International Conference on Business Economics, Social Sciences & Humanities

Applied Cyber Law in Architecture Model for Medical Gasses Cylinder Management.

M A Soetomo[1] , Ivan[2] and H P Ipung [3]
[1]Faculty Of Engineering & Information Technology, Swiss German University, Jl. Jalur Sutera Barat Kav 15, Tangerang 15143, Indonesia
[2]Faculty Of Engineering & Information Technology, Swiss German University, Jl. Jalur Sutera Barat Kav 15, Tangerang 15143, Indonesia
[3]Faculty Of Engineering & Information Technology, Swiss German University, Jl. Jalur Sutera Barat Kav 15, Tangerang 15143, Indonesia

Email: mohammad.soetomo@sgu.ac.id[1] , ivan@student.sgu.ac.id[2] , heru.ipung@sgu.ac.id[3]

Abstract. As digitalization is conveniently managing and controlling our daily activities. The goal of the research is to explore and provide a capability architecture model that may assist a transformation digital platform in the medical sector should have a barrier, such as risk of cybercrime. Method implemented is using TOGAF, and mapping risk analysis potentially related to cybercrimes. Results finding cyberlaws help to control disobedience toward compliance in the digital platform. This research focus on transforming traditional medical gasses for hospital future needs and planning toward digital platform. The impact of the research then identified cybercriminals, like data offenses, fraud, repudiation, false/defamatory statement, and unauthorized access, which are useful for law enforcement facing cybercrimes' trends.

Keywords: medical, gasses, cyber, management, hospital, law, medical gas installation, medical

1. Introduction

Currently, the hospital only uses a digital platform for finance, receipts, medical lab results and registration purposes. In the future, the hospital will transform to digital use for the other hospital facilities. Medical gases installation services as one of the hospital facilities will also transform to a digital platform. According to triangle fraud risk factor model fraud detection may develop due to an opportunity factor, to name few indicators are e.g., insufficient board oversight, internal control environment, etc.[10] Thus, the laws then required as controls should enforce the hospital digital transformation to minimize fraud opportunities committing cybercrimes.

From previous studies showing the significant of cybercrimes' activities are major concerned: Ramli, et.al. stated that privacy, obscenity, defamation, information security and internet crime, are considered of basic principles categories for cybercrime.[1] Bacharuddin further mentioned that anyone is prohibited to tapping any information using electronic devices being referred as data offences.[2] Another case found a research related to the False/Defamatory Statement, i.e., when patients checked in to hospital during the admission not all patients are documented and shown in reports (100%).[3] In the US a vendor for several Veterans Affairs (VA) medical facilities was sentenced for defrauding the VA by creating false invoices and reports for medical gas inspections that never took place.[4] This news related to fraudulent case.

From legally mandatory requirements for hospital facilities are based on Permenkes, Undang-Undang tentang informasi dan transaksi elektronik No. 19 tahun 2016 and Undang-Undang No. 47 tahun 2021 tentang rumah sakit. Authors then conducting literature review based on chapters and articles in Undang-Undang, and observing secondary data gathered from publications.[1-4] to identify and collect risk events and risk categories. Two risk categories found, which are human error and financial management derived from risk events.[11] This process is further determine capabilities required toward Architecture Vision (Table 1). Hence, an enterprise architecture with business layer, application layer, and technology layer ensures the cybercrimes' gap is covered.

2. Methods

The architecture model for medical gas cylinder management is to prevent risks like running out of the cylinder, either above or under the level of a quantity of medical gas cylinder being purchased, wrong medical gas cylinder received, medical gas incident cylinder report, and data inaccuracy, timeliness overrun, inconsistency and irrelevancy. The capabilities needed is the analysis of medical gas usage data, analysis of supply chain data, analysis of repeat order data, analysis of purchase data, analysis of inventory data, analysis of incident cylinder data, analysis of material receiving report data, analysis of medical gas cylinder attribute, analysis of data history medical gas cylinder faulty or defect, analysis of medical gas cost, and analysis of vendor performance. See Table 1 the architecture vision structure is designed and developed by TOGAF architecture with focusing upon business architecture, application architecture and technology architecture.[5]

Table 1. Architecture Vision.

Risk	Risk Category	Capabilities
Run out of cylinder supply	Human error	1. Analysis of medical gas usage data 2. Analysis of supply chain data
Over or under a quantity of medical gas cylinder purchase	Financial Management	3. Analysis of repeat order data. 4. Analysis of purchase data 5. Analysis of inventory data
Wrong medical gas cylinder received	Financial management Human Error	6. Analysis of incident cylinder data 7. Analysis of material receiving report data. 8. Analysis of medical gas cylinder attribute
Medical gas incident cylinder report	Human error	9. Analysis of data history medical gas cylinder faulty or defect.
No data accuracy, timeliness, consistency, and relevancy	Financial management	10. Analysis of medical gas cost. 11. Analysis of vendor performance.

Next, a case study about capabilities from Table 1 are mapped toward architecture layers using TOGAF, e.g.

- Business Architeture
- Application Architecture
- Data Architecture, and
- Technology Architecture.

Additionally, observing capabilities in Table 2, and potentially risk of cybercrimes associated with previous studies[1][2][3][4]: our model is developed based on keywords and definition of selected cybercrimes activities. Hence, the model is qualitatively matched and fit to the architecture vision for medical gasses cylinder management. Table 2 gives a picture of capabilities, business architecture, application architecture, data architecture and technology architecture, mapping with risk of cybercrime criterion. The risk potential for cybercrimes are considered then data offenses, fraud, repudiation, and defamatory/false statements.

Table 2. Capabilities, Business Architecture, Application Architecture, Data Architecture and Technology Architecture and risk of cybercrime of each capability.

Capabilities	Business Architecture	Application Architecture	Data Architecture	Technology Architecture	Risk of Cybercrime
Analysis of medical gas usage data	The technical officer monitoring medical gases usage.	Data analysis of medical gasses usage by a record inspection system	Take data by inspecting manifold	Inspection manifold with mobile apps	Data Offenses
Analysis of supply chain data	The supply chain can't stop with the prediction for abnormal situation	Record data on medical gasses usage. Scheduled inspection system	Average use medical gas cylinder usage today and yesterday	Give information on medical gasses usage and inventory	Data Offenses
Analysis of repeat order data.	Automated replenishment system	Notification, when the inventory of medical gas cylinder hit, reorder point and purchase requisition system	Medical gas cylinder stock	Notification using mobile apps	Repudiation
Analysis of purchase data	Accuracy of how many cylinders should purchase	Purchase requisition system and purchase messaging system	Data analysis of cylinder usage every month or every day	Analyze medical gasses usage using mobile apps	Fraud

Analysis of inventory data	Labeling medical gas cylinder process	QR code scanning system	Take data by QR Code	Mobile apps and QR Code scanner	Repudiation
Analysis of incident cylinder data	Material reject and classified as an incident or faulty cylinder	Material reject system	Data of medical gas cylinder defect and faulty	Checklist using mobile apps	Fraud
Analysis of material receiving report data.	Receiving report system for accuracy and delivery time of material receive	Item master	Data of medical gas cylinder attribute	Mobile apps report system	Data Offenses
Analysis of medical gas cylinder attribute	Physical checking of a medical gas cylinder when received, to make sure cylinder is ready to use	Medical gas cylinder condition checklist form	Data of medical gas cylinder condition	A mobile apps inspection system	False/Defamatory Statement
Analysis of data history medical gas cylinder faulty or defect	Incident cylinder record to prevent faultily and defect cylinder	Incident cylinder input data and release system	Data of medical gas cylinder faulty and defect	Mobile apps incident cylinder record	Data Offenses
Analysis of medical gas cost	Medical gas cost efficiency to minimize fraud	Purchase a system and inspect the manifold system	Data of medical gas purchase and use	Mobile apps cost analysis	Data Offences
Analysis of vendor performance	Vendor performance report to minimize business risk	Vendor information system	Data about time and accuracy of delivery medical gas cylinder	Mobile apps vendor data analysis	Data Offenses

3. Results and Discussion

For validation purposes authors conducting mapping the risk of cybercrimes towards articles and chapters upon the law, Undang-Undang, hence, proven the model proposed fit accordingly identified and confirmed articles and chapters associated for medical gasses cylinder management (see Table 3). This could be inferred Undang-Undang are aligned for cyber laws, though further studies required, particularly from laws perspective and discipline. Data offenses are prohibited by the cyber law of information and electronic transaction in the jurisdiction of Indonesia, based on UU 19 years 2016 act 31, when somebody tries to interception data in a computer, mobile phone or another electronic device, even they are not doing a changing of the data or deleting some data, it is prohibited.[4] Data offense is also against PP no. 46 years 2014 act 29 about data manipulation in healthcare facilities.[5] Repudiation is against PP No. 47 years 2021 act hospital has a responsibility to give correct information about the healthcare services.[6] Fraudulent is against UU No. 11 information and electronic transaction years 2008 about interdiction to do data manipulation.[7] A false or defamatory statement is against UU No. 11 information and electronic transaction years 2008 act 28 about spreading fake information.[1]

Table 3. Risk of cybercrime mapping with cyber law.

Risk of Cybercrime	Capabilities	Cyber Law
Data Offenses[2]	Analysis of medical gas usage data	UU 19 years 2016 act 31 about information and electronic transaction PP no. 46 years 2014 act 29 about the hospital information system
Data Offenses[2]	Analysis of supply chain data	UU 19 years 2016 act 31 about information and electronic transaction PP no. 46 years 2014 act 29 about the hospital information system
Repudiation[1]	Analysis of repeat order data.	PP No. 47 years 2021 about the hospital
Fraud[4]	Analysis of purchase data	UU No. 11 years 2018 about the hospital information system act 35
Repudiation[1]	Analysis of inventory data	PP No. 47 years 2021 about the hospital
Fraud[4]	Analysis of incident cylinder data	UU No. 11 years 2018 about the hospital information system act 35
Data Offences[2]	Analysis of material receiving report data.	UU 19 years 2016 act 31 about information and electronic transaction PP no. 46 years 2014 act 29 about the hospital information system
False/Defamatory Statement[1][3]	Analysis of medical gas cylinder attribute	A false or defamatory statement is against UU No. 11 information and electronic transaction years 2008 act 28
Data Offenses[2]	Analysis of data history medical gas cylinder faulty or defect	UU 19 years 2016 act 31 about information and electronic transaction PP no. 46 years 2014 act 29 about the hospital information system

Data Offenses[2]	Analysis of medical gas cost	UU 19 years 2016 act 31 about information and electronic transaction PP no. 46 years 2014 act 29 about the hospital information system
Data Offenses[2]	Analysis of vendor performance	UU 19 years 2016 act 31 about information and electronic transaction PP no. 46 years 2014 act 29 about the hospital information system

4. Conclusion

The law of information system at the hospital does not give detailed information about the violation in using electronic devices, the law of information system at the hospital just mentions the tip of iceberg the information system at the hospital. This study conducting TOGAF capability and gap analysis towards Undang-Undang to further investigate how chapters and articles may pursue disobedient behaviors particularly in medical gasses management. Therefore, stakeholders and or enforcement institutions or agencies may follow up to prevent incidents may cause not only financially but could be lives; this is the main contribution of the paper. There are many elements of the hospital facilities should be addressed in more detailed to identify and detect associated cybercrimes that are manageable proactively. The hospital is a triage system, and mandatorily for zero faults in their performance, so the law of applying an information system at a hospital should be more precise and improved consistently as mean of controlled and monitored governance and practices.

References

[1] Ramli, T. S. (2019). PRINSIP PRINSIP CYBER LAW PADA MEDIA OVER THE TOP E-COMMERCE BERDASARKAN TRANSFORMASI DIGITAL DI INDONESIA. *Jurnal Legislasi Indonesia*, *16*(3), 392-398.

[2] Bacharuddin Jusuf Habibie 1999 "*UU No. 36 Tahun 1999 tentang Telekomunikasi*"

[3] Madadin, M., Alqarzaie, A. A., Alzahrani, R. S., Alzahrani, F. F., Alqarzea, S. M., Alhajri, K. M., & Al Jumaan, M. A. (2021). Characteristics of Medico-Legal Cases and Errors in Medico-Legal Reports at a Teaching Hospital in Saudi Arabia. *Open Access Emergency Medicine: OAEM*, *13*, 521.

[4] Department of Justice U.S. Attorney's Office 2020 "*Agawam Man Sentenced for Defrauding VA Hospitals by Failing to Inspect Medical Gas Systems*."

[5] Taleb, M., & Cherkaoui, O. (2012). Pattern-oriented approach for enterprise architecture: TOGAF framework.

[6] Joko Widodo 2016 "*UU No. 19 Tahun 2016 tentang Perubahan Atas Undang-Undang Nomor 11 Tahun 2008 Tentang Informasi Dan Transaksi Elektronik*."

[7] DR. H. Susilo Bambang Yudhoyono 2014 "*PP No. 46 Tahun 2014 tentang Sistem Informasi Kesehatan*."

[8] Joko Widodo 2021 "*PP No. 47 Tahun 2021 tentang Penyelenggaraan Bidang Perumahsakitan* ."

[9] DR. H. Susilo Bambang Yudhoyono 2008 "*UU No. 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik*."

[10] Huang, S. Y., Lin, C. C., Chiu, A. A., & Yen, D. C. (2017). Fraud detection using fraud triangle risk factors. *Information Systems Frontiers*, *19*(6), 1343-1356.

[11] Isaca. (2009). *The Risk IT practitioner guide*. ISACA.