Security Assurance Modelling of Security Incident in Healthcare using the Generic Security Template (GST)

Ying He (ying.he@dmu.ac.uk)
"De Montfort University" https://orcid.org/0000-0003-2023-5547
Cunjin Luo
University of Essex

Research article

Keywords: Security Assurance Modelling, Generic Security Template (GST), Security Incident, Healthcare Organization

Posted Date: April 14th, 2020

DOI: https://doi.org/10.21203/rs.3.rs-21578/v1

RESEARCH

Security Assurance Modelling of Security Incident in Healthcare using the Generic Security Template (GST)

Ying He[1] and Cunjin Luo[2,3*]

*Correspondence: cunjin.luo@essex.ac.uk
[2]School of Computer Science and Electronic Engineering, University of Essex, Colchester, UK
[3]Key Lab of Medical Electrophysiology, Ministry of Education, Institute of Cardiovascular Research, Southwest Medical University, Luzhou, China
Full list of author information is available at the end of the article

Abstract

Background: The recent industry reports show that the number of security incidents in healthcare sector is still increasing, especially the high severity incident, such as data leakage incident and ransomware, which can lead to significant impact on healthcare services. It is imperative for the organizations to learn lessons from those incidents. Traditional ways to disseminate lessons learned are based on text approach, the linear format of which can obscure relationships among concepts and discourage readers from integrating information across ideas. Graphical diagrams can serve this purpose, as it can communicate both individual elements of information and relationships between them.

Methods: The Generic Security Template (GST) has been proposed to support the exchange of lessons learned from security incidents. It utilises graphical notations to communicate both individual elements of information and relationships between them. This paper conducts a case study by adopting the GST to capture and structure the incident information of a data leakage incident in a UK healthcare organization in order to facilitate incident exchange.

Results: The results show that, the GST was able to visualize and depict the key elements, including lessons learned, the associated security requirements and organizational contextual information identified from the selected data leakage incident case study from NHS. GST provides a unified way to communicate incident information.

Conclusions: This research has significance for the healthcare organizations to improve their incident learning practices. It fosters an environment where different stakeholders can speak the same language while exchanging the lessons learned from the security incidents. Future work will consider applying the GST to analyse other complex security incidents such as the advanced persistent threats (APTs) in healthcare organizations and extend the use of the GST in other industries.

Keywords: Security Assurance Modelling; Generic Security Template (GST); Security Incident; Healthcare Organization

Background

Security incidents happened in healthcare organizations across the world such as Veterans Affairs' data leakage incidents [1, 2] in North American and Hospital's data leakage incident [3] in China. However, those incidents are just the tip of iceberg. Industry reports show that the number of incidents in healthcare organization is still increasing. Symantec reports that the healthcare attacks accounts for 18% across all sectors and continues to grow about 10% each year [4]. Existing work has

confirmed the patients' and public's worries about the security risks associated with their medical records [5, 6] and the use of healthcare related technologies[7, 8].

Security incidents can cause significant financial loss to healthcare organizations. Healthcare organizations can be fined if they fail to protect patients' personal information. For instance, the healthcare organizations in UK were fined hundreds of thousands pounds following data breaches affecting thousands of patients and staff [9, 10]. There is good research effort in protecting the healthcare systems, such as security and privacy risk assessment frameworks [11], secure authentication protocols [12], security modelling [13], secure access systems [14] and medical device security protection [15], however, the same security incidents still occur. It is imperative for the healthcare organizations to learn lessons from those incidents [16, 17, 18] and take actions to prevent recurrence.

The European General Data Protection Regulation [19] comes with a strict data protection compliance regime that organizations can be fined fined up to £20 million, or 4% of the organisation's annual turnover, whichever is higher, in the case of severe data breaches and failure to report data breach involving sensitive information to the supervisory authority. Organizations are under a legal obligation to strengthen their security mechanisms to prevent incidents. The UK has launched the Cyber Security Information Sharing Partnership (CISP) to help exchange information on threats and vulnerabilities in real time [10]. There is a need to promote incident lessons learned exchange by providing the capability to analyse and redistribute the lessons learned effectively [10].

A key activity in the incident (i.e. adverse event) response process is the capacity to learn from the errors or mistakes made throughout the incident handling process, to learn about the effectiveness of security policies, procedures, technical processes and to feed this knowledge back into the information security management process [20, 21]. Current research has realised the importance to learn from past security incidents [22, 23, 24].

Traditional ways to disseminate information about an incident include a series of formal reports, emails, newsletters, meetings and presentations to management [20, 21]. These contain less information comparing to the formal post-incident reports. Post-incident reports document information obtained throughout the security incident investigation process. Examples include the VA data leakage incidents [1, 2] from the US, and the NHS IT Asset disposal incident [25] and Ransomware incident [26] from UK. They provide a reference that can be used to assist in handling similar incidents [21]. Contents include the causes of the incident, the recommendations on remediation, the security requirements violated and improvements on procedures. Although this information is related, details can be scattered throughout a report. This makes it difficult for readers to understand how the security solutions are brought together to support different security requirements [27]. This problem has been compounded by usually lengthy written security incident reports, which can be hundred of pages. There is a need for the conversion of the textual information into a learning document, which can easily communicate security lessons [22]. Traditional ways to disseminate lessons learned are based on text approach. The linear format of a text can obscure relationships among concepts and discourage readers from integrating information across ideas [28]. Graphical diagrams can serve

this purpose, as it can communicate both individual elements of information and relationships between them.

The motivation of this paper is to adopt the Generic Security Template (GST) [29], an evidence-based security assurance modelling approach, to capture and visualize the findings of a data leakage incident in order to support the exchange of the lessons learned. GST is graphical notation that has extended the application of the Goal Structuring Notation (GSN) [30], which is an evidence-based safety assurance modelling approach that links the findings from the adverse event to support the security requirements. The GST provides a unified way to communicate adverse event information [27]. However, it has not been used in a healthcare context in UK. This paper makes the following contributions:

1 Adopts the GST to capture and structure the findings of a data leakage incident to support lessons learned exchange.
2 Evaluates the GST in a UK Healthcare Context for the first time in the literature.
3 Presents the success criteria and insight into current practices in the lessons learned exchange of incidents in healthcare context.

The remainder of this paper is structured as follows. The Methods section introduces the Generic Security Template (GST) and the selection of the case study. The Results section presents the results of the case study on the adoption of the GST to visualize a data leakage incident in NHS. The Discussion section compares with existing research, presents insight and recommendations into current practices in the exchange of security lessons learned in healthcare and the success criteria. The last section concludes the research and outlines future work.

Methods

This section presents a case study on applying a security assurance modelling approach, the Generic Security Template (GST), to structure the key lessons learned and findings from an enquiry into an NHS data leakage incident. The GST will be used to visualize and capture the key elements, including lessons learned as well as the associated security requirements and organizational contextual information in order to facilitate the exchange of the lessons learned from the security incident.

The Generic Security Template (GST)

The *Generic Security Template (GST)* is defined as "a documented body of lessons learned identified from a security incident that can support the security requirements of the organization" [29]. A *security incident* is defined as "a violation or imminent threat of violation of security policies, acceptable use policies, or standard security practices" [29]. *Lessons learned*, are defined as the knowledge obtained from experience. It refers to (1) security causes of a security incident and (2) security solution to avoid the recurrence of similar incidents. *Security requirements*, are usually in the form of a set of security standards or guidelines that the organization is currently applying. The GST is an evidence-based security assurance modelling approach that links the findings from the incident to support the security requirements.

The GST follows the security assurance model [31, 32]. Figure 1 presents a workflow chart on how the assurance modelling framework connects lessons learned with

security requirements. The framework starts with top level security requirements. It is then decomposed into three directions, which are "Further requirements needed", "Supporting solutions needed" and "Security arguments needed", which will be further elaborated. "Further requirements needed" is elaborated with different levels of security requirements derived from the security policies/standards/guidelines. This process completes when it reaches the level that all further requirements of the security policies/standards/guidelines are added to this model. "Supporting solutions needed" is elaborated with the security lessons learned derived from the security incidents. The lessons learned that were not covered by the security standards can be added to the framework. These added lessons learned can compliment the existing security policies/standards/guidelines. Some of the lessons learned might conflict with existing policies/standards/guidelines, then an argument needs to be developed to deal with the conflictions. This process completes when all the lessons learned are added to this model. "Security arguments needed" typical deal with the conflict between the lessons learned and the existing policies/standards/guidelines. The stakeholder's reviews towards the security incidents and the security policies/standards/guidelines can also be documented here. This feedback can also enrich the security policies/standards/guidelines in the organizations. This process completes when all the arguments development have been added to this model. The security assurance model captures security requirements, lessons learned as well as the stakeholders reviews of the incident. The GST adopted the security assurance model through linking the analysis of an incident to specific security standards or guidelines that help to implement particular solutions. GST is intended to be applicable across different classes of organization and not specifically to the place where an incident occurred.

Figure 1 Security Assurance Model Workflow [31, 32]. Figure 1 presents a work-flow chart on how the assurance modelling framework connects lessons learned with security requirements.

GST is an adaption of the Goal Structuring Notation (GSN), which was developed in the early 1990s [30]. GSN has been widely used in the UK defence sector in order to present argument by creating graphical structure between goals, subgoals, evidence/solutions, strategies and contexts [33]. GST syntactic components to document *Lessons learned*, *Security requirements*, *Strategies* and *Context*. The *Goal* component captures statements of the system security. It is usually in the form of a security requirement from security standards or guidelines. For example, "NHS Surrey IT System is acceptably secure". The *Lessons learned* component captures security causes and solutions, for example, "Sensitive Data" is the security cause, and the solution is "Should wipe medical and sensitive information before sending for disposal". The *Strategies* component is inserted between the *Goals* and *Lessons learned*, capturing the explanation on how the top-level goal is addressed by the aggregation of the goals or lessons learned presented at the lower level. *Context* is used to provide supplementary information such as the explanation of a concept. The four principal components of the GST are shown in Figure 2. Figure 3 shows how the four principal components are related to each other to present security arguments to support the goal and sub goals with necessary evidence and contextual information.

Figure 2 Principal Components of GST Notations [29]. Figure 2 presents the principal components of GST notations.

Figure 3 Evidence based Security Assurance Modelling. Figure 3 presents the evidence based security assurance modelling framework.

Below are the detailed step by step explanation to apply the GTS to structure and visualize the security incident,

Step1: Build the goal structure. The top goal is always to state the system is secure. It is then decomposed into lower level goals that usually appear in the form of security requirements of security standards or guidelines that are currently applied by the organization. This decomposition continues until reaching the level, where the goals can be directly supported by the lessons learned in a security incident report.

Step 2: Derive the lessons learned from the security incident. Lessons learned can be derived by looking for the security causes and solutions from the security incident report. The level of abstraction has not been defined and the users are advised to define their own level of abstraction according to individual business requirements. These were then added to the GST using a structured textual format. The security causes should be in the form of <Noun-Phrase>. The solutions are in the form of <Verb-Phrase><Noun-Phrase>.

Step 3: Connect lessons learned to the goal structure. The lessons learned identified from step 2 usually contains different level of details that will be mapped to goals at different levels in the goal structure. The analysts are required to identify the relationships between the lessons and the goals using a bottom-up approach [30]. There are circumstances that the lessons learned are not suitable to map to any existing goals. They will be mapped to a newly created goal named "Standard non-existent" which is linked to the top goal. This is usually due to a missing security requirement, meaning the organization may need to consider adding new security requirements to their currently applied security standards or guidelines.

Step 4: Specify Context and Strategy. The Strategy notation captures the methods and justification of the goal decomposition. It is positioned between the goals and sub-goals. The Strategy should be described in the form of "argument by <approach>", "argument over <approach>", "argument using <approach>", "argument of <approach>". The Context notation captures supplementary information such as an explanation of a concept. It can be described in the form of free text.

The Case Selection

In UK, information about security incidents can be found from Information Commissioner's Office (ICO). A good number of those incidents are from healthcare organizations. We selected the NHS Surrey IT Asset Disposal Incident [25] because it has a detailed money penalty report that documents the causes, recommendations and violated security requirements. Incident description in the incident report is semi-structured text. This allows us to model security incident from a different resource rather than news clips and security incident reports that have been studied

before [27]. This case study will follow the fours steps outlined in Generic Security Template subsection.

Here is a brief description of the selected case "The Information Commissioner's Office (ICO) has issued NHS Surrey with a monetary penalty of £200,000 after more than 3,000 patient records were found on a second hand computer bought through an online auction site. The sensitive information was inadvertently left on the computer and sold by a data destruction company employed by NHS Surrey since March 2010 to wipe and destroy their old computer equipment. The company carried out the service for free, with an agreement that they could sell any salvageable materials after the hard drives had been securely destroyed. The ICO's investigation found that NHS Surrey had no contract in place with their new provider, which clearly explained the provider's legal requirements under the Data Protection Act, and failed to observe and monitor the data destruction process." [34].

Results

This section reports the results of the visualisation of the key lessons learned and findings from an enquiry into an NHS data leakage incident using the security assurance modelling approach, the Generic Security Template (GST). It follows the fours steps outlined in the Methods section about the GST.

Step 1: Build the goal structure. The Information Commissioner's Office (ICO) provided the IT asset disposal guideline [35], which is part of a series of guidance, but with more details compared to the main Data Protection Act (DPA) regarding data protection. It aims to promote good practices and assist the data controller to better understand their responsibility. It provides instructions to the data controller regarding what need to be considered when disposing IT equipment that may contain personal private information. We use this guideline as the goal structure for this incident study. The top goal is always to state the system is secure. In this case, it is stated as"NHS Surrey IT Asset is acceptably secure". It is then decomposed into lower level goals that appear in the form of security requirements derived from IT asset disposal guideline [35]. An example is "An IT Asset Disposal Strategy has been created".

Step 2: Derive the lessons learned from the security incident. We follow the GST adoption instructions by searching for the lessons learned (security causes and solutions) from the security incident report. The lessons learned are listed in Table 1. The security causes should be in the form of <Noun-Phrase>. The solutions are in the form of <Verb-Phrase><Noun-Phrase>. These are then added to the GST using a structured textual format.

Table 1 NHS Surrey IT Asset Disposal Incident Lessons Learned

Security Causes	Security Solutions
Risk Assessment	Carry out a risk assessment when using a data processor to dispose the redundant drives.
Sensitive Data	Wipe medical and sensitive information before sending for disposal.
Disposal Contract	Have a written contract with the data processor.
Disposal Monitoring	Monitor the destruction process through keeping audit trails and checking inventory logs of the destroyed hard drives using the serial numbers in the destruction certificates for each drive.
Remedial Action	Develop a new policy framework to address the appropriate use of data for redundant equipment.

Step 3: Connect lessons learned to the goal structure. The lessons learned with different levels of details are mapped to the goals at different levels in the goal structure. The analyst is required to decide on the relationships between the goals and the lessons learned. In this case, four lessons learned were successfully mapped to the goal structure. There is one, "Remedial Action: develop a new policy framework and procedure to address the appropriate use of data disposal for redundant equipment", that is not covered by any existing goals. It is mapped to a newly created goal named "Guideline non-existent" which is linked to the top goal through a strategy. This is due to a missing security requirement in the IT asset disposal guideline [35], meaning the organization may need to consider adding a new security requirement to their currently applied IT asset disposal guideline.

Step 4: Specify Context and Strategy. The Strategy we used for the goal decomposition is described as "Argument over IT Asset Disposal Guideline". It is further explained by using a Context notation, stated as "An IT Asset Disposal guideline proposed by Information Commissioner's Office (ICO) according to Data Protection Act (DPA)". The strategy "Argument over All Missing Security Solutions" is added to the goal structure to link the lessons learned that is not covered or addressed by the IT asset disposal guideline [35].

Figure 4 presents the lessons learned and findings from the NHS Surrey 2013 IT Asset Disposal Incident. Five lessons learned are captured and connected to the goals (i.e. security requirements), which are "Risk Assessment", "Sensitive Data", "Disposal Contract", "Disposal Monitoring", and "Remedial Action". We are not able to identify a goal that can be mapped to "Remedial Action", which indicates there is probably a missing security requirement of the IT Asset Disposal guideline.

Figure 4 Visualisation of NHS Surrey IT Asset Disposal Incident. Figure 4 presents the visualisation of NHS Surrey IT Asset Disposal Incident.

This case study demonstrate the suitability of the GST in presenting the lessons learned from real world security incidents from healthcare organization in UK. The GST was able to capture the key elements, including lessons learned as well as the associated security requirements and organizational contextual information.

Discussion

Healthcare Incident Learning

Incident learning happens in the "follow-up" phase of the incident response process [21]. This information should feed relevant knowledge and changes into the security management process to inform the creation of further reference material on how to respond to similar incidents [21, 36, 37]. In particular, such activities feed information back to the "preparedness" phase to determine if additional tools, increased security budgets, improved training programs and alterations to the incident response procedures are required.

There are legislative requirements to report and exchange security incidents. This is to facilitate the sharing of the security incidents with different organisations so that lessons can be learned and the same incidents can be prevented [38, 39]. Organizations can be fines up to £20 million, or 4% of the organization's annual turnover,

whichever is higher according to the General Data Protection Regulation (GDPR) if they failed to prevent a severe data incident or failed to report a personal data breach to the supervisory authority. Another important step is the proposed Cyber Security Strategy [19]. The National Health Service (NHS) in UK is required to report serious incidents to the NHS Business Service Authority (BSA). In the US, the security incidents in healthcare are reported to the Health Information Sharing and Analysis Center (H-ISAC). In China, there has not been any legislative requirement although some good efforts made in protecting patients' data [40]. However, the main reason is the lack of motivations to protect patient data as a result of the traditional Chinese culture and immaturity of healthcare systems in China, that are likely to trigger privacy violation [41]. There is a need to promote incident lessons learned exchanging by providing the ability to analyse and redistribute this knowledge effectively [10], which can ultimately strengthen cyber security knowledge, skills and capability in healthcare organizations.

Lessons Learned Sharing

Incident dissemination is enacted through a series of formal reports, informal meetings, emails, newsletters, and presentations to management [20, 21]. Meetings are held and communicative notes are gathered to address responses, disagreements, suggestions and additions to security policies and the incident procedures [20]. Issues to document include an estimation of the damage caused, actions taken during the incident, policies and procedures that require an update and any electronic evidence that can be used for pursuing those responsible [22]. Comparing to the formal incident report, emails, newsletters, meetings and presentations to management contain less information than the post-incident report. They are usually presented in a free-style way and less information are provided to communicate the lessons learned to inform improvements of the security management processes.

There is usually a formal post-incident report produced after the security incident to document findings throughout the incident response process. Information contained in the report is typically classified into business impact and remediation information [20]. Business impact information involves how the incident is affecting the organization in terms of mission impact, financial impact, etc. Many organizations do not want to share business impact information with outside companies unless there is clear value proposition or formal reporting requirements [42, 43]. When sharing information with peers and partner organizations, incident response teams should focus on exchanging remediation information [20]. This information is inter-related, however, it is scattered throughout a report. This issue has been compounded in lengthy security incident reports [2]. Stakeholders responsible for protecting patient data lack the time and the motivation to spend the many hours needed to read and digest existing reports [27]. This creates significant problems within the wider scope of security management systems. It can be difficult to accurately assess the likelihood or consequences of future attacks when managers are unaware of previous incidents.

Lessons Learned Sharing using Diagrams

Traditional ways to disseminate lessons learned are based on textual description. The linear format of a text can discourage readers from obtaining comprehensive understanding of relationships among ideas across paragraphs due to working memory

limitations [44]. Graphical diagrams can serve this purpose, as it can communicate not only individual elements of information but also relationships among those elements. Empirical case studies [22, 27] have identified the difficulties when text was the only medium available for communicating security lessons. Similar difficulties were identified in safety area, when text was the only approach for expressing complex safety arguments [45]. The free-style text is considered to be unclear and not well structured, the meaning of the text, and therefore the structure of the safety argument, can be ambiguous and unclear [30]. The use of free text makes is difficult to ensure that all stakeholders share the same understanding of the argument [30]. Clear written communication and the capability to process knowledge in an organised manner are essential skills in incident response teams [46]. The cyber security communities have realised the importance and believe that interactive visualisation systems can help improve security decision making in incident response [47, 48].

Implications for the IT and Healthcare Professionals.

This paper for the first time adopts the GST to structure and visualize the lesson learned from security incident happened in a healthcare organizations in UK. A key benefit of this approach is that their subjective reasoning is documented in the nodes of the Generic Security Template. A range of stakeholders can then check the resulting diagrams to determine when key lessons have been omitted or if additional work is required to support the exchange of security lessons. They could check the reasoning and experience can be borrowed from safety area on how to avoid and detecting fallacious reasoning in the arguments [30]. This can also help feedback into the organizations' risk assessment procedure as it usually requires the causal analysis of the incidents as well as the security recommendations to mitigate the risks [49, 50, 51, 52, 53]. The use of a graphical notation provides stakeholders with an overview of key issues before being forced to read the hundreds of pages of detailed prose that increasingly documents the findings of security investigations. The graphical visualisation contributes to addressing the current frustration faced by the IT and healthcare professional who do not have time to read the security incident report. It enables the lengthy written report to be more accessible and usable.

Through mapping lessons learned to security requirements, it allows the IT professionals in healthcare organizations to assess whether they have any missing security requirements. The incident information captured by the four principal components is mainly generic remediation information, which can serve the purpose of incident exchange without revealing business impact or sensitive information.

Success Criteria

The data sources of case studies can be diversified such as the official security incident reports used in the analysis of the VA incidents [1, 2], and the money penalty report used in the analysis of IT asset disposing incident [25]. Existing work suggests that the GST can be used to structure the security lessons identified from various data sources [27, 32, 54, 55], However, the following requirements have to be met in order to be successful.

Security requirements can be captured based on the existing security standards applied by the organization. As most healthcare organization adopted security standards/guideline. This should not be a challenge. This has been confirmed in the previous case studies [27, 32, 54, 55]. If the organizations did not apply any security standards/guidelines, security requirements have to be retrieved from the case descriptive materials.

Lessons learned can be derived from different data source. Although incident description comes from different data sources, lessons learned can be identified through using content analysis [56]. This can be achieved through relying on the security analyst's expertise or the use of existing content analysis techniques [57].

Lessons learned can be connected to the security requirements. This relies on the analyst's expertise and the validity of the guidance needs to be further evaluated in real practice. As the main purpose of the GST is to facilitate the exchange and communication of the security incidents, it allows the analysts to perform security arguments using the GST.

Context and Strategies can be captured and extracted from the incident description in the related documents. This has been confirmed in the current and previous case studies [27, 32, 54, 55].

Conclusions and Future Work

This paper for the first time adopts the evidence-based security assurance approach, the GST to structure and visualize the lesson learned from an data leakage incident happened in the healthcare organizations in UK. The GST was able to capture the key elements, including lessons learned together with the associated security requirements and organizational contextual information. The graphical visualisation contributes to addressing the current frustration faced by the IT and healthcare professional who do not have time to read the security incident report. It enables the lengthy written report to be more accessible and usable. It can also serve as a platform for the security analysts and stakeholders to formulate security arguments, which is an important component in cyber security management [58].

This research has significance for the healthcare organizations to improve their incident learning practices. It fosters an environment where different stakeholders can speak the same language while exchanging the lessons learned. In the future, we look to apply the GST to analyse other complex security incidents such as the Ransomware attack in the NHS [26] and advanced persistent threats (APTs) in healthcare organizations. APTs are usually complicated and documented using lengthy reports following the kill chain analysis logic [59]. We will elaborate the GST by considering the quantitative measurements on the level of confidence of the formulated security arguments as well as its accuracy. Future work will also look to evaluate GST in healthcare organizations in UK, bringing together the IT and healthcare professionals to work collaboratively to visualize the incident information and enhance the exchange of lessons learned from security incidents. We will ultimately extend the use of the GST in other industries such as finance, aviation, telecommunication and other security critical businesses.

Competing interests
We declare no conflict(s) of interest associated with this research.

Author's contributions
YH conceptualised this research. YH and CL selected the case study and analysed the case. The manuscript was written by YH and CL. All authors have read and approved the manuscript.

Funding
This research is funded by National Natural Science Foundation of China (NSFC) under Grant No. 61803318 (Cunjin Luo).

Availability of data and materials
All data generated or analyzed for this study are included in this manuscript.

Ethics approval and consent to participate
Not applicable.

Consent for publication
All authors agreed to publish this manuscript.

Acknowledgements
We would like to thank the anonymous reviewers for their insightful comments that helped improve the quality of the paper.

Author details
[1]School of Computer Science and Informatics, De Montfort University, Leicester, UK. [2]School of Computer Science and Electronic Engineering, University of Essex, Colchester, UK. [3]Key Lab of Medical Electrophysiology, Ministry of Education, Institute of Cardiovascular Research, Southwest Medical University, Luzhou, China.

References

1. Department of Veterans Affairs: Review of issues related to the loss of va information involving the identity of millions of veterans. Technical report (2006)
2. Department of Veterans Affairs: Administrative investigation loss of va information va medical center birmingham, al. Technical report (2007)
3. China Hospital Information Management Association (CHIMA): Report on China's Hospital Information Systems 2017/2018. https://www.useit.com.cn/forum.php?mod=viewthreadtid=20408. [online: accessed 10-Mar-2019] (2018)
4. Symantec Corporation: Cyber Security and Healthcare: An Evolving Understanding of Risk (2018)
5. Papoutsi, C., Reed, J.E., Marston, C., Lewis, R., Majeed, A., Bell, D.: Patient and public views about the security and privacy of electronic health records (ehrs) in the uk: results from a mixed methods study. BMC medical informatics and decision making **15**(1), 86 (2015)
6. Peikari, H.R., Ramayah, T., Shah, M.H., Lo, M.C.: Patients' perception of the information security management in health centers: the role of organizational and human factors. BMC medical informatics and decision making **18**(1), 102 (2018)
7. Meinert, E., Alturkistani, A., Brindley, D., Knight, P., Wells, G., de Pennington, N.: Weighing benefits and risks in aspects of security, privacy and adoption of technology in a value-based healthcare system. BMC medical informatics and decision making **18**(1), 1–4 (2018)
8. Henriksen, E., Burkow, T.M., Johnsen, E., Vognild, L.K.: Privacy and information security risks in a technology platform for home-based chronic disease rehabilitation and education. BMC medical informatics and decision making **13**(1), 85 (2013)
9. IT Governance UK: UK healthcare companies fined for data breaches caused by staff misconduct. https://www.itgovernance.co.uk/blog/uk-healthcare-companies-fined-for-databreaches-caused-by-staff-misconduct. [online: accessed 10-Mar-2019] (2019)
10. Information Commissioner's Office: Private health firm fined £200,000 after IVF patients' confidential conversations revealed online. https://ico.org.uk/about-the-ico/news-and-events/news-and-blogs/2017/02/private-health-firm-fined-200-000after-ivf-patients-confidentialconversations-revealed-online/. [online: accessed 10-Mar-2019] (2017)
11. Yasqoob, T., Abbas, H., Shafqat, N.: Integrated security, safety, and privacy risk assessment framework for medical devices. IEEE journal of biomedical and health informatics (2019)
12. Das, A.K., Wazid, M., Kumar, N., Khan, M.K., Choo, K.-K.R., Park, Y.: Design of secure and lightweight authentication protocol for wearable devices environment. IEEE journal of biomedical and health informatics **22**(4), 1310–1322 (2017)
13. Rubio, Ó.J., Trigo, J.D., Alesanco, Á., Serrano, L., García, J.: Analysis of iso/ieee 11073 built-in security and its potential ihe-based extensibility. Journal of biomedical informatics **60**, 270–285 (2016)
14. Jones, K.H., Ford, D.V., Jones, C., Dsilva, R., Thompson, S., Brooks, C.J., Heaven, M.L., Thayer, D.S., McNerney, C.L., Lyons, R.A.: A case study of the secure anonymous information linkage (sail) gateway: a privacy-protecting remote access system for health-related research and evaluation. Journal of biomedical informatics **50**, 196–204 (2014)
15. Camara, C., Peris-Lopez, P., Tapiador, J.E.: Security and privacy issues in implantable medical devices: A comprehensive survey. Journal of biomedical informatics **55**, 272–289 (2015)
16. Kapoor, A., Kamis, A., Spil, T.A., Bozan, K.: Introduction to the minitrack on it adoption, diffusion and evaluation in healthcare. In: HICSS, p. 1 (2019)

17. Bozan, K., Datta, P.: Satisfaction with health informatics system characteristics and their effect on openness to frequent use. In: Contemporary Consumer Health Informatics, pp. 125–152. Springer, ??? (2016)
18. Bozan, K., Berger, A.: The effect of unmet expectations of information quality on post-acceptance workarounds among healthcare providers. In: Proceedings of the 51st Hawaii International Conference on System Sciences (HICSS) (2018)
19. Voigt, P., Von dem Bussche, A.: The eu general data protection regulation (gdpr). A Practical Guide, 1st Ed., Cham: Springer International Publishing (2017)
20. Northcutt, S.: Computer Security Incident Handling: Step by Step, a Survival Guide for Computer Security Incident Handling. Sans Institute, ??? (2001)
21. Cichonski, P., Millar, T., Grance, T., Scarfone, K.: Computer security incident handling guide. NIST Special Publication **800**(61), 1–147 (2012)
22. Ahmad, A., Hadgkiss, J., Ruighaver, A.B.: Incident response teams–challenges in supporting the organisational security function. Computers & Security **31**(5), 643–652 (2012)
23. Grispos, G., Glisson, W.B., Storer, T.: Rethinking security incident response: The integration of agile principles. In: 20th Americas Conference on Information Systems (AMCIS 2014)
24. Ahmad, A., Maynard, S.B., Shanks, G.: A case analysis of information systems and security incident responses. International Journal of Information Management **35**(6), 717–723 (2015)
25. Information Commissioner's Office: NHS Surrey c/o department of health regional legacy management team, Data Protection Act 1998 monetary penalty notice. http://breachwatch.com/wp-content/uploads/2013/07/nhs-surrey-monetary-penalty-notice.pdf. [online: accessed 10-Mar-2019] (2013)
26. Thomas, J., Galligher, G.: Improving backup system evaluations in information security risk assessments to combat ransomware. Computer and Information Science **11**(1) (2018)
27. He, Y., Johnson, C.: Generic security cases for information system security in healthcare systems. IET, ??? (2012)
28. Robinson, D.H., Kiewra, K.A.: Visual argument: Graphic organizers are superior to outlines in improving learning from text. Journal of educational psychology **87**(3), 455 (1995)
29. He, Y., Johnson, C., Renaud, K., Lu, Y., Jebriel, S.: An empirical study on the use of the generic security template for structuring the lessons from information security incidents. In: 2014 6th International Conference on Computer Science and Information Technology (CSIT), pp. 178–188 (2014). IEEE
30. Kelly, T.P.: Arguing safety: a systematic approach to managing safety cases. PhD thesis, University of York York, UK (1999)
31. He, Y., Johnson, C.: Challenges of information security incident learning: An industrial case study in a chinese healthcare organization. Informatics for Health and Social Care **42**(4), 393–408 (2017)
32. He, Y., Johnson, C.: Improving the redistribution of the security lessons in healthcare: An evaluation of the generic security template. International Journal of Medical Informatics **84**(11), 941–949 (2015)
33. Kelly, T.: A systematic approach to safety case management. Technical report, SAE Technical Paper (2004)
34. Information Commissioner's Office: ICO fines NHS Surrey for failing to check the destruction of old computers. https://www.databreaches.net/ico-fines-nhs-surrey-for-failing-tocheck-the-destruction-of-old-computers/. [online: accessed 10-Mar-2019] (2013)
35. Information Commissioner's Office: IT asset disposal for organisations - Data Protection Act
36. Grispos, G., Glisson, W.B., Storer, T.: Enhancing security incident response follow-up efforts with lightweight agile retrospectives. Digital Investigation **22**, 62–73 (2017)
37. Grispos, G., Glisson, W.B., Storer, T.: Security incident response criteria: A practitioner's perspective. In: Proceedings of the 21st Americas Conference on Information Systems (AMCIS 2015) (2015). AIS
38. Mayer, E., Flott, K., Callahan, R., Darzi, A.: National reporting and learning system research and development (2016)
39. Agency, N.P.S.: National framework for reporting and learning from serious incidents requiring investigation. NPSA London (2010)
40. Wei, M., Xue-guo, X.: Discussion of patients' confidentiality in sharing electric medical records. Soft Science of Health **3**, 034 (2009)
41. Gao, X., Xu, J., Sorwar, G., Croll, P.: Implementation of e-health record systems and e-medical record systems in china. The International Technology Management Review **3**(2), 127–139 (2013)
42. Zhao, W., White, G.: An evolution roadmap for community cyber security information sharing maturity model. In: Proceedings of the 50th Hawaii International Conference on System Sciences (HICSS) (2017)
43. Spears, J.L., San Nicolas-Rocca, T.: Information security capacity building in community-based organizations: Examining the effects of knowledge transfer. In: 2016 49th Hawaii International Conference on System Sciences (HICSS), pp. 4011–4020 (2016). IEEE
44. Daneman, M., Carpenter, P.A.: Individual differences in working memory and reading. Journal of verbal learning and verbal behavior **19**(4), 450–466 (1980)
45. Johnson, C.W.: Proving properties of accidents. Reliability Engineering & System Safety **67**(2), 175–191 (2000)
46. McLaughlin, M.-D., DArcy, J., Cram, W.A., Gogan, J.: Capabilities and skill configurations of information security incident responders. In: Proceedings of the 50th Hawaii International Conference on System Sciences (HICSS) (2017)
47. Becker, J., Heddier, M., Öksüz, A., Knackstedt, R.: The effect of providing visualizations in privacy policies on trust in data privacy and security. In: 2014 47th Hawaii International Conference on System Sciences (HICSS), pp. 3224–3233 (2014). IEEE
48. Ebert, D.S., Ertl, T., Gaither, K.: Introduction to visualization and analytics for decision support, operational management, and scientific discovery minitrack. In: 2014 47th Hawaii International Conference on System Sciences (HICSS), pp. 1353–1353 (2014). IEEE
49. Lopez, D., Pastor, O., Villalba, L.J.G.: Data model extension for security event notification with dynamic risk assessment purpose. Science China Information Sciences **56**(11), 1–9 (2013)

50. Li, S., Bi, F., Chen, W., Miao, X., Liu, J., Tang, C.: An improved information security risk assessments method for cyber-physical-social computing and networking. IEEE Access **6**, 10311–10319 (2018)
51. Li, X., Li, H.: A visual analysis of research on information security risk by using citespace. IEEE Access **6**, 63243–63257 (2018)
52. Evans, M., He, Y., Luo, C., Yevseyeva, I., Janicke, H., Maglaras, L.A.: Employee perspective on information security related human error in healthcare: Proactive use of is-chec in questionnaire form. IEEE Access **7**, 102087–102101 (2019)
53. Evans, M., He, Y., Luo, C., Yevseyeva, I., Janicke, H., Zamani, E., Maglaras, L.A.: Real-time information security incident management: a case study using the is-chec technique. IEEE Access **7**, 142147–142175 (2019)
54. He, Y., Johnson, C., Lu, Y., Lin, Y.: Improving the information security management: An industrial study in the privacy of electronic patient records. In: 2014 IEEE 27th International Symposium on Computer-Based Medical Systems, pp. 525–526 (2014). IEEE
55. He, Y., Johnson, C., Evangelopoulou, M., Lin, Z.-S.: Diagraming approach to structure the security lessons: Evaluation using cognitive dimensions. In: International Conference on Trust and Trustworthy Computing, pp. 216–217 (2014). Springer
56. Hsieh, H.-F., Shannon, S.E.: Three approaches to qualitative content analysis. Qualitative health research **15**(9), 1277–1288 (2005)
57. Krippendorff, K.: Content Analysis: An Introduction to Its Methodology. Sage publications, ??? (2018)
58. Shen, C., Zhang, H., Feng, D., Cao, Z., Huang, J.: Survey of information security. Science in China Series F: Information Sciences **50**(3), 273–298 (2007)
59. Wen, S., He, N., Yan, H.: Detecting and predicting apt based on the study of cyber kill chain with hierarchical knowledge reasoning. In: Proceedings of the 2017 VI International Conference on Network, Communication and Computing, pp. 115–119 (2017). ACM

Figures

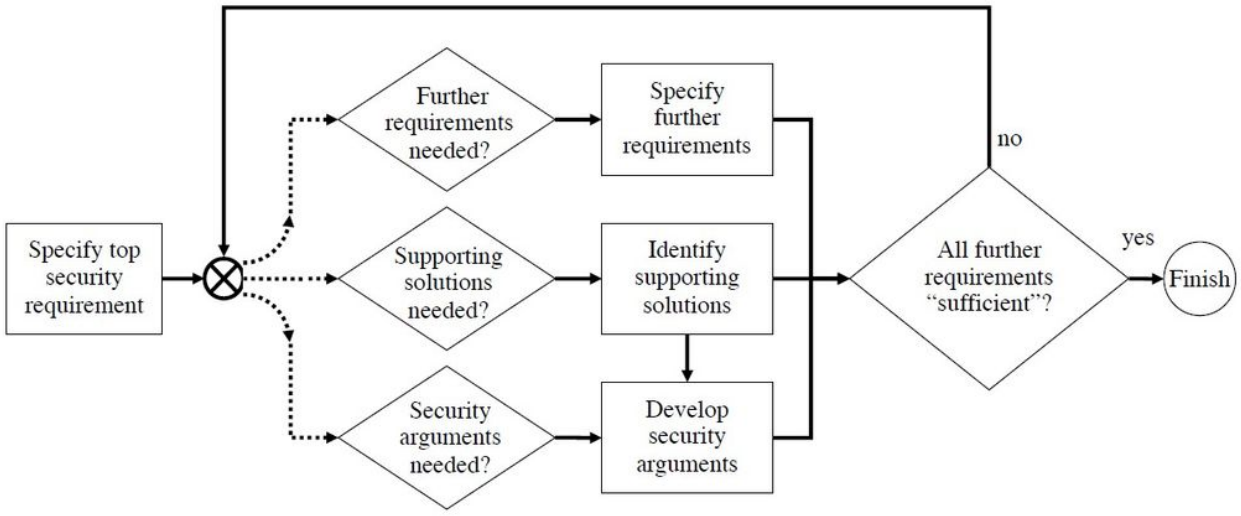

Figure 1

Security Assurance Model Workflow.

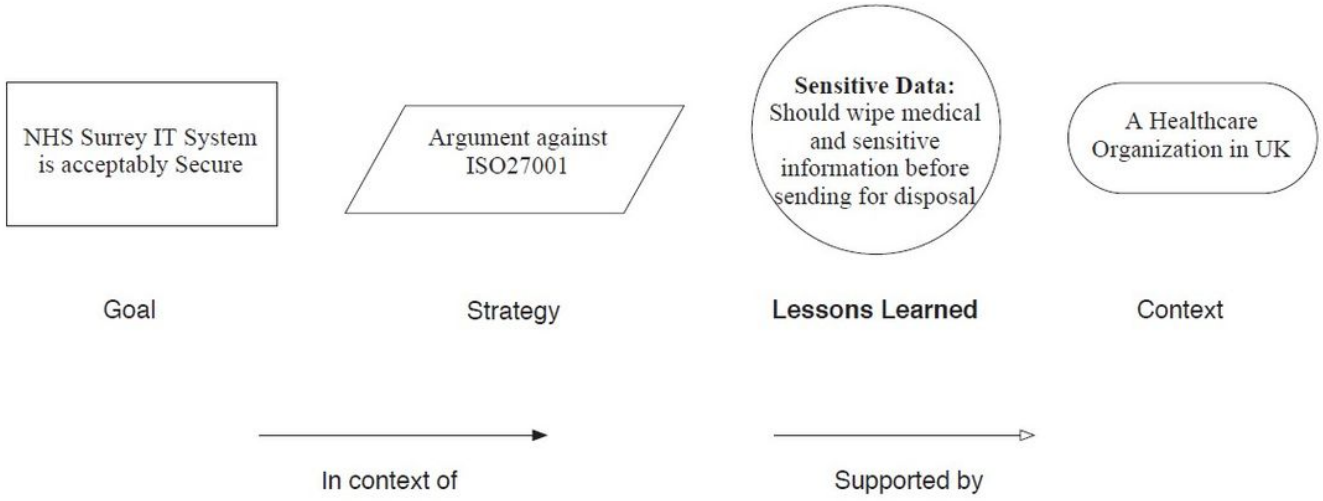

Figure 2

Principal Components of GST Notations.

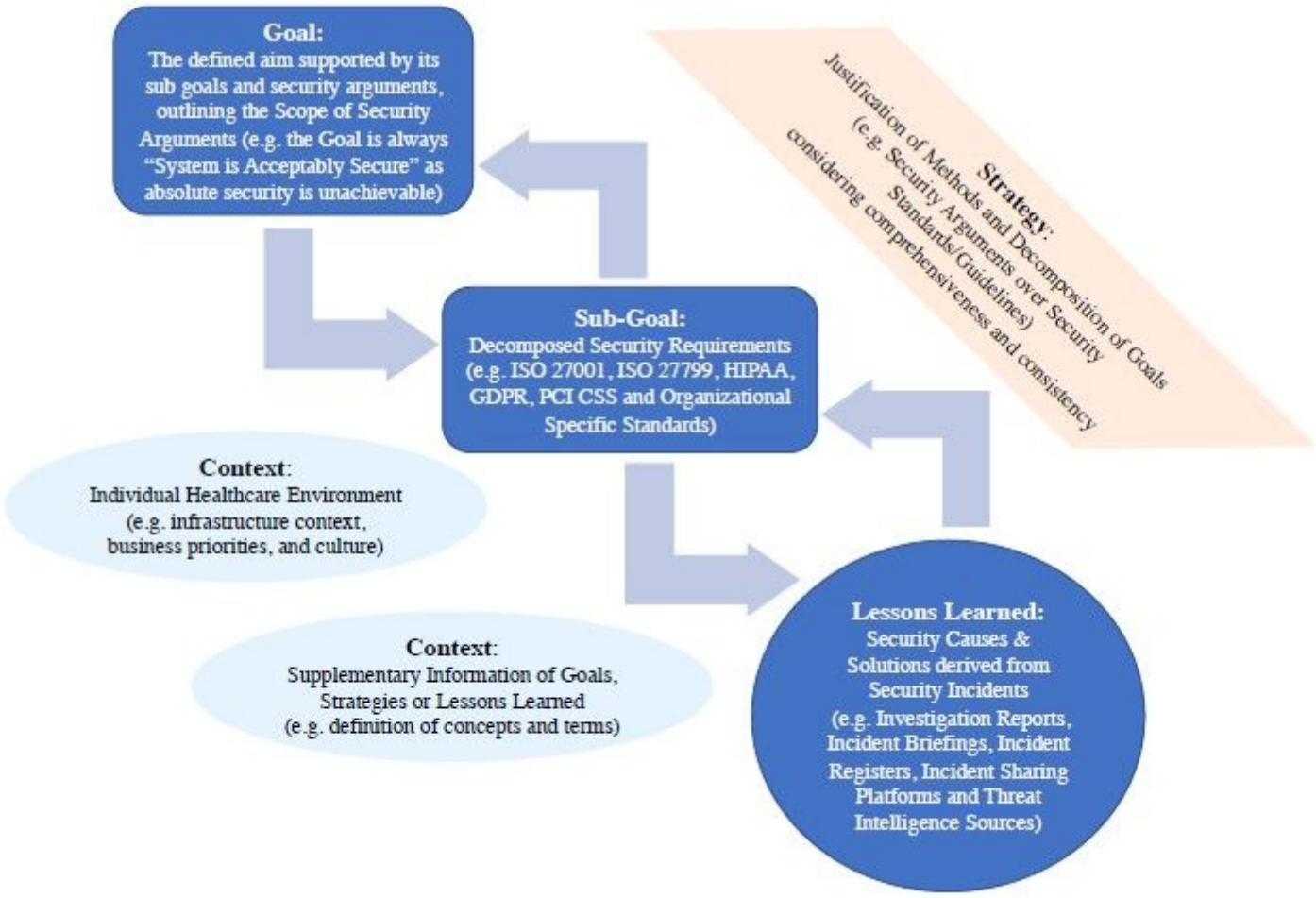

Figure 3

Evidence based Security Assurance Modelling

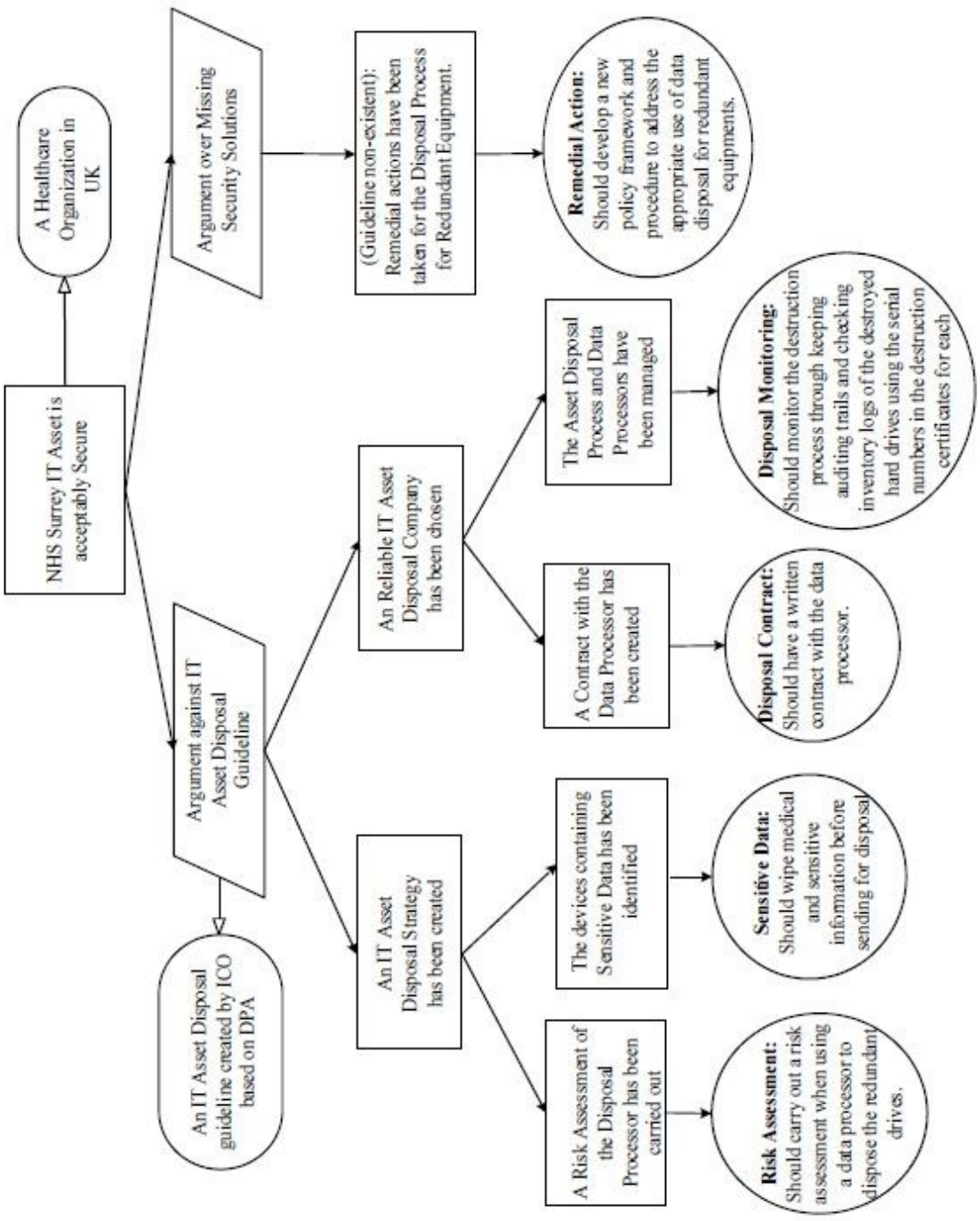

Figure 4

Visualisation of NHS Surrey IT Asset Disposal Incident