HAL open science

Cyber Security in Healthcare Organisations

Dhrisya Ravidas, Malcolm R. Pattinson, Paula Oliver

To cite this version:

Dhrisya Ravidas, Malcolm R. Pattinson, Paula Oliver. Cyber Security in Healthcare Organisations. 15th International Symposium on Human Aspects of Information Security and Assurance (HAISA), Jul 2021, Virtual, United Kingdom. pp.3-11, 10.1007/978-3-030-81111-2_1 . hal-04041067

HAL Id: hal-04041067

https://inria.hal.science/hal-04041067v1

Submitted on 22 Mar 2023

HAL is a multi-disciplinary open access archive for the deposit and dissemination of scientific research documents, whether they are published or not. The documents may come from teaching and research institutions in France or abroad, or from public or private research centers.

L'archive ouverte pluridisciplinaire **HAL**, est destinée au dépôt et à la diffusion de documents scientifiques de niveau recherche, publiés ou non, émanant des établissements d'enseignement et de recherche français ou étrangers, des laboratoires publics ou privés.

Distributed under a Creative Commons Attribution 4.0 International License

This document is the original author manuscript of a paper submitted to an IFIP conference proceedings or other IFIP publication by Springer Nature. As such, there may be some differences in the official published version of the paper. Such differences, if any, are usually due to reformatting during preparation for publication or minor corrections made by the author(s) during final proofreading of the publication manuscript.

Cyber Security in Healthcare Organisations

Dhrisya Ravidas[1], Malcolm R Pattinson[2], Paula Oliver[3]

[1]Adelaide Business School, University of Adelaide, South Australia
dhrisya.ravidas@adelaide.edu.au

[2]Adelaide Business School, University of Adelaide, South Australia
malcolm.pattinson@adelaide.edu.au

[3]AustCyber SA Node, Department of Innovation and Skills,
Adelaide, South Australia
paula.oliver@sa.gov.au

Abstract. The aim of the research described in this paper was to develop a cyber security survey for the purpose of assessing the state of cyber security controls in a selection of healthcare organisations in South Australia. To achieve this aim, a gap analysis was conducted, using the collected data, that identified cyber security controls which had not been implemented satisfactorily, according to management. An acceptable level of cyber security is dependent on a specific set of controls that should have been implemented in order to maintain the Confidentiality, Integrity and Availability (CIA) of digital healthcare data and the risk appetite of the organisations. Specifically, in this case, healthcare management was concerned about the increasing number of cyber threats to Patient Health Information (PHI). In this era of a connected world, information is highly sought after and vulnerable to cyber security breaches. In this context, cyber security can be seen to be very similar to personal hygiene, such that, personal hygiene is only achieved if the appropriate practices, routines, actions, and behaviours are in place.

Keywords: Digital Information Systems (DIS), Goal Attainment Scaling (GAS), Cyber Security, Healthcare Sector, Confidentiality, Integrity and Availability (CIA), Gap Analysis, Patient Health Information (PHI), Notifiable Data Breaches (NDB).

1 Introduction

Cyber security has become a critical issue for most organisations today, particularly those with a significant investment in Digital Information Systems (DIS). However, management and internal auditors still ask, ‘is our information secure?’ or ‘do we have the necessary blend of controls in place to withstand the various threats to our information?’. These questions are still tough to answer. In the past, management has sought answers by having both internal and external specialists conduct information security reviews and risk analysis on a regular basis. These projects were typically costly, time-consuming, and resource-intensive, because they were originally designed for large organisations with extensive information systems (Love, 1991). The Healthcare Sector (hospitals, clinics and other healthcare facilities) has become globally dependent on digital technology to monitor, send, retrieve, store and share healthcare data. It is clear that cyber security threats are more common due to the rising value of sensitive health information and the increased dependency on digital systems. Cyber security breaches in the Healthcare Sector will negatively impact both patients and healthcare organisations, potentially life-threatening consequences such as PHI being compromised (Andre, 2017). Healthcare organisations are vulnerable due to the historic lack of investment in cyber security and vulnerabilities in existing hardware and software. However, employee actions, processes, routines or behaviour (Coventry and Branley, 2018) continue to be the primary source of risk. As we move forward, cyber security must be an integral part of healthcare organisations' responsibilities. Although the management of cyber security risks and their mitigation is the responsibility of individual organisations, the government should also enact laws and regulations to secure the general public from such cyber threats.

Cyber security plays an integral role in making Australia a safer and highly trusted place to do business. The rapid and widespread uptake of digital technology by households and businesses following the COVID-19 pandemic underscores the importance of digital technology as an economic enabler (Offner, et al., 2020). Millions of Australians are working from home, staying connected through software apps and using essential digital services such as telehealth (Jalali, et al., 2019). Consequently, there is an urgent need to put in place a framework of controls to ensure a level of cyber security that is acceptable to management. Evolving government policies and fast technological advancement are exposing the vulnerabilities of the healthcare sector to cyber security breaches. While other sectors, like finance and defense, have invested in securing their data and systems, healthcare organisations still fall behind in adapting to the newer regulations, security protocols and the pace at which it adopts more modern technology (Andre, 2017). This is identified as the reason that the healthcare sector is a prime target for PHI security breaches. Furthermore, it is essential that cyber security is paid its due attention to ensure the protection of personal health information of healthcare stakeholders (Australian Cyber Security Centre, 2020). It does this by ensuring that the Confidentiality, Integrity and Availability (CIA) of PHI is achieved and maintained.

1.1 Research Aim

The research described in this paper aims to develop a cyber security survey to assess the state of cyber security controls within selected South Australian healthcare organisations. A gap analysis methodology known as Goal Attainment Scaling (GAS) was used to achieve this aim.

2 Literature Review

As part of the literature review, various types of cyber security breaches were investigated together with their associated threats and risks. There have been multiple cyber incidents, including the WannaCry (Ehrenfeld, 2016) and NotPetya (Smith, 2019) ransomware attacks, which are indicative of poor cyber security in healthcare organisations.

In September 2016, the Health Minister of Australia disclosed that the data of 3 million patients had been accessed due to vulnerability of the Medicare system. This gave perpetrators access to doctors' prescriptions and PHI (Spooner & Towell, 2016).

Recently the Australian Cyber Security Centre (ACSC) reported that there is a significant increase in malicious cyber activity in healthcare or COVID-19 environments such as aged-care facilities and other healthcare sectors. For example, some financially motivated perpetrators used the 'Maze' ransomware attack to lock an organisation's valuable information so that they could steal important business information and threaten to post this information online unless a ransom was paid (Australian Cyber Security Centre, 2020).

The Office of the Australian Information Commissioner (OAIC) compared notifications made under the Notifiable Data Breaches (NDB) scheme across the top five industry sectors. It stated that during the reporting period from January to June 2020, the health service sector recorded 115 data breaches. These statistics imply that the healthcare industry has become a prime target for cyber adversaries (Notifiable Data Breaches Report: January–June 2020, 2021).

Furthermore, the OAIC report found that the leading cause of the data breaches during the 12 months was phishing, causing 153 violations. Still, over a third of all notifiable data breaches were directly due to human error (52 per cent). It is to be noted that other leading sources of human error are the unintended release or publication of PHI (20 per cent) and the loss of paperwork or data storage devices (23 per cent) (Eddy, 2019).

According to recently released data compiled by the Centre for Strategic and International Systems (CSIS), Australia is in the top six most hacked countries in the world, with 16 significant cyber-attacks reported in the period between May 2006 and June 2020 (Livingstone, 2020).

3 Research Method

This research used an email-distributed questionnaire that utilised the Goal Attainment Scaling (GAS) methodology to identify the potential cyber security vulnerabilities in selected organisations within the healthcare sector in South Australia. This research was conducted in three phases. In the first phase, the cyber security controls were identified as the essential eight cyber security practices, together with five implementation levels of the controls and the GAS-based instrument was developed using the Qualtrics online survey. In the second phase, data collection was done using this online survey to conduct the assessment. In the third phase, the results were calculated, analysed, and reported to the selected management.

3.1 Description of Goal Attainment Scaling (GAS)

The GAS methodology is a program evaluation methodology used to evaluate the effectiveness of a program or project (Kiresuk *et al*, 2014). A program evaluation methodology is a process of determining how well a particular program is achieving or has achieved its stated aims and expectations. Kiresuk and Lund (1982) state that program evaluation is a process of establishing "...the degree to which an organisation is doing what it is supposed to do and achieving what it is supposed to achieve." (p. 227). Goal Attainment Scaling (GAS) has been in use for 35 years as a means of measuring outcomes from different contexts and enabling these measures to be represented by a quantitative measure (Pattinson, 2001).

One of the essential components of the GAS methodology is the evaluation instrument. This is primarily a table or matrix whereby the columns represent objectives to be assessed and the rows represent levels of attainment of those objectives. Kiresuk *et al* (1994) refer to these objectives as goals or scales within a GAS Follow-up Guide. The rows represent contiguous descriptions of the degree of expected goal outcomes. These can range from the best-case level of goal attainment to the worst case, with the middle row being the most preferred level of goal attainment.

It is "a flexible tool for internal evaluation" (Love, 1991, p. 93), enabling different organisations to set their own objectives and measurement criteria. This is in contrast to most other evaluation techniques that have pre-set standards that cannot be readily modified by stakeholders. This is primarily a table or matrix whereby the columns represent objectives to be assessed, and the rows represent levels of attainment of those objectives. These can range from the best-case level of goal attainment to the worst case, with the middle row being the most likely level of goal attainment. Goal attainment scaling is rated using the standard 5-point scale (-2 to +2) and formula to derive aggregated T-scores, as recommended by its originators (Kiresuk et al 2014).

The sample GAS Follow-up Guide in Fig. 1 below is one of the eight follow-up guides that comprised the complete evaluation tool in this study.

PASSWORD USE

Please click on only ONE box in each of the three CONTROL columns

LEVEL OF IMPLEMENTATION	CONTROL 1 Password complexity	CONTROL 2 Multi-factor authentication (MFA)	CONTROL 3 Passwords for different accounts
Much less than expected	• Passwords are NOT used or have less than 12-characters • Does NOT use a combination of uppercase, lowercase letters, numbers or special characters	• MFA is NOT used to access networks and applications	• Use the SAME passwords for ALL accounts
Somewhat less than expected	• Passwords have a minimum 12-characters • Does NOT use a combination of uppercase, lowercase letters, numbers or special characters	• MFA is used to access MOST networks and applications	• Use DIFFERENT passwords for MOST accounts
Expected	• Passwords have a minimum 12-characters • Use AT LEAST one uppercase, lowercase letters, numbers or special characters	• MFA is used to access ALL networks and applications	• Use DIFFERENT passwords for all IMPORTANT accounts
Somewhat more than expected	• Passwords have a greater than 12-characters • Use MORE than one uppercase, lowercase letters, numbers or special characters	+ Use of swipe card or biometrics identification	• Use COMPLEX passwords for SOME accounts
Much more than expected	+ Forced to change the password every month + Re-use of passwords not allowed	+ Reviewed and audited at least 3-MONTHLY	• Use COMPLEX passwords or passphrase for all IMPORTANT accounts

Fig. 1. Password Use GAS Chart

3.2 Phase 1: Development of the GAS Evaluation Instrument

This phase utilises the eight essential controls referenced by the Cyber Check me document (Edith Cowan University, 2019) on the information assets and the security CIA that applies across the South Australian healthcare sector (CyberCheckMe, 2019).

A GAS follow-up guide for each of the eight essential practices was developed by identifying three of the most highly critical cyber security controls as per Fig. 2 below. This gave a total of twenty-four controls to be evaluated within the selected healthcare systems. The specific implementation of the controls may differ according to the technology choice and security needs of the respective organisation.

Essential Practices	Control No. 1	Control No. 2	Control No. 3
PASSWORD USE	Password complexity	Multi-factor authentication (MFA)	Passwords for different accounts
INTERNET USE	Using public Wi-Fi	Using virtual private network (VPN)	Using HTTPS website addresses
EMAIL USE	Suspicious files & links	Report suspicious emails	Encrypt confidential emails
SOFTWARE UPDATES	Anti-virus software	Application patches	Operating system patches
PHYSICAL DEVICE PROTECTION	Physical entry controls	Working in secure areas	Clean desk & clear screen policy
DATA BACKUPS	Identify the data to be backed up	Backup stored in a safe location	Data backup frequency
INCIDENT REPORTING	Reporting cyber security incidents	Follow up from incidents	Disciplinary process
EMPLOYEE TRAINING	Cyber security training	Frequency of training	Type of training

Fig. 2. Practices and controls used

3.3 Phase 2: Use the GAS evaluation instrument

This phase of the research relates to the distribution of the survey by email to the ICT authority of the five selected SA healthcare organisations. The GAS charts are interpreted to evaluate the essential controls. This is to encourage readability and positive engagement of the user. The principal objective of obtaining valuable data through an online survey is to develop a survey questionnaire specifically designed for the selected participants. Each respondent will select one appropriate level of implementation for each of the 24 controls within the eight essential practices. The chosen level of implementation should be the one that best describes their current situation.

The research described in this paper is a preliminary study only and will be extended to many more healthcare organisations and respondents. This will provide more validity of the GAS methodology and, therefore, a more accurate assessment of an organisation's level of cyber security.

3.4 Phase 3: Analyse the evaluation results and report to management

This phase involves the analysis of the data collected after all responses had been received. Raw scores were converted into GAS T-scores for each of the eight Follow-up Guides in accordance with the Kiresuk *et al* (1994) methodology. The data from each survey response consisted of 24 scores within the range values of -2.-1, 0, +1 and +2 as per the GAS methodology. All responses for any one organisation would then be combined and converted to into one non-weighted T-score for each of the 8 follow-up guides.

A GAS T-score is a linear transformation of the average of the raw scores in each follow-up guide using the formulae documented by Kiresuk et al (1994) and is presented below:

$$T-score = 50 + \frac{10\sum w_i x_i}{\sqrt{(1-p)\sum w_i^2 + p(\sum w_i)^2}}$$

where x_i is the outcome score for the ith scale with a weight of w_i, and p is the weighted average inter-correlation of the scale scores and commonly set at 0.3. Scores on the individual scales between -2 and +2 each are assumed to have a theoretical distribution with a mean of zero and a standard deviation of 1. This formula then produces T-scores with a mean of 50 and a standard deviation of 10 when each scaled control is scored using the -2 to +2 scale by Kiresuk *et al* (1994). The five-point range of levels for cyber security controls is shown in Fig. 3 below.

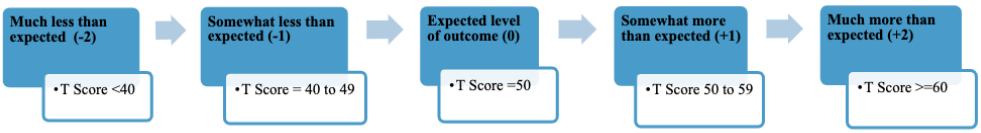

Fig. 3. Goal Attainment Scaling Score

The GAS T-scores were calculated for each of the 8 follow-up guides, and a non-weighted T-score graph is depicted in the results, as shown in Fig. 4 below.

4 Results

A GAS T-score of 50 or more indicates that, on average, the controls specified within a GAS follow-up guide for a particular cyber security practice are considered acceptable to management. This assumes that management is aware of the levels of management expectations and compliance requirements with the specific cyber security policies and guidelines. If these controls are representative of all controls specified for this cyber security practice, then it can be contended that the controls in place are generally acceptable to management.

The extent of management expectations is reflected in the amount that the score is greater than 50. Conversely, a GAS T-score of less than 50 for a particular cyber security practice indicates that, in general, the cyber security controls in place are not acceptable to management. Therefore, the organisation is at risk of being breached through exploitation of that weak control. Fig. 4 below is indicative of the eventual data analysis results. For example, Employee Training appears to be satisfactory whereas

Password Use and Physical Device Protection are seriously inadequate and need to be addressed by the organisations management.

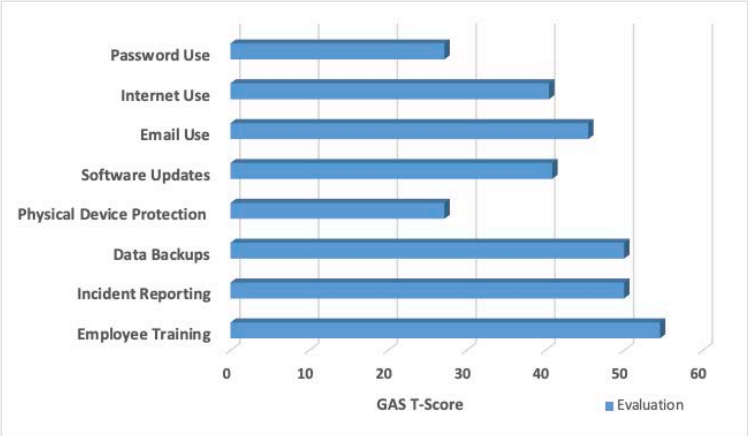

Fig. 4. Non-weighted GAS T-Scores

5 Limitations & Future Research

The research outlined in this paper needs to be replicated in several private South Australian healthcare organisations and with many ICT managers' responses before the methodology is considered to be validated. This research was only intended to be a preliminary study prior to a full-scale study.

An evaluation of controls in this way, is not considered an audit of cyber security controls. In other words, it does not test inputs, processes, outputs, and business operations for conformance against a Standard. Instead, it measures stakeholder perceptions of the current state of play. Hence, it is recommended that the results be validated by conducting an independent audit of the controls. Further research is guaranteed to address the following research questions:

- Is the GAS methodology suitable for different sized organisations?
- Is the GAS methodology suitable for different organisations other than Healthcare?
- Is the GAS methodology suitable in organisations with multiple digital platforms?
- Could this GAS methodology be used to compare the state of cyber security controls within different organisations?

6 Conclusions

This research demonstrated that the GAS methodology, combined with a specific set of cyber security controls, is a feasible methodology to evaluate cyber security effectively and enable management to address the state of cyber security controls. Some attributes that contribute to this claim are:

- It is "a flexible tool for internal evaluation" (Love, 1991, p. 93), enabling different organisations to set their own objectives and measurement criteria. This is in contrast to most other evaluation techniques that have pre-set criteria that stakeholders cannot readily modify.
- It is particularly suitable for assessing management controls because it involves both summative and formative evaluations (Love, 1991, p. 93). The summative evaluation equates to assessing the level of attainment of cyber security controls after they have been implemented. The formative evaluation relates to on-going assessments of how well the cyber security controls are being maintained.
- It differs from many traditional evaluation approaches in that the assessment of a single control can result in one of five possible outcomes. Most other methods rely on dichotomous outcomes. For example, the approaches such as "Management by Objectives and Goal Monitoring", measure whether a goal was attained or not (Love, 1991).
- It is one of the few evaluation techniques that converts a qualitative assessment of an area or issue into a quantitative result. More specifically, the GAS methodology generates a number for each Follow-up Guide by averaging evaluator raw scores. These numbers facilitate the comparison between evaluations at different times.

References

Andre, T., 2017. Cybersecurity an enterprise risk issue. *Healthcare Financial Management*, *71*(2), pp.40-46.

Australian Cyber Security Centre (ACSC). 2020. [online]
Available at:<https://www.cyber.gov.au/acsc/view-all-content/advisories/2020-013-ransomware-targeting-australian-aged-care-and-healthcare-sectors>

Coventry, L. and Branley, D., 2018. Cybersecurity in healthcare: a narrative review of trends, threats and ways forward. *Maturitas*, *113*, pp.48-52.

CyberCheck.me. 2020. Cyber Guides. [Online]
Available at: <https://www.cybercheck.me/cyber-guides.html>

Edith Cowan University. 2020. Cyber Hints and Tips. [Online] Available at: <https://www.ecu.edu.au/schools/science/research-activity/ecu-security-research-institute/cybercheckme/cyber-hints-and-tips.>

Eddy, N., 2019. Healthcare IT news. [Online], Available at: <https://www.healthcareit.com.au/article/healthcare-leads-data-breaches-security-issues-report-finds>

Ehrenfeld, J.M., 2017. Wannacry, cybersecurity and health information technology: A time to act. *Journal of medical systems*, *41*(7), p.104.

Isaac, S. & Michael, W. B., 1995, Handbook in Research and Evaluation, 3rd Ed., Edits Publishers, San Diego, California, USA.

Jalali, M.S., Razak, S., Gordon, W., Perakslis, E. and Madnick, S., 2019. Health care and cybersecurity: bibliometric analysis of the literature. *Journal of medical Internet research*, *21*(2), p.e12644.

Kiresuk, T.J. and Lund, S.H., 1982. Goal attainment scaling: A medical-correctional application. *Med. & L.*, *1*, p.227.

Kiresuk, T.J., Smith, A. and Cardillo, J.E. eds., 2014. *Goal attainment scaling: Applications, theory, and measurement*. Psychology Press.

Livingstone, T., 2020. 9News. [Online] Available at: <https://www.9news.com.au/national/cyber-attacks-australia-sixth-most-hacked-country-in-world-new-data-reveals/4a762e06-9342-4c8a-a7af-1632a1d1042a>

Love, A. J., 1991, *Internal Evaluation: Building Organizations from Within*, Sage Publications, Newbury Park, USA.

News.ambest.com. 2019. *Going Dark*. [online]
Available at:
<http://news.ambest.com/ArticleContent.aspx?pc=1009&altsrc=158&refnum=285596>

OAIC. 2021. *Notifiable Data Breaches Report: January–June 2020*. [online] Available at: <https://www.oaic.gov.au/privacy/notifiable-data-breaches/notifiable-data-breaches-statistics/notifiable-data-breaches-report-january-june-2020/#malicious-or-criminal-attack-breaches-top-five-industry-sectors.>

Offner, K.L., Sitnikova, E., Joiner, K. and MacIntyre, C.R., 2020. Towards understanding cybersecurity capability in Australian healthcare organisations: a systematic review of recent trends, threats and mitigation. *Intelligence and National Security*, *35*(4), pp.556-585.

Owen, J. M., 1993, *Program Evaluation: Forms and Approaches*, Allen & Unwin, NSW, Australia.

Pattinson, M.R., 2001. *Evaluating Information System Security: An Application of Goal Attainment Scaling* (Doctoral dissertation, Flinders University of South Australia, School of Commerce).

Towell, R., 2016. *Fears that patients' personal medical information has been leaked in Medicare data breach*. [online] The Sydney Morning Herald. Available at: <https://www.smh.com.au/public-service/privacy-watchdog-called-after-health-department-data-breach-20160929-grr2m1.html.>