ITS IMPACT ON SURROUNDING COMMUNITIES. International Journal of Educational Review, Law And Social Sciences (IJERLAS), 3(1), 91–104. https://doi.org/10.54443/ijerlas.v3i1.492

Mahfud *et all* (2021). PEMANFAATAN TRADISI RESIK LAWON SUKU USING SEBAGAI SUMBER BELAJAR SEJARAH LOKAL PADA SMA DI BANYUWANGI. Media Bina Ilmiah Vol.16 No.3 Oktober 2021. http://ejurnal.binawakya.or.id/index.php/MBI/article/view/1294/pdf

Mahfud *et all* (2020). Developing a Problem-Based Learning Model through E-Learning for Historical Subjects to Enhance Students Learning Outcomes at SMA Negeri 1 Rogojampi. *IOP Conf. Series: Earth and Environmental Science 485 (2020) 012014* doi:10.1088/1755-1315/485/1/012014

Majied Sumatrani Saragih, M. ., Hikmah Saragih, U. ., & Nur Ilham, R. . (2021). RELATIONSHIP BETWEEN MOTIVATION AND EXTRINSIC MOTIVATION TO ICREASING ENTREPRENEURSHIP IMPLEMENTATION FROM SPP AL-FALAH GROUP AT BLOK 10 VILLAGE DOLOK MASIHUL. *MORFAI JOURNAL*, *1*(1), 1–12. https://doi.org/10.54443/morfai.v1i1.11

Negara, E. S., & Andryani, R. (2014). *A Review : Security Framework Information Technology for University Based on Cloud Computing*. *February*, 20–21.

Nur Ilham, R. ., Arliansyah, A., Juanda, R., Multazam, M. ., & Saifanur, A. . (2021). RELATHIONSIP BETWEEN MONEY VELOCITY AND INFLATION TO INCREASING STOCK INVESTMENT RETURN: EFFECTIVE STRATEGIC BY JAKARTA AUTOMATED TRADING SYSTEM NEXT GENERATION (JATS-NG) PLATFORM. *International Journal of Economic, Business, Accounting, Agriculture Management and Sharia Administration (IJEBAS)*, *1*(1), 87–92. https://doi.org/10.54443/ijebas.v1i1.27

Nur Ilham, R., Heikal, M. ., Khaddafi, M. ., F, F., Ichsan, I., F, F., Abbas, D. ., Fauzul Hakim Hasibuan, A. ., Munandar, M., & Chalirafi, C. (2021). Survey of Leading Commodities Of Aceh Province As Academic Effort To Join And Build The Country. *IRPITAGE JOURNAL*, *1*(1), 13–18. https://doi.org/10.54443/irpitage.v1i1.19

Nur ilham, R., Likdanawati, L., Hamdiah, H., Adnan, A., & Sinta, I. . (2022). COMMUNITY SERVICE ACTIVITIES "SOCIALIZATION AVOID STUDY INVESTMENT" TO THE STUDENT BOND OF SERDANG BEDAGAI. *IRPITAGE JOURNAL*, *2*(2), 61–64. https://doi.org/10.54443/irpitage.v2i2.312

Nur Ilham, R., Arliansyah, A., Juanda, R. ., Sinta, I. ., Multazam, M. ., & Syahputri, L. . (2022). APPLICATION OF GOOD CORPORATE GOVERNANCE PRINCIPLES IN IMPROVING BENEFITS OF STATE-OWNED ENTERPRISES (An Emperical Evidence from Indonesian Stock Exchange at Moment of Covid-19). *International Journal of Economic, Business, Accounting, Agriculture Management and Sharia Administration (IJEBAS)*, *2*(5), 761–772. https://doi.org/10.54443/ijebas.v2i5.410

Nur ilham, R., Likdanawati, L., Hamdiah, H., Adnan, A., & Sinta, I. . (2022). COMMUNITY SERVICE ACTIVITIES "SOCIALIZATION AVOID STUDY INVESTMENT" TO THE STUDENT BOND OF SERDANG

BEDAGAI. *IRPITAGE JOURNAL*, *2*(2), 61–64. https://doi.org/10.54443/irpitage.v2i2.312

Nur Ilham, R., Arliansyah, A., Juanda, R. ., Sinta, I. ., Multazam, M. ., & Syahputri, L. . (2022). APPLICATION OF GOOD CORPORATE GOVERNANCE PRINCIPLES IN IMPROVING BENEFITS OF STATE-OWNED ENTERPRISES (An Emperical Evidence from Indonesian Stock Exchange at Moment of Covid-19). *International Journal of Economic, Business, Accounting, Agriculture Management and Sharia Administration (IJEBAS)*, *2*(5), 761–772. https://doi.org/10.54443/ijebas.v2i5.410

Oriyano, S.-P. (2017). Issaf. *CEH^{TM}v9*, 549–564. https://doi.org/10.1002/9781119419303.app2

Patil, J. (2008). INFORMATION SECURITY FRAMEWORK: CASE STUDY OF A MANUFACTURING ORGANIZATION. *Master Thesis*, *1*, 461. https://www.bertelsmann-stiftung.de/fileadmin/files/BSt/Publikationen/GrauePublikationen/MT_Globalization_Report_2018.pdf%0Ahttp://eprints.lse.ac.uk/43447/1/India_globalisation%2C society and inequalities%28lsero%29.pdf%0Ahttps://www.quora.com/What-is-the

Rahmaniar, R., Subhan, S., Saharuddin, S., Nur Ilham, R. ., & Anwar, K. . (2022). THE INFLUENCE OF ENTREPRENEURSHIP ASPECTS ON THE SUCCESS OF THE CHIPS INDUSTRY IN MATANG GLUMPANG DUA AND PANTON PUMP. International Journal of Social Science, Educational, Economics, Agriculture Research, and Technology (IJSET), 1(7), 337–348. https://doi.org/10.54443/ijset.v1i7.36

Rico Nur Ilham, Irada Sinta, & Mangasi Sinurat. (2022). THE EFFECT OF TECHNICAL ANALYSIS ON CRYPTOCURRENCY INVESTMENT RETURNS WITH THE 5 (FIVE) HIGHEST MARKET CAPITALIZATIONS IN INDONESIA. *Jurnal Ekonomi*, *11*(02), 1022–1035. Retrieved from http://ejournal.seaninstitute.or.id/index.php/Ekonomi/article/view/481

Sadowsky, G., Dempsey, J. X., Greenberg, A., Mack, B. J., & Schwartz, A. (2003). *Information Technology Security Handbook*. http://infodev.org

Salimovna, F. D. (2019). *Security issues in E-Learning system*.

Sandi, H. ., Afni Yunita, N. ., Heikal, M. ., Nur Ilham, R. ., & Sinta, I. . (2021). RELATIONSHIP BETWEEN BUDGET PARTICIPATION, JOB CHARACTERISTICS, EMOTIONAL INTELLIGENCE AND WORK MOTIVATION AS MEDIATOR VARIABLES TO STRENGTHENING USER POWER PERFORMANCE: AN EMPERICAL EVIDENCE FROM INDONESIA GOVERNMENT. *MORFAI JOURNAL*, *1*(1), 36–48. https://doi.org/10.54443/morfai.v1i1.14

Saudi Arabian Monetary Authority (SAMA). (2017). *Cyber Security Framework*. *May*, 1–56. http://www.sama.gov.sa/en-US/Laws/BankingRules/SAMA Cyber Security Framework.pdf

Savulescu, C., Polkowski, Z., Cosmin, D. I., & Elena, B. C. (2015). Security in e-learning systems. *Proceedings of the 2015 7th International Conference on Electronics, Computers and Artificial Intelligence, ECAI 2015*, WE19–WE24. https://doi.org/10.1109/ECAI.2015.7301225

Shen, Y.-T., Lin, F., Tapie Rohm, C., & Tapie, C. (2009). A Framework for Enterprise

Security Architecture and Its Application in Information Security Incident Management. *Communications of the IIMA*, *9*(4). http://scholarworks.lib.csusb.edu/ciimahttp://scholarworks.lib.csusb.edu/ciima/vol9/iss4/2

Shivshankar, S., & Paul, S. (2016). E-Learning Environment-The Security and Privacy Challenges Focusing on the Counter Measures. *Proceedings - 2015 International Conference on Developments in ESystems Engineering, DeSE 2015*, 176–179. https://doi.org/10.1109/DeSE.2015.31

Sinurat, M. ., Heikal, M. ., Simanjuntak, A. ., Siahaan, R. ., & Nur Ilham, R. . (2021). PRODUCT QUALITY ON CONSUMER PURCHASE INTEREST WITH CUSTOMER SATISFACTION AS A VARIABLE INTERVENING IN BLACK ONLINE STORE HIGH CLICK MARKET: Case Study on Customers of the Tebing Tinggi Black Market Online Store. *MORFAI JOURNAL*, *1*(1), 13–21. https://doi.org/10.54443/morfai.v1i1.12

Stewart, J. M. (2016). *Cybersecurity Frameworks to Consider for Organization-wide Integration*. 1–9. www.globalknowledge.com

Ula, M., Ismail, Z., & Sidek, Z. (2011). A Framework for the Governance of Information Security in Banking System. *Journal of Information Assurance & Cybersecurity*, *2011*, 1–12. https://doi.org/10.5171/2011.726196

Violettas, G. E., Theodorou, T. L., & Stephanides, G. C. (2013). E-learning software security: Tested for security vulnerabilities and issues. *Proceedings - 2013 4th International Conference on e-Learning Best Practices in Management, Design and Development of e-Courses: Standards of Excellence and Creativity, ECONF 2013*, 233–240. https://doi.org/10.1109/ECONF.2013.66

Wijayanto, H., & Kom, M. (2020). *POLICY BRIEF KESIAPAN PERGURUAN TINGGI WILAYAH JAWA TENGAH DALAM MENGHADAPI SERANGAN SIBER*.

Wayan Mertha, I. ., & Mahfud, M. (2022). HISTORY LEARNING BASED ON WORDWALL APPLICATIONS TO IMPROVE STUDENT LEARNING RESULTS CLASS X IPS IN MA AS'ADIYAH KETAPANG. International Journal of Educational Review, Law And Social Sciences (IJERLAS), 2(5), 507–612. https://doi.org/10.54443/ijerlas.v2i5.369

Yusuf Iis, E., Wahyuddin, W., Thoyib, A., Nur Ilham, R., & Sinta, I. (2022). THE EFFECT OF CAREER DEVELOPMENT AND WORK ENVIRONMENT ON EMPLOYEE PERFORMANCE WITH WORK MOTIVATION AS INTERVENING VARIABLE AT THE OFFICE OF AGRICULTURE AND LIVESTOCK IN ACEH. *International Journal of Economic, Business, Accounting, Agriculture Management and Sharia Administration (IJEBAS)*, *2*(2), 227–236. https://doi.org/10.54443/ijebas.v2i2.191