An Ontology for Effective Security Incident Management

Sabarathinam Chockalingam[1] and Clara Maathuis[2]
[1]Institute for Energy Technology, Halden, Norway.
[2]Open University of the Netherlands, Heerlen, The Netherlands.
Sabarathinam.Chockalingam@ife.no
clara.maathuis@ou.nl

Abstract: With the evolution of technologies like Internet of Things (IoTs), there will be more and more connected devices in use around the world. This is one of the reasons why cyber security is critical to contemporary society as it makes the large majority susceptible to cyber-attacks. Such cyber-attacks not only impact confidentiality, integrity, and availability but also can cause physical damage. This is evident from cyber-attacks like Stuxnet and German steel mill. Effective security incident management plays an important role in minimising negative impact of such attacks mainly in terms of the organizations' finance, reputation, and personnel safety. Typically, the main phases of security incident management include: (i) preparation, (ii) mid-incident, and (iv) post-incident. There are diverse set of concepts like Structured Threat Information Expression (STIX) and Incident Object Description Exchange Format (IODEF) in the above-mentioned phases of security incident management. However, a comprehensive overview of different concepts and the relationships between such concepts in security incident management is missing. In this paper, we develop an ontology model with relevant concepts and their corresponding relationships between them especially in the mid-incident and post-incident phases of security incident management. Furthermore, we demonstrate the proposed ontology model using colonial pipeline example case study. The proposed model will help incident responders to operationalise concepts, by having a clear understanding on different concepts and their corresponding relationships, which in turn would also make the incident response more effective in practice.

Keywords: Cyber incident recovery, Cyber security, Incident response, Ontology, Security incident management

1. Introduction

There will be more and more connected devices in use around the world with the evolution of technologies like Internet of Things (IoTs). Furthermore, with the emergence of remote working, people and critical systems in organizations are increasingly connected through the internet. At the same time, there is an increased rate of cyber-attacks during this Covid-19 pandemic (Lallie et al, 2021). Some of the well-known cyber-attacks include Brno university hospital cyber-attack (Pranggono et al, 2020), colonial pipeline ransomware attack (TechTarget, 2021) during this period. Such cyber-attacks may have different types of harms including physical or digital, economical, psychological, reputational, and societal (Agrafiotis et al, 2018).

Effective cyber security incident management plays a crucial role in reducing the dire consequences of cyber-attacks (Kulikova et al, 2012) especially in terms of the above-mentioned types of harms. There are four main phases of NIST incident response lifecycle: (i) preparation, (ii) detection and analysis, (iii) containment, eradication, and recovery, and (iv) post-incident activity. (Cichonski et al, 2012) also list relevant information/concepts corresponding to each phase of NIST incident response lifecycle. For instance, attack vectors, precursors, indicators, sources of precursors and indicators, incident analysis, incident documentation, and incident notification correspond to detection and analysis phase, whereas lessons learned, using collected incident data, and evidence retention corresponds to post-incident activity phase. Likewise, there are various globally accepted standards like Structured Threat Information Expression (STIX) and Incident Object Description Exchange Format (IODEF) in addition to concepts like contributory factors, and observations (test results) that are highlighted in other studies.

It is important for the incident responders to have an overview of relevant concepts which can aid an effective cyber security incident management in their organization. However, there is a lack of model that can provide a holistic overview of such concepts and their relationships. Ontologies have the capability to tackle this challenge especially based on their existing applications as it can help to represent, structure, and simulate the relevant concepts as classes and sub-classes in addition to labelling their relationships (Oltramari et al., 2015). Therefore, in this study, we will tackle the following research question (RQ): *"How can we develop an ontology model that*

provides a holistic overview of relevant concepts in security incident management?". In order to address this RQ, we will consider the following research objectives (ROs):
RO1. To review scientific literature in security incident management and identify relevant concepts.
RO2. To develop and evaluate an ontology model which provides the holistic overview of the identified relevant concepts and their relationships.

The main contributions of this paper are as follows:

1. we identify relevant concepts in security incident management from scientific literature.
2. we develop an approach to provide an overview of the identified concepts and their relationships.
3. we demonstrate the proposed approach using an example case study.

The remainder of this paper is structured as follows: In Section 2, we describe the research method followed by the review of literature on security incident management especially covering the mid-incident and post-incident phases in Section 3. We propose the security incident management ontology based on the considered requirements followed by the demonstration through colonial pipeline example incident in Section 4. Section 5 highlights the related work on ontologies followed by conclusions and future work directions in Section 6.

2. Method

With the aim of designing a model that captures the security incident management process while focusing on the mid-incident and post-incident phases, this research intends to answer the above-mentioned RQ. To answer it, an extensive literature review followed by a case study were conducted in a Design Science Research approach (Peffers, Tuunanen and Niehaves, 2018; Hevner, March, and Park, 2004) using the Methontology methodology (Fernández-López, Gómez-Pérez and Juristo, 1997). Hence, the following activities are taken:

Specification: the objective, requirements, and the necessary knowledge for developing the model are defined.

Knowledge Acquisition: the information required for building the model is gathered from sources extracted during the literature review and the case study on an ICS cyber incident. An extensive literature review is conducted based on the steps considered by (Okoli, 2015; Cooper et al, 2018). The aim of this literature search is to identify relevant scientific literature in security incident management especially the mid-incident and post-incident phases.

Conceptualization: the information collected is conceptualized in taxonomies with concepts, characteristics, and relations between the concepts. The adoption of ontology for the proposed model is due to its richness, robustness, explainable nature, and its spread use in diverse decision-making processes (Mavroeidis and Bromander, 2017).

Formalization: the architecture of the model is built, is depicted in Figure 1, and described in Section 4.

Integration: other relevant models found during the review process are considered in related work. The model proposed is designed from scratch with important aspects found during this process.

Implementation: the software environment i.e., Protégé is prepared to develop the model using OWL (Ontology Web Language), which is a well-known approach used by researchers and practitioners in this field. Furthermore, the model is implemented capturing the concepts, their attributes, and the relations between these concepts.

Maintenance: the implemented model is updated to make sure that further operations are possible.

Evaluation: the evaluation of the model is done adopting a two-step process: (i) by considering its structure and consistency, and (ii) through exemplification based on a case study conducted on an ICS cyber security incident.

Documentation: the documentation of the model is done considering the descriptions provided during the development process. This documentation is embedded in different sections of this paper.

3. Review on Security Incident Management

(Lee et al, 2018) proposed a model for security incident handling based on the survey of existing incident handling models. The proposed model consists of three components including monitoring, incident response, and forensics. They highlighted the three key phases within incident response: (i) detection and diagnosis, (ii) incident analysis and response, (iii) post-incident analysis. Finally, they also listed the main actions corresponding to each phase. The actions corresponding to detection and diagnosis are to: identify suspicious behaviour, analyse precursor and indicators, look for correlating information, perform preliminary impact assessment and determine potential damage to prioritize incident, and categorize the event and classify the security level. (Staves et al, 2020) developed a framework that help operators in incident response and recovery operations. The proposed framework consists of four different phases including: (i) planning, (ii) preparation, (iii) mid-incident, (iv) post-incident. They also listed main actions corresponding to each phase. (Shinde and Kulkarni, 2021) reviewed different incident management approaches. Furthermore, Shinde et al. proposed an incident management framework with primary components including alerts, logs and data, existing knowledge, policies, frameworks, and tools. Similar to Lee et al. and Staves et al., Shinde et al. highlighted the different phases of incident management and the important actions corresponding to each phase. (He, Inglut and Luo, 2022) et al. proposed a malware incident response lifecycle based on the NIST incident response lifecycle. In this work, they also tackled the different phases of incident management and the main actions related to each phase.

Even though the phases highlighted in these works differ, it can be categorized into three different phases: pre-incident, mid-incident, and post-incident. The focus of this paper is on mid-incident and post-incident phase as there are tools/methods that can be applied across different organisations unlike the pre-incident phase. Additionally, as a part of relevant actions, the following themes are identified in these two phases for extensive literature review which includes root cause analysis, information sharing, forensics, and lessons learned.

Root Cause Analysis: (Findrik et al, 2017) proposed a high-level architecture based on Evidential Networks (ENs) approach to help operators during the detection and analysis phase of security incident management to determine the root cause of an incident. The key components of the proposed architecture include: (i) detectors, (ii) reasoning engine, (iii) containment engine, and (iv) remedial actions. Detectors play a similar role to Intrusion Detection System (IDS) which takes data (example: network traffic) as input and generate an event (example: alarm in case of malicious behavior). However, on a holistic viewpoint considering both cyber and physical data from different systems, to detect a cyber-attack. The reasoning engine based on ENs consider the events generated from detectors and determine the control system state as compromised, erroneous, or normal. This would support operators in understanding what they are dealing against and aid containment engine to choose appropriate containment actions from the list of containment actions. (Chockalingam et al, 2018) developed a framework which would help to develop Bayesian Network (BN) models for distinguishing attacks and technical failures. These models would help operators during the detection and analysis phase of security incident management to determine the root cause of an incident (cyber-attack or technical failure). There are three different types of variables in the developed framework which includes: (i) contributory factors, (ii) problem, (iii) observations (or test results). (Chockalingam et al, 2021) developed a BN model for the problem of incorrect sensor measurements in the flood management domain based on the proposed framework for distinguishing attacks and technical failures.

(Chockalingam et al, 2019) proposed a framework which would help to develop BN models for determining the failure cause in case the considered problem is caused by a technical failure or attack vector when the considered problem is caused by an attack. These models would support operators during the detection and analysis phase of security incident management to determine the root cause of an incident (failure cause in case of a technical failure or attack vector in case of an attack). (Piatkowska et al, 2020) proposed EN-based REASENS framework to support reasoning and determining the root causes of software rollout failures in the smart grid based on events collected from distributed and heterogenous sensors in a smart grid. The key components of REASENS framework includes: (i) sensors, (ii) causal reasoning engine, (iii) systems state (transients, misconfigurations, cyber-attacks). Sensors (or detectors) and causal reasoning engine are defined as in (Findrik et al, 2017).

Information Sharing: (Goodwin et al, 2015) proposed a framework for cyber security information sharing. Its building blocks include: (i) types of information exchanged (incidents, threats, vulnerabilities, mitigations, situational awareness, best practices, strategic analysis), (ii) actors involved in information sharing (Government, private critical infrastructure, business enterprises, IT companies, IT security firms, security researchers), (iii)

models of exchange (voluntary exchange models, mandatory disclosure models), (iv) mechanisms of exchange (person to person, machine to machine), (v) methods of exchange (formalized exchanges – based on agreement, security-clearance based exchanges, trust based exchanges, ad hoc exchanges), (vi) information formats (open response – any formats, unique information sharing, structured information sharing). (Alrimawi et al, 2018) developed a share incident knowledge approach across different cyber-physical systems (CPS) through two different meta-models including incident-patterns and CPS. The incident-pattern meta-model represents activity, scene (set of activities), crime script (set of scenes), asset, asset type (physical/digital), actor (offender/victim), resource (tool needed to perform an activity), type of resource (physical/digital), location, type of location (physical/digital), connection (between a location and other entities), and activity initiator. The CPS meta-model captures action, asset, asset type (physical/digital), containment, connection (physical/digital), actor, process (status: running/stopped), physical structure (part of the smart building layout), computing device (example: fire alarm). This helps to extract common incident patterns based on the above-mentioned meta-models and apply appropriate security measures in the future to prevent such incidents. (Rajamaki et al, 2019) highlighted technical standards for sharing cyber information including Structured Cyber Observable eX-pression (CybOX), Threat Information eXpression (STIX), Trusted Automated eXchange of Indicator Information (TAXII). (Luiijf et al, 2015) also highlighted technical standards of sharing cyber information like CybOX, STIX, TAXII, and Malware Attribute Enumeration and Characterization (MAEC).

Cyber Incident Data and Analysis Working Group (CIDAWG, 2015) identified 16 data categories that can be shared anonymously to help organizations in security incident management especially by assessing their risks effectively, putting in place appropriate control measures. The data categories include: (i) type of incident (example: ransomware), (ii) severity of incident, (iii) use of information security standards and best practices, (iv) timeline (date of detection of a cyber incident in addition to date of effective control), (v) apparent goals (or motives – which could be financial), (vi) contributing causes, (vii) security control decay – a security control that is in place, but failed to withstand an incident, (viii) assets compromised/affected, (ix) type of impact(s), (x) incident detection techniques, (xi) incident response playbook – how an operator/decision maker respond to an incident (actions, methods, procedures and tools used), (xii) internal skill sufficiency, (xiii) mitigation/prevention measures, (xiv) costs, (xv) vendor incident support, (xvi) related events.

Forensics: (Van Vliet, Kechadi and Le-Khac, 2015) demonstrated a method to safeguard important information for digital forensic investigations in Industrial Control Systems using a wind turbine case study. They highlighted two important source of information which includes network and device data. The sources of network data include live network data (examples: raw network data, arp tables), historical network data (examples: host-based logs, firewall logs), other log files (examples: access point logs, historians). The sources of device data include running program data (examples: RAM dump, CHIP images), activity log files (examples: active processes, control room logs), transaction log files (examples: error logs, event logs). (Spyridopoulos, Tryfonas and May, 2013) investigated the state of SCADA operators to analyze cyber security incidents in addition to developing digital forensic readiness. They pointed the five different phases in a digital forensic process which includes: (i) examination, (ii) identification, (iii) collection, (iv) analysis, (v) documentation. They also described the information that should be obtained in each phase of the digital forensic process. For instance, during the examination phase of the digital forensic process, at minimum level, network diagrams, configuration details, change logs and authentication credentials needs to be obtained. Furthermore, in the identification phase, type of system, operating system used, type and manufacture of the PLCs, and network design and implementation need to be obtained. (Stirland et al, 2014) explores the challenges of forensic analysis in industrial control systems and proposes a forensic methodology for such systems. They highlighted the different phases in a digital forensic process which includes: (i) identification and preparation, (ii) identifying data sources, (iii) volatility assessment, containment impact analysis and preservation, prioritizing and collection, (iv) examination, (v) analysis, (vi) reporting and presentation, and (vii) reviewing results. This is like the phases highlighted by (Spyridopoulos, Tryfonas and May, 2013). (Spyridopoulos, Tryfonas and May, 2013) described the information that should be obtained in each phase of the digital forensic process in addition to example tools needed in each phase. For instance, example tools needed in the phase of volatility assessment, containment impact analysis and preservation, prioritizing and collection includes write blockers, firewire PCI card, HD camera, FTK imager, EnCase, Helix, TCP dump, data hashing tool, and text editor.

Lesson Learned: The literature that was identified as part of lessons learned focused on the specifics of the corresponding incident (Hassanzadeh et al, 2020) (Hemsley and Fisher, 2018) (Lee, Asante, and Conway, 2016). For instance, (Lee, Asante, and Conway, 2016) analysed the cyber-attack on the Ukrainian power grid. They

analysed technical components used by the attacker, attack mapped on to the ICS cyber kill chain to understand the attack elements, and opportunities to disrupt/restore. The information gathered from this review is used as the basis for developing the security incident management ontology model.

4. Effective Security Incident Management Ontology

In this section, the design requirements and choices considered to build the proposed model are described.

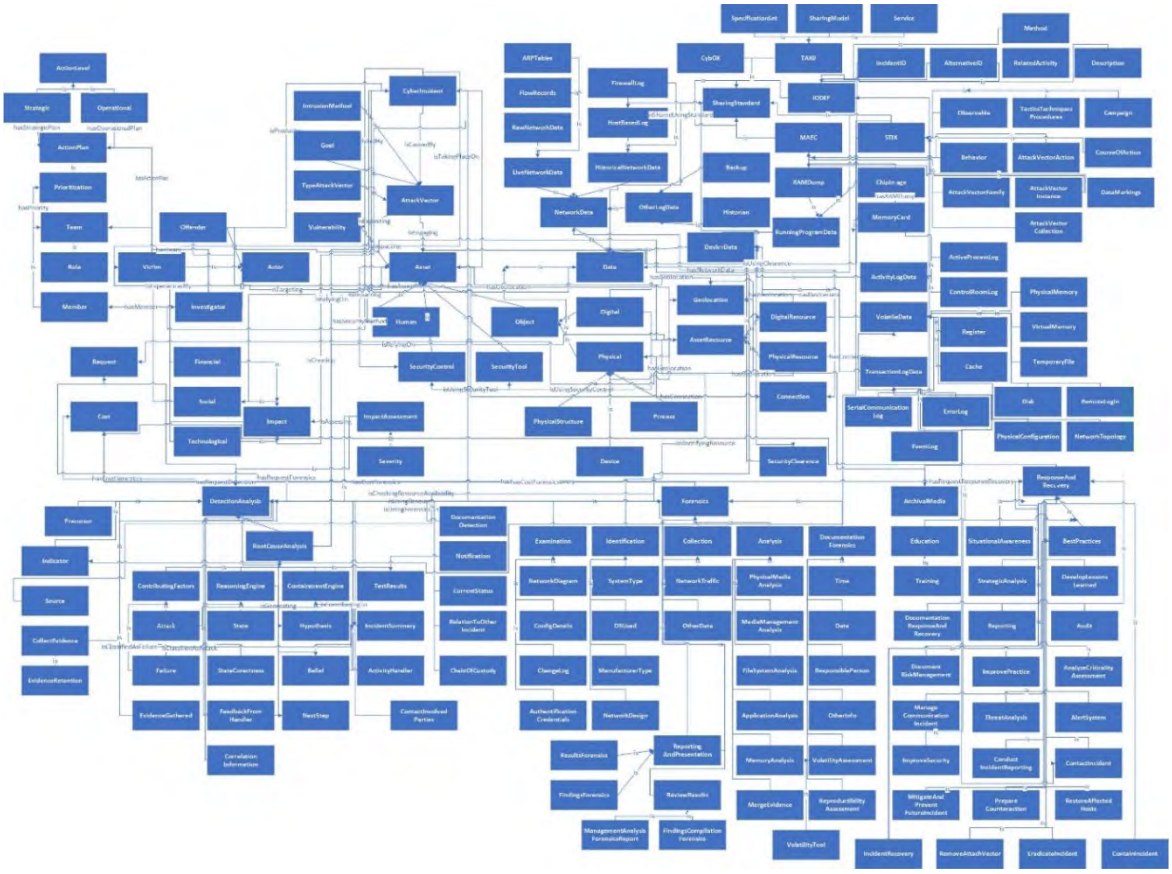

Figure 1: Model Architecture

This research considers the following design requirements (Dipert, 2013):

- to be humanly understandable by using controlled vocabularies.
- to be an ontology that uses widely known and accepted concepts.
- to be represented in one of the best available languages for formalizing ontologies, such as OWL or Common Logic; and
- to be able to apply methodologies for building ontologies and for illustrating instance-level data.

Further, as described in Section 2, the goal of the model is specified, the necessary information is collected and after that conceptualized and formalized in the fourth phase. Consequently, the architecture of the model containing the classes is illustrated in Figure 1, the global view of the model containing is depicted in Figure 2-left, the metrics of the model are captured in Figure 2-right, and the formal definition is provided in Equation (1) below:

Ontology metrics:	
Class count	**191**
Object property count	**40**
Data property count	**401**
Individual count	**44**

Figure 2: Global view model (left) and its metrics (right)

Model = {UC, SC, I, AR} (1)

In (1), UC represents the set of main classes of the model (i.e., first layer); SC represents the set of sub-classes of the model (i.e., second layer); I represent the set of instances / data values of the model (i.e., third layer); AR represents the set of attributes of classes and the relations between their instances.

From Figure 2-left, a series of different units with distinct colors are contained. The blue circles represent classes and sub-classes of the model, the blue rectangles represent the relations between the instances of these classes, the green rectangles represent the attributes of the classes while the orange rectangles represent the type of these attributes e.g., string or double. Furthermore, the followed layered perspective is considered to capture the elements of the model. On the first level are the upper classes (i.e., set UC) which extend the mother class Thing are located. These classes are Actor, AttackVector, Asset, ActionLevel, ActionPlan, Request, Team, SharingStandard, CyberIncident, Impact, Cost, DetectionAnalysis, Forensics, and ResponseAndRecovery. All other sub-classes (child classes) extend the upper classes.

On the second level, the child classes are located i.e., the sub-classes (i.e., set SC) that elaborate the concepts from the first level, such as Investigator (sub-class of Actor), DigitalResource (sub-class of Asset), IntrusionMethod (sub-class of AttackVector), ImpactAssessment (sub-class of DetectionAnalysis), Examination (sub-class of Forensics), ContainIncident (sub-class of ResponseAndRecovery), and Technological (sub-class of Impact). In Figure 3 are depicted a series of sub-classes of class ResponseAndRecovery which shows the processes and activities involved in the response and recovery phases of a cyber security incident.

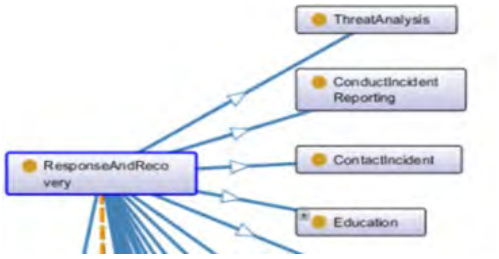

Figure 3: Selection of Sub-classes of Class ResponseAndRecovery

On the third level, the instances (i.e., set I) that classes and sub-classes have, are represented. For exemplification purposes, in Figure 4, data of class *Actor -> Investigator* i.e. actors that have directly investigated this incident can be seen, response and recovery actions contained by class *ResponseAndRecovery -> RestoreAffectedHosts*, social effects that the incident had in class *Impact -> Social*, technological effects in class *Impact -> Technological*, and three types of requests for detection, forensics, and response and recovery actions that investigators put in place for the incident are contained in class *Request*.

On the fourth level, the attributes of classes are placed i.e., data properties (i.e., set AR) together with the relationships between them i.e., object properties. Accordingly, a selection them is further explained and depicted in Figure 5:

- *AnalysisStatus:* attribute of class *Analysis* that depicts the status of ongoing forensics analysis process and has two possible values: *{on, off}.*
- *EventLogPath:* attribute of class EventLog that contains the system path of the event log investigated and which is of type *string.*
- *IncidentSummaryAvailability:* attribute of class *IncidentSummary* which shows if the summary of an analysis conducted during the detection phase is available, and has two possible values: *{yes, no}.*
- *ResponseAndRecoveryDescription:* attribute of class *ResponseAndRecovery* that contains a brief description of the response and recovery phases of a cyber security incident, and which is of type *string.*
- *isAnalyzedBy*: relationship between class *CyberIncident* and class *Investigator* that shows the fact that a cyber security incident is analyzed by a security investigator e.g., defender who could be represented by an individual or a group of individuals in a security department or organization.
- *hasDeviceData:* relationship between classes *Physical, Digital, PhysicalResource, DigitalResource* and class *DeviceData* which shows which resource contain data retrieved from investigated devices.
- *hasRequestForensics:* relationship between class *Forensics* and class *Request* which shows the request done for starting the forensics process on a cyber security incident.

- *isSharedUsingStandard:* relationship between class *Data* and class *SharingStandard* to show how data is exchanged between two or more investigating entities.

Figure 4: Instances or Data for the Colonial Pipeline Cyber Security Incident

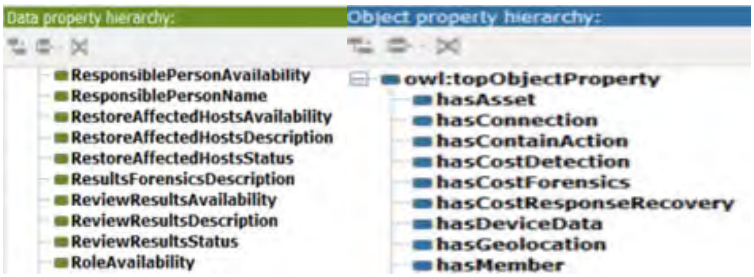

Figure 5: Selection of Attributes and Relationships in the Model

Determination of Layers in this Model: the first layer capture main phases, aspects, and agents involved in different processes of a cyber security incident; the second layer represent entities contained in the first layer with a focus on important activities and resources used; the third layer contain data-values or instances of the classes belonging to the first and second layer, and represent real or mimicked cyber incident data; the fourth layer embed characteristics of classes contained in the first and second layers that show attributes of these entities, and further captures relations between the instances or data-values corresponding to a cyber incident.

Until now, the results of the first seven phases of the methodological approach considered were presented i.e., the proposed implemented model. Furthermore, in the eighth phase the evaluation process takes place. Hence, the evaluation is carried out in two phases. First, by considering evaluation criteria such as consistency and reusability (Sawsaa & Lu, J 2012; Esposito, Zappatore & Tarricone, 2011). And second, through exemplification on a real-life ICS cyber incident. The evaluation from the first case is done in the development environment using the Hermit reasoner and was successful. The evaluation from the second case i.e., through exemplification is further presented.

Case Study Description: Colonial Pipeline operates over 5500 miles of pipeline extending from Texas to New Jersey in the United States (US) (TechTarget, 2021). It transports refined oil for gasoline, jet fuel, and home heating oil. It also directly serves jet fuel to about seven airports (TechTarget, 2021). Moreover, nearly 45% of east coast of US get their fuel from Colonial Pipeline. In May 2021, hacking group known as *"DarkSide"* carried out a ransomware attack on Colonial Pipeline (TechTarget, 2021). Ransomware is a type of malware which encrypts a victim's files. The adversary might then demand ransom to restore access to the encrypted files upon payment. Even though this ransomware attack mainly affected the IT environment of Colonial Pipeline including its billing and accounting systems, this also disrupted fuel supplies as the operations were shut down as an immediate response to this ransomware attack and prevent the spreading of ransomware (TechTarget, 2021). This shut down led to panic buying, spike in gasoline price, and localized fuel shortage. This ransomware attack seems to be initiated through the stolen password for VPN (Reuters, 2021). Additionally, this legacy VPN system did not have multi-factor authentication, which made it easier for the adversary (Reuters, 2021). Personnel in the company seems to have used the same password for different accounts. One of which seems to be hacked earlier and the corresponding password was leaked in the dark web, which is then used for this purpose of getting into the VPN and carrying out the ransomware attack. DarkSide accessed the colonial pipeline network, stole 100 gigabytes of data within a two-hour window. Later, an employee noticed the ransom note and notified the operations supervisor. This led to the immediate shut down of operations. A security firm named "Mandiant" was involved in the investigation of this attack (TechTarget, 2021). Law enforcement and Government was also notified about this attack. The company paid the ransom to get access and reduce the recovery time (Reuters, 2021). In addition, at the later stage of the investigation, some of the ransom paid was recovered from the adversary group (Reuters, 2021). This ransomware attack was initiated on 7th May 2021 and the pipeline operations were restored on 12th May 2021 (TechTarget, 2021).

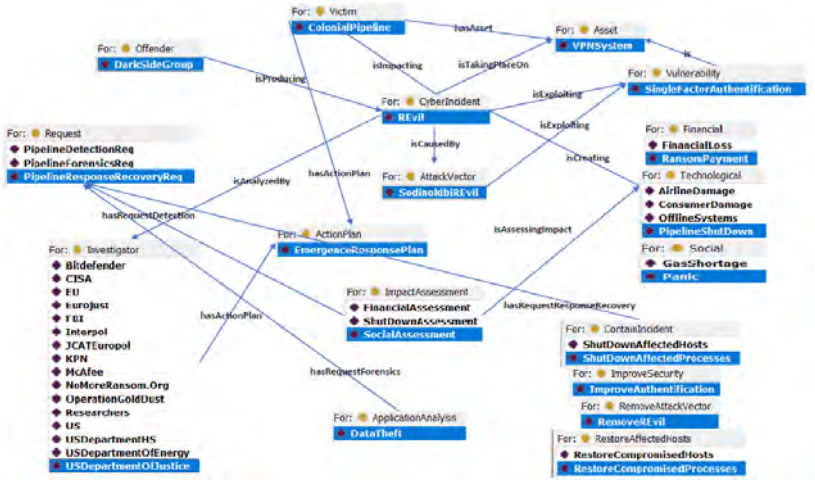

Figure 6: Colonial Pipeline Cyber Security Incident Data Visualization through Model Instantiation

To demonstrate the proposed model, the data obtained from the case study was populated in the model as depicted in Figure 6. This is compliant with the fourth design requirement (Dipert, 2013) considered when building the model, and further facilitates the following activities: (i) can serve as a common understanding basis for relevant stakeholders, (ii) can help to visualize relevant details of cyber security incidents during the mid-incident and post-incident phase for appropriately responding to an incident/learn relevant lessons from the incidents

5. Related Work

(Agrafiotis et al, 2018) advances a taxonomy of harm types that could be experienced by organizations from cyber-attacks. Furthermore, they have identified the stakeholders involved, their perceptions and priorities when dealing with the effects produced by cyber security incidents. (Arbanas & Čubrilo, 2015) provides a review of security ontologies based on a decade of scientific research until 2014. (Oltramari et al., 2015) developed an ontology for assessing human factors in cyber security by capturing individual characteristics, situational characteristics, and relationships influencing trust aiming at providing a useful basis for predicting and quantifying risk in required cyber risks assessments procedures. (Mundie et al., 2014) propose a meta-level ontological model for cyber security incident management which includes activities such as collecting evidence about the incident, analyzing the causes of the incidents, as well as drawing, and forming lessons learned.

(Mundie & Ruefle, 2012) discusses the current body of knowledge for cyber security incident management in a systematic approach. (Paul & Whitley, 2013) present a taxonomy for cyber security awareness questions that could support different activities taken while designing and developing cyber security awareness technologies. Among the aspects identified, the one named Damage Assessment is useful in this research as it refers to the response taken to effects occurred after these have been fully understood. (Onwubiko, 2018) advances an ontology for cyber security incident analysis. Notably, relevant to this research are the aspects involved in the need of escalation when managing cyber security incidents. (Maathuis et al, 2018a) propose an ontology that captures the essential entities and their corresponding relations in military Cyber Operations e.g., Effect which represents the impact that Cyber Operations have on targets and collateral entities. (Maathuis et al, 2018a) introduce a model for analyzing the effects of military Cyber Operations such as collateral damage and military advantage as a basis for military targeting decisions taken in Cyber Warfare. (Tagarev & Ratchev, 2020) propose a taxonomy for crisis management functions which although are not dedicated to the cyber security domain, they are still relevant to this paper. The authors identified a set of activities like making resources available to tackle an incident focusing on both short- and long-term response and recovery activities. Accordingly, both perspectives are integrated in the model proposed.

6. Conclusions and Future Work Directions

Efficacious security incident management plays a crucial role in lessening the negative consequences of an incident in terms of organization's economy, reputation, and personnel safety in addition to recovering/restoring back to normal operations after the incident in a short down time. There are various concepts that are proposed in addition to globally accepted standards like CybOX, STIX, TAXII in the scientific literature relevant for security incident management. However, a holistic overview of such concepts and their

relationships that could help to operationalize them during incident response is missing. Therefore, in this paper, we conducted an extensive literature review on security incident management especially covering the mid-incident and post-incident phases. This is categorized as four different themes including root cause analysis. Information sharing, forensics, and lessons learned. Based on the extensive literature review, a security incident management ontology model is developed with relevant classes and sub-classes. Firstly, the developed model is evaluated using Hermit reasoner. Additionally, the model is populated with the relevant information from the colonial pipeline cyber security incident to show how this developed model can be used during the post-incident phase of security incident management. In the future, using the proposed approach, the model can be further extended with additional information from the relevant grey literature like white papers, standards, technical reports which might be more applicable for security incident management. This model represents the basis for the development of Artificial Intelligence (AI)/Machine Learning (ML)-based models. For instance, in root cause analysis, the developed ontology model can provide inputs in terms of variables and their relationships to the structural development of AI/ML-based models that would help identify the root cause and select effective response strategies. Moreover, the effectiveness of the developed security incident management ontology model needs to be evaluated in the future during an ongoing incident/mock incident.

References

Alrimawi, F., Pasquale, L., Mehta, D. and Nuseibeh, B., 2018, May. I've seen this before: Sharing cyber-physical incident knowledge. In *Proceedings of the 1st International Workshop on Security Awareness from Design to Deployment* (pp. 33-40).

Cichonski, P., Millar, T., Grance, T. and Scarfone, K., 2012. Computer security incident handling guide. NIST Special Publication.

Chockalingam, S., Pieters, W., Teixeira, A., Khakzad, N. and Gelder, P.V., 2018. Combining Bayesian networks and fishbone diagrams to distinguish between intentional attacks and accidental technical failures. In *International Workshop on Graphical Models for Security* (pp. 31-50).

Chockalingam, S. and Katta, V., 2019, December. Developing a Bayesian Network Framework for Root Cause Analysis of Observable Problems in Cyber-Physical Systems. In *2019 IEEE Conference on Information and Communication Technology*.

Chockalingam, S., Pieters, W., Teixeira, A., and van Gelder, P., 2021. Bayesian network model to distinguish between intentional attacks and accidental technical failures: a case study of floodgates. *Cybersecurity*, *4*(1), pp.1-19.

CIDAWG, 2015. Enhancing Resilience Through Cyber Incident Data Sharing and Analysis.

Cooper, C., Booth, A., Varley-Campbell, J., Britten, N. and Garside, R., 2018. Defining the process to literature searching in systematic reviews: a literature review of guidance and supporting studies. *BMC medical research methodology*, *18*(1), pp.1-14.

Esposito, A, Zappatore, M & Tarricone, L 2011, 'Evaluating scientific domain ontologies for the electromagnetic knowledge domain: A general methodology', *Journal of Web & Semantic Technology*. vol. 2, no. 2, pp. 1-19.

Fernández-López, M, Gómez-Pérez, A & Juristo, N (1997) 'Methontology: From ontological art towards ontological engineering', *Proceedings of the fourteenth national conference on Artificial Intelligence*, *AAAI-97*, Spring Symposium Series, pp. 33-40.

Findrik, M., et al., 2017. Trustworthy Computer Security Incident Response for Nuclear Facilities.

Goodwin, C., Nicholas, J.P., Bryant, J., Ciglic, K., Kleiner, A., Kutterer, C., Massagli, A., Mckay, A., Mckitrick, P., Neutze, J. and Storch, T., 2015. A framework for cybersecurity information sharing and risk reduction. *Microsoft*.

Hassanzadeh, A., Rasekh, A., Galelli, S., Aghashahi, M., Taormina, R., Ostfeld, A. and Banks, M.K., 2020. A review of cybersecurity incidents in the water sector. *Journal of Environmental Engineering*, *146*(5), p.03120003.

He, Y., Inglut, E. and Luo, C., 2022. Malware incident response (IR) informed by cyber threat intelligence (CTI). *Science China Information Sciences*, *65*(7), pp.1-3.

Hemsley, K.E. and Fisher, E., 2018. *History of industrial control system cyber incidents* (No. INL/CON-18-44411-Rev002). Idaho National Lab, United States.

Hevner, AR, March, ST & Park, J. (2004), 'Design research in information systems research', *MIS Quarterly,* vol. 28, no. 1.

Kulikova, O., Heil, R., van den Berg, J. and Pieters, W., 2012, December. Cyber Crisis Management: A decision-support framework for disclosing security incident information. In 2012 International conference on cyber security (pp. 103-112). IEEE.

Lallie, H.S., et al., 2021. Cyber security in the age of covid-19: A timeline and analysis of cyber-crime and cyber-attacks during the pandemic. Computers & Security, 105, p.102248.

Lee, R.M., Assante, M.J., Conway, T., 2016. Analysis of the cyber-attack on the Ukrainian power grid. *Electricity Information Sharing and Analysis Center (E-ISAC)*, *388*.

Lee, J.W., Song, J.G., Son, J.Y. and Choi, J.G., 2018. Propositions for Effective Cyber Incident Handling.

Luiijf, et al. "On the sharing of cyber security information." International Conference on Critical Infrastructure Protection". 2015.

Maathuis, C., Pieters, W. & van den Berg, J. (2018a). 'A Computational Ontology for Cyber Operations'. In *Proceedings of the 17th International Conference on Cyber Warfare and Security*, ICCWS, pp. 278-88.

Maathuis, C., Pieters, W., & van den Berg, J. (2018b). A knowledge-based model for assessing the effects of cyber warfare. In *Proceedings of the 12th NATO Conference on Operations Research and Analysis*.

Mavroeidis, V., & Bromander, S. (2017). Cyber threat intelligence model: an evaluation of taxonomies, sharing standards, and ontologies within cyber threat intelligence. In *2017 European Intelligence and Security Informatics Conference (EISIC)*, pp. 91-98.

Mundie, D. A., & Ruefle, R. (2012, August). Building an incident management body of knowledge. In *2012 Seventh International Conference on Availability, Reliability and Security*. IEEE (pp. 507-513).

Mundie, D. A., et al. (2014, January). An Incident Management Ontology. In *STIDS* (pp. 62-71).

Okoli, C., 2015. A guide to conducting a standalone systematic literature review. *Communications of the Association for Information Systems*, *37*(1), p.43.

Oltramari, A., Henshel, D. S., Cains, M., & Hoffman, B. (2015). Towards a Human Factors Ontology for Cyber Security. *Stids*, *2015*.

Onwubiko, C. (2018). Cocoa: An ontology for cybersecurity operations centre analysis process. In *2018 International Conference on Cyber Situational Awareness, Data Analytics and Assessment (Cyber SA)* IEEE (pp. 1-8).

Paul, C. L., & Whitley, K. (2013). A taxonomy of cyber awareness questions for the user-centered design of cyber situation awareness. In *International Conference on Human Aspects of Information Security, Privacy, and Trust*. Springer (pp. 145-154).

Peffers, K., Tuunanen, T., & Niehaves, B. (2018). Design science research genres: introduction to the special issue on exemplars and criteria for applicable design science research.

Piatkowska, E., et al., 2020. Online Reasoning about the Root Causes of Software Rollout Failures in the Smart Grid. In *2020 IEEE International Conference on Communications, Control, and Computing Technologies for Smart Grids (SmartGridComm)* (pp. 1-7).

Pranggono, B. and Arabo, A., 2021. COVID-19 pandemic cybersecurity issues. Internet Technology Letters, 4(2).

Rajamäki, J., Tikanmäki, I. and Räsänen, J., 2019. CISE as a Tool for Sharing Sensitive Cyber Information in Maritime Domain.

Reuters, 2021, One password allowed hackers to disrupt Colonial Pipeline. https://www.reuters.com/business/colonial-pipeline-ceo-tells-senate-cyber-defenses-were-compromised-ahead-hack-2021-06-08/

Sawsaa, AF & Lu, J 2012, 'Building information science ontology (OIS) with Methontology and Protégé', *Journal of Internet Technology and Secured Transactions*, no. 1, vol. 3/4.

Shinde, N. and Kulkarni, P., 2021. Cyber incident response and planning: a flexible approach. *Computer Fraud & Security*, *2021*(1).

Spyridopoulos, T., Tryfonas, T. and May, J., 2013. Incident analysis & digital forensics in SCADA and industrial control systems.

Staves, A., Balderstone, H., Green, B., Gouglidis, A. and Hutchison, D., 2020, May. A Framework to Support ICS Cyber Incident Response and Recovery. In *the 17th International Conference on Information Systems for Crisis Response and Management*.

Stirland, J., et al., 2014, October. Developing cyber forensics for SCADA industrial control systems. In *The International Conference on Information Security and Cyber Forensics (InfoSec2014).* pp. 98-111.

TechTarget, 2021. Colonial Pipeline hack explained: Everything you need to know. https://whatis.techtarget.com/feature/Colonial-Pipeline-hack-explained-Everything-you-need-to-know

Van Vliet, P., Kechadi, M.T. and Le-Khac, N.A., 2015. Forensics in industrial control system: a case study. In *Security of Industrial Control Systems and Cyber Physical Systems* (pp. 147-156).