Computers & Security 134 (2023) 103454

Contents lists available at ScienceDirect

Computers & Security

journal homepage: www.elsevier.com/locate/cose

Operations-informed incident response playbooks

Avi Shaked [a,b,*], Yulia Cherdantseva [a], Pete Burnap [a], Peter Maynard [a]

[a] School of Computer Science & Informatics, Cardiff University, Wales, UK
[b] Department of Computer Science, University of Oxford, England, UK

ARTICLE INFO

Keywords:
Cyber security
Incident response
Critical national infrastructure
Model of operations
Impact analysis
Organizational capability

ABSTRACT

Cyber security incident response playbooks are critical for establishing an effective incident response capability within organizations. We identify a significant conceptual gap in the current research and practice of cyber security playbook design: the lack of ability to communicate the operational impact of an incident and of incident response on an organization. In this paper, we present a mechanism to address the gap by introducing the operational context into an incident response playbook. This conceptual contribution calls for a shift from playbooks that consist only of process models to playbooks that consist of process models closely linked with a model of operations. We describe a novel approach to embed a model of operations into the incident response playbook and link it with the playbook's incident response activities. This allows to reflect, in an accurate and systematic way, the interdependencies and mutual influences of incident response activities on operations and vice versa. The approach includes the use of a new metric for evaluating the change in operations in coordination with critical thresholds, supporting decision-making during cyber security incident response. We demonstrate the application of the proposed approach to playbook design in the context of a ransomware attack incident response, using a newly developed open-source tool.

1. Introduction

Cyber security Incident Response (IR) is a crucial element of coping with cyber security incidents and assuring operational resilience. A cyber security incident is any form of an attack which involves an artifact in the cyber/digital domain, whether as a primary target or as a means to achieving the end goal of an attack. Risk management and introduction of cyber security controls into the designs of systems and organizations can raise the level of security. However, once a cyber security incident occurs, it is essential to respond to it effectively. IR is a collective term which relates to the planning and execution of such response and is considered to be a key organizational cyber security capability (Ahmad et al., 2012; Stouffer et al., 2022).

Explaining to the boards and executives how a cyber security incident and IR might impact the operations of their organization is highly important. In a tabletop exercise on concurrent cyber and emergency incident response, it was observed that executives often fail to understand organizational cyber security risks (Korn et al., 2021). The United States National Institute of Standards and Technology (NIST) explicitly advises to communicate the impact of process shutdowns or communication disconnections on business operations with all stakeholders during IR (Stouffer et al., 2022).

Despite the acknowledged need for reflecting the impact of IR on operations, IR is typically executed only with technical considerations in mind, failing to consider the associated impact on business operations. The impact of a cyber security incident on an organization could have a wide range of consequences including physical/digital, economic, psychological, reputational and social/societal (Agrafiotis et al., 2018).

The traditional approach to IR, which is limited to the technical aspect, becomes even more problematic in the Critical National Infrastructure (CNI) context[1]. Failure to consider the impact on the availability of CNI systems may lead to tragic consequences. For example, a typical way to address a malware infection is to disconnect an infected device from a network. However, this is a poor and dangerous strategy when the infected device performs critical tasks (Huang et al., 2019). A vivid example of the dangerous unsuitability of the disconnection strategy in the CNI context is the 2021 Colonial Pipeline cyber incident, in which this strategy was employed and resulted in a serious disruption

* Corresponding author at: School of Computer Science & Informatics, Cardiff University, Wales, UK.
E-mail address: avi.shaked@cs.ox.ac.uk (A. Shaked).

[1] CNI refers to systems and assets that are vital to the functioning of a country and whose disruption would have a significant impact on national security, economic stability, or public health and safety. Examples of CNI sectors include energy, finance, healthcare, and transportation.

https://doi.org/10.1016/j.cose.2023.103454
Received 11 July 2023; Accepted 22 August 2023
Available online 30 August 2023

to service with a lasting impact on fuel supply (Tsvetanov and Slaria, 2021). We further discuss this incident in Section 2.

Ahmad et al. (2012) discuss the additional importance of IR in the context of organizational learning, as a practice which produces information for subsequent risk assessments. In a later, related work, Ahmad et al. (2020) expand the discussion, calling for integration between the security management organizational function – which produces risk-informed policies – and the IR organizational function. They state that *"providing IR with strategic and tactical guidance on policy… improves the effectiveness and efficiency of the organizational security response."* However, neither of these publications explains how IR should be informed by risk assessment and policy – while the incident takes place – or suggests a rigorous method for providing the said guidance to IR.

Similarly, Stamper et al. (2019) identify that risk tolerance definitions and IR require input from multiple stakeholders, particularly from executives; and that often chief security officers, who oversee IR, make risk-related decisions that affect business and that are outside of their remit of responsibility. Furthermore, Stamper et al. (2019) state that it is desirable to build an IR plan based on business (or mission/operations) impact analysis which incorporates the risk appetite. While stating the importance of incorporating all relevant stakeholders as members of an IR team and discussing a general principle according to which playbooks should prescribe the specific organization's response to address common types of incidents, no guidance is offered by Stamper et al. (2019) for an impact and risk informed IR design. Furthermore, a needs assessment for computer security IR effectiveness identifies prominent gaps in IR tools, specifically mentioning the need for *"a tool for estimating the initial impact and risk of a reported cyber security incident in a structured way"* (Van der Kleij et al., 2017).

Cyber security practitioners typically rely on playbooks to provide instructions and guidance on IR (Ahmad et al., 2021; Naseer et al., 2021; Schlette et al., 2021; Staves et al., 2022). An IR playbook is an action plan prescribing a set of steps that should be carried out in response to a given incident (Bartock et al., 2016; Onwubiko, 2018). A recent empirical evaluation of the usability of IR playbooks suggests that a potential improvement for playbook designs is the consideration of the organizational concerns and constraints, yet no method is provided to address this (Stevens et al., 2022). Another publication about developing a decision support system for cyber security and incident managers outlined the need to address the impact on operations when preparing IR playbooks, but only provided a very general memory aid to account for that (van der Kleij et al., 2022). In Section 2.A, we discuss further the limitations in the state-of-the-art in playbooks design. Our analysis shows that while a playbook is a useful and widely used instrument for managing and handling cyber security IR there is a significant room for improvement in the IR playbook design theory and practice.

In this paper, we propose a conceptual and applicable extension of the IR playbook concept, which addresses the gaps discussed above and allows communicating the impact of an incident on operations and showing how an incident and an IR process can affect an intended operational status. Our contribution is two-fold. First, we introduce the concept of an operations-informed playbook, identifying that IR playbooks should be extended from a pure process orientation to a process model connected and aligned with a model of operations. Second, we provide a concrete modelling approach – supported by an open-source application developed as part of our research – that supports the design of these extended playbooks. We demonstrate the value of the new IR approach in a widely applicable ransomware attack scenario. In Section 2, we discuss background regarding the design of IR playbooks with respect to impact on operations, dependency modelling and ransomware attacks. In Section 3, we present our novel concept of an extended cyber security IR playbook, and outline a practical, tool-supported approach to designing the extended playbooks, demonstrating the feasibility of applying the new concept. In Section 4, we detail a case study of responding to a ransomware attack and use it to validate our suggested approach. Finally, in Section 5, we discuss the advantages and the limitations of our approach and suggest future work.

2. Background

A. Impact in playbooks design

IR is expected to be driven by the impact of the detected incident on operations (Stamper et al., 2019). Additionally, IR should consider the impact of the response activities while devising or enacting the response (Ahmad et al., 2020). Playbooks are often used to orchestrate IR and can be used as a decision support system in the IR context (van der Kleij et al., 2022). IR playbooks are process models that depict incident response activities as workflows (Schlette et al., 2021). Typical representation mechanisms for IR playbooks are

(1) text (narrative and description of steps), e.g., Microsoft's IR playbooks (Microsoft, 2023);
(2) graphical flow diagrams, either informal or semi-formal (i.e., using a process modelling standard), e.g., the Scottish government's ransomware playbook (Scottish Government, 2020);
(3) markup languages, e.g., the CACAO playbooks (OASIS Open, 2021)
(4) tables, e.g., the Canadian Center for Cyber Security's ransomware playbook (Canadian Centre for Cyber Security, 2021).

NIST's guide for cyber security event recovery explicitly acknowledges the need to include dependency maps in playbooks to help in devising a response according to the desirable restoration priority, and even discusses this in an example of recovery from a ransomware incident (Bartock et al., 2016). However, the guide does not specify what form these dependency maps may take or what they are expected to include, only implicitly hinting at some sort of representation of the operational structure. Furthermore, the guide does not offer any specific mechanisms or methods to incorporate such dependency maps in the playbooks and in the actual IR[2].

A comparative study of IR playbook formats acknowledges the importance of identifying the impact of IR activities with respect to operations, yet the study does not identify *impact* as a standalone IR concept (Schlette et al., 2021). The same study identifies *prioritization* as an IR security concept, and states that it is *"mostly realized with indicating severity."* An identification of severity is merely an overall assessment of the impact, usually as a qualitative, ordinal ranking, and it does not provide concrete details about the impact, such as affected services and disruptions to operations.

Based on their analysis of the drawbacks of the examined playbook standards, (Schlette et al., 2021) advise to *"document the potential impact of incident response procedures"* and identify this as a motivation for incorporating approval mechanisms represented by the *authorization* security concept. Also, we note that the *impact* concept is implemented in two of the playbook formats surveyed: in CACAO, where an impact value indicates organizational consequences of the execution of a playbook (OASIS Open, 2021); and in the discontinued RECAST, where a free-form description allows to specify the consequence as a contextual characteristic of an entire playbook (Applebaum et al., 2018). These implementations, however, are limited in being a single value/description for the entire playbook. Accordingly, these formats do not provide means to incorporate and align a fine-grained cyber security impact analysis into playbooks, neither during the playbook design nor upon enactment of the playbook.

[2] In fact, the guide implicitly mentions that dependency maps emerge from threat modelling, while referring to a 2016 threat modelling guide – NIST SP 800-154 – which has never advanced beyond a draft release and has no mention of dependency maps.

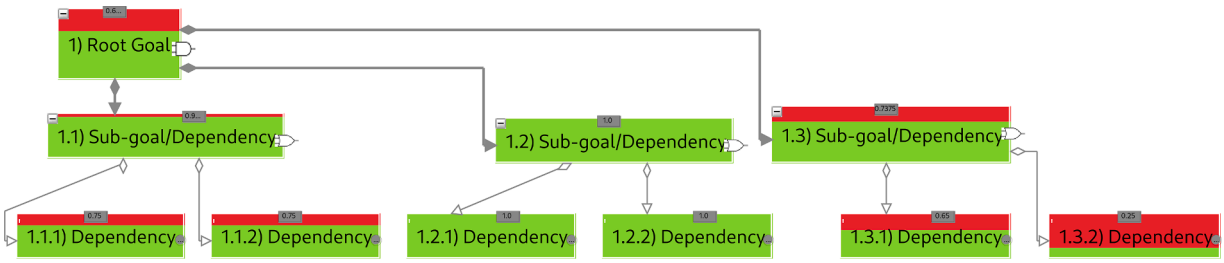

Fig. 1. An example of a dependency modelling artifact.

Furthermore, CACAO and RECAST do not explicitly reference a model of operations, and therefore are not sustainable in terms of monitoring operational changes and/or revised security assessment during enactment of an IR procedure; both of which are typical consequences of IR in the organizational cyber security landscape.

There remains a significant gap in both IR research and practice in associating IR actions with operational impact. This is manifested in the lack of capability within the existing IR playbook standards and design approaches to model and capture the impact of IR on operations. This missing capability undermines effective IR planning and enactment, and decision making.

B. *Dependency modelling*

In risk assessment, the impact of a cyber security incident is typically captured as an element of risk (alongside feasibility) (Shaked, 2023). Fault Tree Analysis (FTA) is commonly used in reliability and safety engineering to perform assessments of component failures by performing a deductive analysis. FTA allows mapping a technical system using a tree-like structure. When applied to cyber security, FTA results in attack trees (Nagaraju et al., 2017). However, the downside to this approach is that only technical aspects of the system are modelled, failing to provide a wider scope for the implications of the attacks. MITRE's Structured Cyber Resilience Analysis Methodology (Bodeau and Graubart, 2016) in combination with Crown Jewels Analysis (Kertzner et al., 2022) and Cyber Resiliency Engineering Framework (Bodeau and Graubart, 2011) can be used to build a cyber dependency map. However, this is limited to the cyber domain, e.g., hardware and software lifecycles from development to system deployment, lacking a wider scope, specifically with respect to organizational operational objectives. To capture the impact of IR on complex systems or organizations, it is necessary to use modelling methods that provide a system-level perspective. System-level cyber security risk assessment methods are in their infancy.

Dependency Modelling (DM) is a method for organizational risk management based on a data model that can be applied as a system-level method (The Open Group, 2012). Unlike other system-level risk analysis methods – such as STPA-Sec (Young and Leveson, 2013) – DM is a quantitative method, and as such it promotes the ability to establish quantitative metrics; providing a more fine-grained assessment system to support decision making. Furthermore, as opposed to typical failure-oriented approaches (e.g., the aforementioned STPA-Sec), DM employs a positivist approach to phrasing the operational statements, describing a desirable state of operations as a context for analyzing and managing risks. This positivist, constructive approach details what needs to be done or maintained (as opposed to what should be avoided) for an organization to perform as intended, and as such it is better suited for informing system-related designs, such as the design of incident response. Accordingly, and perhaps most pertinent to our work, DM relies on representing operational dependencies explicitly in a data model as a critical step. This results in a model of operations being readily available as part of the DM risk assessment process. DM can provide valuable models of operations in CNI-related context (Cherdantseva et al., 2022; Rotibi et al., 2023), corresponding with the scope of our case study application.

Fig. 1 illustrates a typical artifact resulting from dependency modelling, expressed visually using the tool we developed for this research, as mentioned in Section 3. The nodes in the directed graph represent goals and sub-goals, with leaf nodes representing the lowest level of dependencies, and the edges represent the relations between goals and sub-goals. The relations may be OR-typed – represented in the figure by hollow diamond at the dependant goal end and empty arrowhead at the sub-goal end, or AND-typed – represented in the figure by filled diamond and arrowhead. OR-typed dependencies reduce the risk to the parent, as every one of the possible dependencies is sufficient to accomplish the parent goal; while AND-typed dependencies increase the risk, as the parent goal relies on all its dependencies, i.e., a compromise of a single dependency can lead to a parent goal's failure. Each node has a state represented by the probability of success (relative green area of the node) or failure (relative red area of the node). In the figure, the success probability explicitly appears in a little grey box attached to each node.

C. *Ransomware attacks on critical national infrastructure*

Our case study explores the use of our approach to playbooks design in the context of a ransomware attack on CNI. In this subsection, we provide the related background to rationalize the selection of this context for our case study, highlighting that it is a valid and prominent type of cyber incident and a genuine challenge for effective IR.

Ransomware is a type of malware the encrypts data on computer systems, and then demands payment to be made for the user to regain access to the data. The motivation for ransomware attacks is financial, with the attackers encrypting the victim's data and demanding payment in exchange for the decryption key. Ransomware attacks have become a significant concern for organizations, particularly those in CNI sectors, with far-reaching and long-lasting consequences, as the disruption of the CNI may significantly impact national security, economic stability, or public health and safety. Furthermore, the techniques used by ransomware are used in offensive operations designed to cause maximum interference with a system e.g., CRASHOVERRIDE, which deployed a wiper tool to disable CNI systems (Dragos Inc., 2017).

There have been several notable ransomware attacks on CNI organizations in recent years. Some of the most widely known attacks follow. The 2017 WannaCry attack affected organizations in various CNI sectors, including healthcare, transportation, and telecommunications. The attack spread rapidly by using a worm-like malware that exploited a vulnerability in Microsoft Windows (Akbanov et al., 2019; US Department of Homeland Security's National Cybersecurity and Communications Integration Center, 2017). Even though a kill switch preventing further infection was discovered few hours after the attack and quickly exercised, WannaCry resulted in widespread disruption to operations and significant financial losses (see, for example, (Ghafur et al., 2019)). This increased the awareness that "*it is crucial to develop and implement an agreed strategy for measuring the true effect of cybersecurity incidents*" and that "*a systems approach and clear plan are required*" (Martin et al., 2018). The 2019 LockerGoga attack targeted one of the world's largest

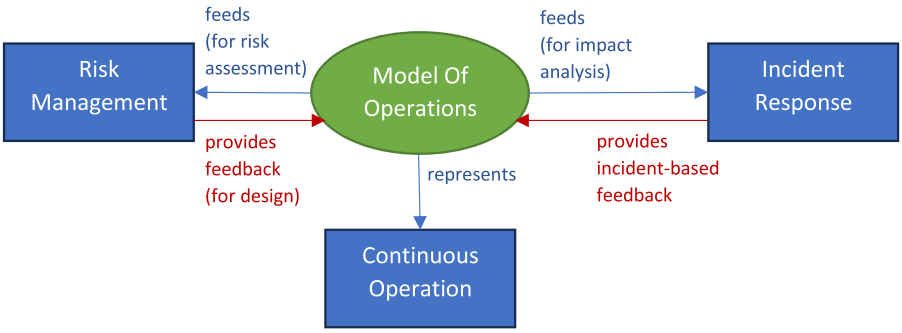

Fig. 2. Model of operations as a link between risk management and incident response.

aluminum manufacturers and disrupted the company's operations (Adamov et al., 2019; Akramova Nargiza, 2022). IR planning was suggested, in retrospect, as an effective countermeasure to the attack (Akramova Nargiza, 2022). The 2020 SolarWinds attack targeted US government agencies as well as private companies like FireEye and Microsoft (U.S. Government Accountability Office, 2021). The attack was conducted through supply chain attack where the attackers hid a trojan in a software update of the SolarWinds Orion software, which is a widely used Information Technology monitoring and management platform (Freas et al., 2022). In 2021, a ransomware compromised the Colonial Pipeline, a company responsible for gasoline distribution in the U.S. east coast. The incident had a significant impact on the U.S. economy and daily life as the pipeline – responsible for about 45% of the East Coast's fuel supply – was shut down in response and in attempt to minimize damage; causing long lines at gas stations, and spiking gas prices (Freas et al., 2022; Spaulding, 2021). The Colonial Pipeline company reportedly paid the attackers a ransom of about $4.4 million at the time, to regain access to their systems. Anecdotal evidence suggests that the attackers claim they did not intend to disrupt the pipeline operations; nevertheless, the impact on the operations was significant (Spaulding, 2021). While the shutdown lasted for six days, it had a lasting impact (Tsvetanov and Slaria, 2021), and this highlighted the vulnerability of the country's critical infrastructure to cyber-attacks and the need for better preparedness and IR plans (Freas et al., 2022). Specifically, it was identified that "*planning … incident response to reduce the impact of a successful hack is one of the most important, and often underappreciated, elements of managing cyber risk*" (Spaulding, 2021).

3. Operations-informed incident response playbook

In this section, we introduce the operations-informed IR playbook, to address the gap with respect to the incident and IR operational impact analysis (discussed in Sections 1 and 2). Our new type of playbook integrates a process model, which is the prominent form of playbook, with an operational model in the form of a dependency map.

Our novel approach to IR playbooks design is to create operations-informed IR playbooks. This is achieved by associating activities in an IR process model with respective operational context. We relate to this as "operations-informed playbooks".

For simplicity purposes, in this paper we use a previously developed IR process model (Shaked et al., 2022). This does not limit the applicability of our concept: our approach remains applicable to any process model which relates to workflows or activities. Specifically, all models surveyed by Schlette et al. (2021) are suitable, and so are any playbooks in a form of a flow-chart. An adaptation can also be made to support tabular forms when each row of a table entry translates into an activity in a process model.

In our newly devised, extended playbook, we connect activities of a process model with elements of a model of the operations. We use DM to create the model of operations. DM was selected due to being a constructive approach that results in a model of operations (as explained in Section 2.B). We note that the original use of DM is for organizational risk management (The Open Group, 2012). Our novel reading of a dependency model as a model of operations is based on the consideration that a dependency model captures all statements that assure proper

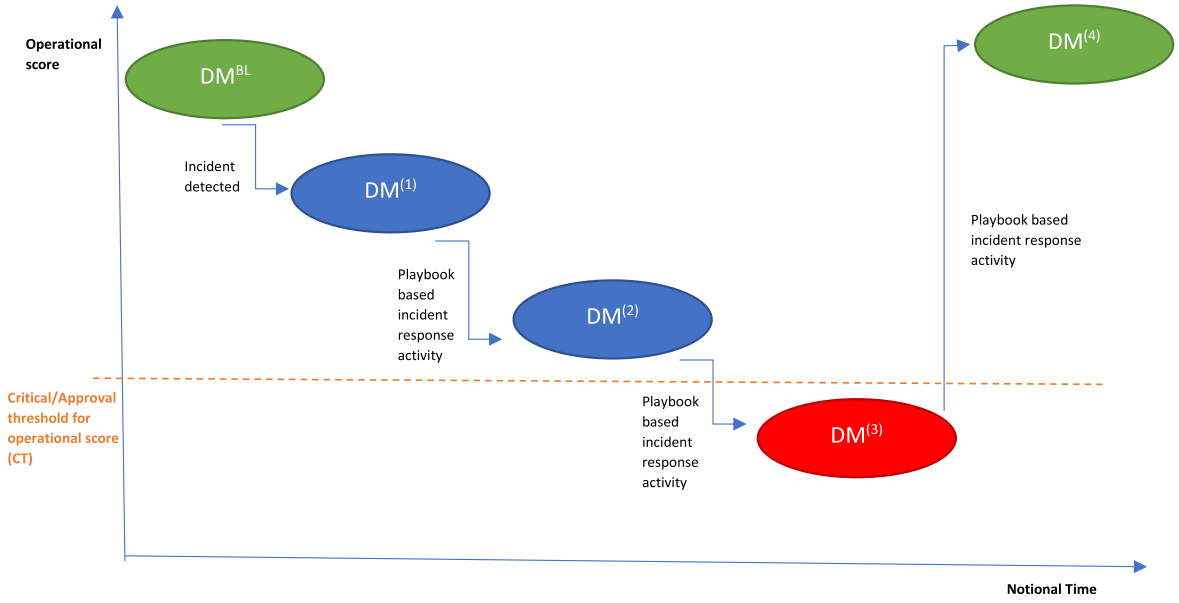

Fig. 3. Operational situational awareness evolving during incident response, based on dependency models and response activities.

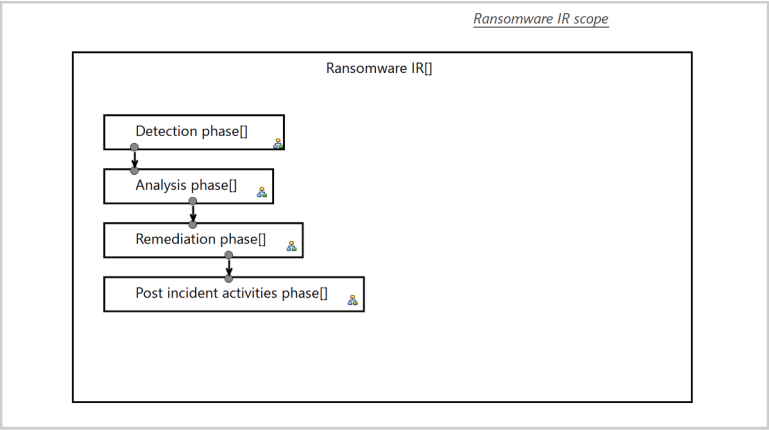

Fig. 4. Suggested phases of incident response.

operation. In this research, DM is an enabler of establishing and maintaining a consistent view on operations, providing a bi-directional link between risk management and incident response to address the gap we established in Section 1. Fig. 2 illustrates the organizational role of the model of operations, as we identify, implement and leverage in this paper. The model of operations is a representation of the organization's operations that can be used to feed risk management for operations-informed risk assessment. Risk management can provide feedback on the design of the model of operations, e.g., how operations can become more resilient to failures by introducing alternative dependencies to achieve operational goals (OR-typed dependencies, as we discussed Section 2). The model of operations can also feed incident response for operations-informed impact analysis, leading to an operations-informed response for incidents. Incident response can, in return, improve the credibility of the model of operations with respect to the actual organizational operation, e.g., by reflecting details and dependencies that were discovered during investigations but are missing from the model. An example of this is provided shortly in our case study (Section 4), when we revise a previously validated dependency model to accommodate lower-level dependencies for one of the elements. Such feedback from incident response can lead to a more accurate organizational situational awareness, which then feeds updates to both risk management and to incident response, for assessing future risks and designing and executing future IR playbooks respectively.

Fig. 3 illustrates the underlying approach of integrating DM into IR. Initially, a baseline dependency model of operations DM^{BL} exists, reflecting normal operations of the CNI systems. This dependency model depicts the system objective/s and dependencies in the form of operational statements with an associated operational value, calculated based on lower-level dependencies if these exist. Examples of such models are shown and discussed shortly. The dependency model of operations may be the result of a risk assessment activity (with operational values being assigned in the form of probabilities). Once an incident is identified, its impact analysis – which is a typical IR best practice activity (Ahmad et al., 2020; Bartock et al., 2016) – is captured in a new version of the model, $DM^{(1)}$, which describes the new situation from an operational perspective. The goal of IR is therefore to restore the operational status to DM^{BL} or to improve it beyond the original baseline. This already places a clear operational context on IR, which is missing from current playbook approaches.

Next, we can analyse the effect of IR activities on the dependency model of operations. Each planned IR activity can be associated with respective statements in the dependency model. The respective statements are the lowest level elements of the dependency model of operations that are identified as affected by the activity. The association between an activity and an affected statement clearly indicates if the activity has a restorative or an adverse effect with respect to the operational statement. These associations can be made in advance, i.e., when designing IR playbooks for future use; or while analyzing a specific incident and the proposed response, when an organization is trying to figure out the correct way to respond and how this will affect its business.

Before initiating an activity (including incident detection) during IR, an alternative operational status is considered/produced, based on the value change in affected statements. These are represented in derived models of operations, denoted $DM^{(x)}$. Inspired by a notation of denoting derivation; the number x can represent the number of scenarios that are generated during the IR up to a specific point in time. The overall change from the current existing operational value of a specific statement in the dependency model to IR-induced operational value is computed. This change reflects the impact of the incident or the incident response activity on the operations, and we refer to this metric as *Change in Operations* (CiO). This CiO metric allows the IR team:

1. to better understand the operational impact of a new incident. This can include the full realization of risk/compromise, by turning the overall value associated with an operational statement to zero (0);
2. to better understand the impact of performing an incident response activity;
3. to control and orchestrate the IR activities that are performed, e.g., by authorizing such activities with higher level management or coordinating them with stakeholders. The operations-informed playbook can hold a requirement to notify/approve the design/execution of a playbook activity if the resulting CiO to a high-level operational statement falls below a critical threshold (CT); or a requirement to coordinate with a regulator if the value associated with a specific operational statement drops below a critical threshold.

We implemented the operations-informed playbook using a software tool that we developed and offer as an open-source tool[3]. This tool allows us to rigorously evaluate the new concept and demonstrate its feasibility. The playbook figures that follow are screenshots of the tool's functional representations. This is designed to prove the technical validity and feasibility of the proposed approach.

4. Case study evaluation

This section demonstrates the value of using our new approach to IR Playbooks, by presenting a case study of ransomware IR playbook

[3] Security Modelling Framework, https://github.com/CardiffUniCOMSC/SecMoF/, accessed: 11/7/2023.

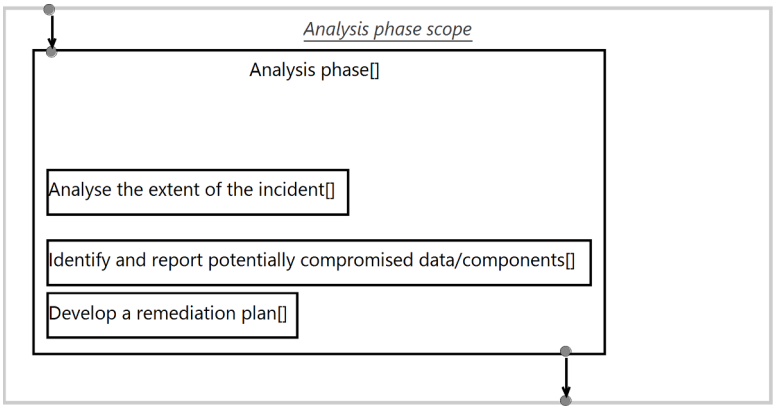

Fig. 5. The analysis phase activities.

design. The case study relies on real life incidents, with prominent examples identified in the Background section. Furthermore, the case study employs a real playbook, the Scottish Government Generic Ransomware Playbook (Scottish Government, 2020); adapting it to the specific case study as well as abstracting it for readability and proper scoping. The specific playbook does not limit the general applicability of our approach. The playbook was selected due to its relative clarity and organization, as its phases correspond well with IR best practices, such as those captured by NIST (Cichonski et al., 2012). Specifically, the ransomware IR playbook offered by the Scottish Government covers the different aspects of ransomware IR. The playbook relates to five phases: 1. Preparation, 2. Detection, 3. Analysis, 4. Remediation, and 5. Post Incident. These correspond – to a high degree – with the phases defined by NIST (1. Preparation, 2. Detection & Analysis, 3. Containment, Eradication and Recovery, and 4. Post-Incident activity). The preparation IR phase largely involves establishing an IR capability. In accord with the scope of this paper, this phase is represented by the activity of designing an IR playbook. A playbook details relevant processes, whose design is essential to organizational capacity building (Shaked and Reich, 2019). The remaining four phases relate to the content of the playbook, and as such are captured in our playbook's process model. Fig. 4 illustrates this. In this paper, for the purpose of brevity and readability, we concentrate on the Analysis and Remediation phases, while acknowledging that the design should include further breakdown of the other phases. This does not limit the applicability or the generality of the proposed approach to create operations-informed playbooks.

The Analysis phase includes three activities: analyze the extent of the incident, identify and report potentially compromised data, and develop a remediation plan. We adapt the second activity to the context of CNI by extending it to relate to components and not only data. Compromised components may have impact with respect to integrity and availability, and in some cases even confidentiality (e.g., when a cryptographic mechanism fails); and these notions of impact seem to be missing in the original Scottish Government playbook. While beyond the scope of our work, we note – as further elaboration – that each activity includes suggestions for lower-level activities. In the case of the second activity, such lower-level activities include: "Identify any data impacted by the ransomware attack" and "Engage data owners and the business to understand the business impact of the compromised data." Our adaptation calls for revising these as "Identify any data or component impacted by the ransomware attack" and "Engage data owners, CNI architects or systems engineers and the business to understand the business/service impact of the compromised data and/or component." This adaptation to CNI is noteworthy as it demonstrates: 1. that the original playbook fails to properly relate to ransomware attacks in CNI context; 2. that playbooks should be carefully adapted to their context of use. We capture the Analysis phase's high-level activities in our IR process model (Fig. 5).

The Remediation phase also includes three high-level activities:

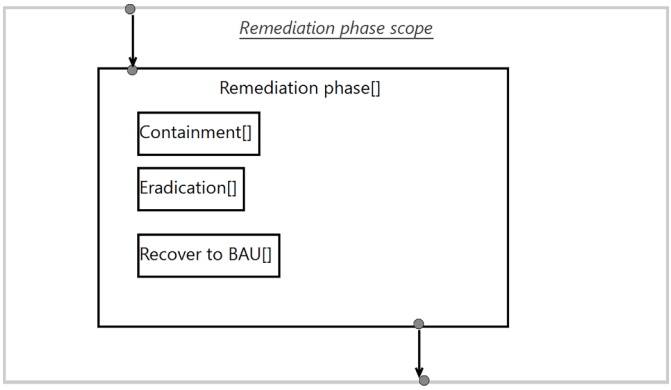

Fig. 6. The remediation phase activities.

Containment, Eradication, and Recover to BAU (business as usual). This is also captured in the IR process model (Fig. 6). Each of these activities includes suggested lower-level activity guidelines, such as "Reduce any further malicious activity by quarantining affected systems and removing them from the network, where possible, or applying access controls to isolate from production networks" (in Containment), "Reinstall any standalone systems from a clean OS back-up before updating with trusted data back-ups" (in Eradication), and "Reintegrate previously compromised systems" (in Recover to BAU). However, the previous phase's "Develop a remediation plan" activity requires lower-level details of the remediation phase's activities to be designed based on the analysis of the incident and its impact. This necessitates a coherent view of the operations to be consistently maintained between the Analysis and the Remediation phases. And this is the point at which playbooks typically break and fail.

We now show how contextualizing the playbook process with respect to the relevant organizational/service operations contributes to maintaining a coherent view in support of designing and executing the IR remediation plan. First, we associate the playbook with a model of operations. This model of operations is based on a previously established dependency model for SCADA systems (Cherdantseva et al., 2022). We limit our discussion to a binary model of operations, with the value '1' representing an "operational" status for a specific statement and the value '0' representing a "non-operational" status for a specific statement. We assign the operational value for the model statements by replacing the values of all statements typed "uncontrollable" (the leaf nodes in the dependency model) to the value '1', denoting a fully functional operational status (i.e., a baseline with no operational issues). This is done in order to provide a clear and easily communicable representation of our approach. There is no loss of generality in this simplification. Specifically, operational models can be used with

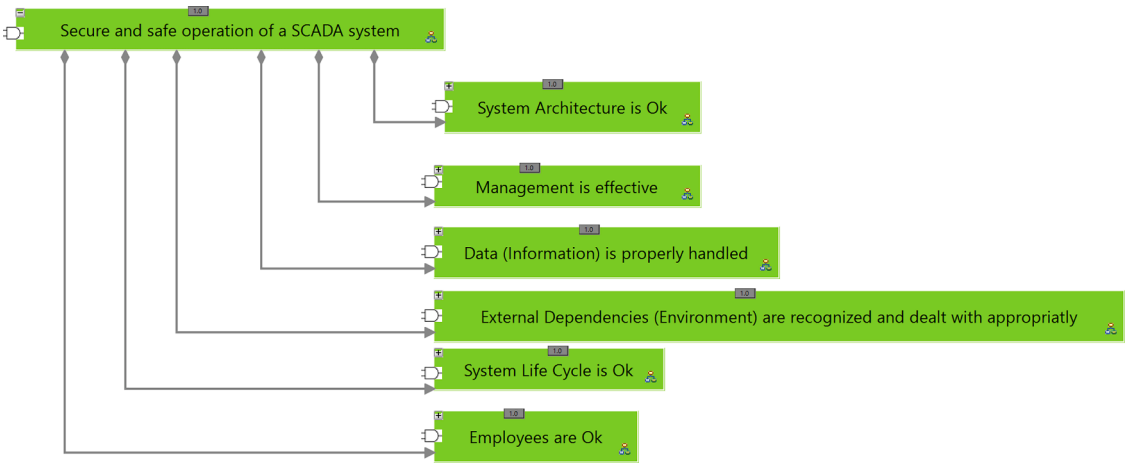

Fig. 7. The top-level hierarchy of the SCADA-DM.

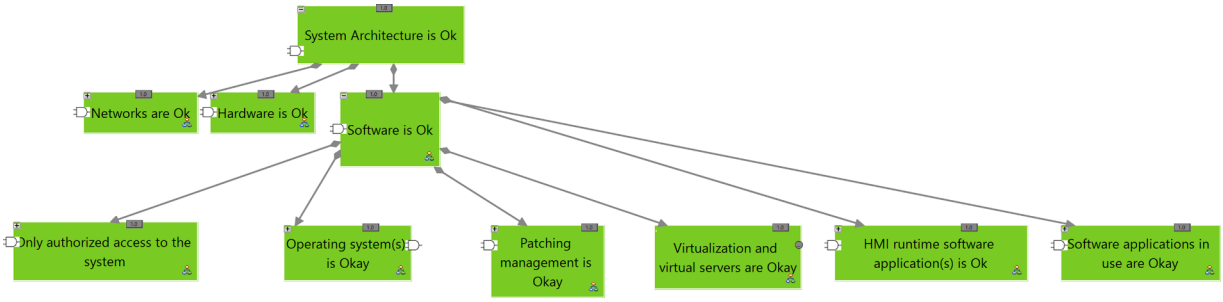

Fig. 8. Further decomposition of system architecture and software dependencies.

probability values to denote a more quantitative status of operation. Discussing various operational model designs, their advantages and limitations is beyond the scope of this paper. We, therefore, focus on a simple yet still effective operational model, as established shortly by its integration as the context in our playbook.

Fig. 7 shows the top hierarchy of the adopted SCADA dependency model (henceforth abbreviated "SCADA-DM"). Fig. 8 shows further decomposition of the "System Architecture is Ok" statement (which appears on the previous figure) in terms of its dependencies, as well as further breakdown of the "Software is Ok" statement dependencies. The

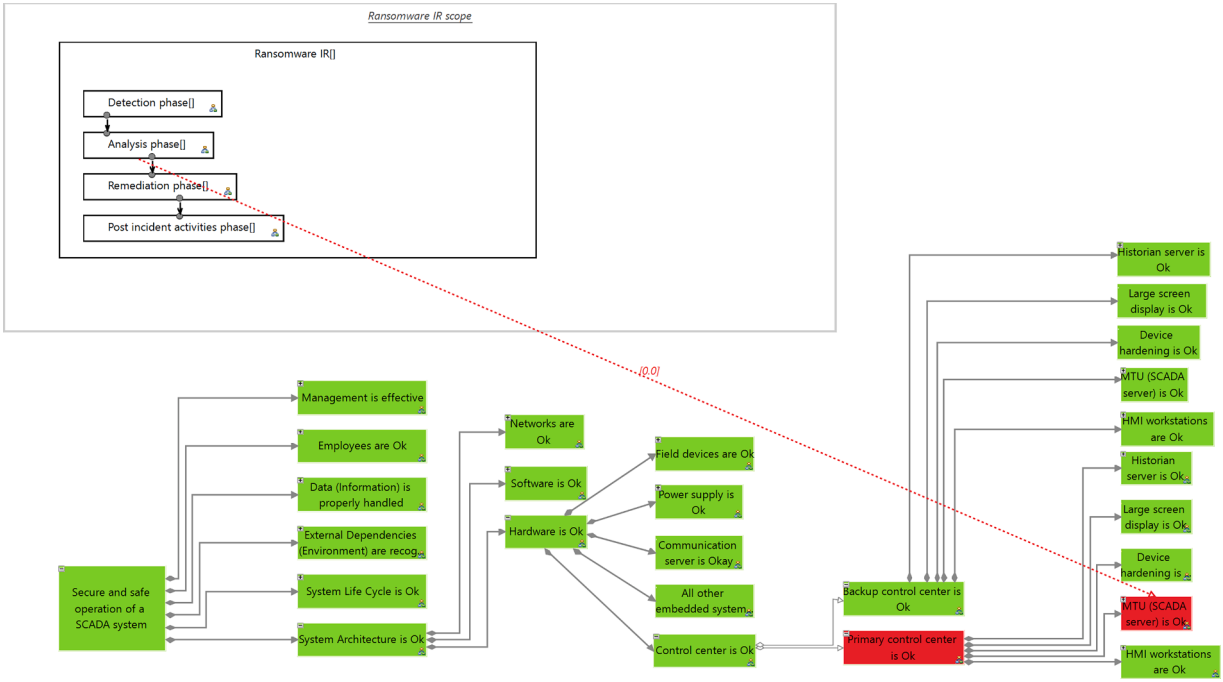

Fig. 9. Operations-informed ransomware playbook, high-level.

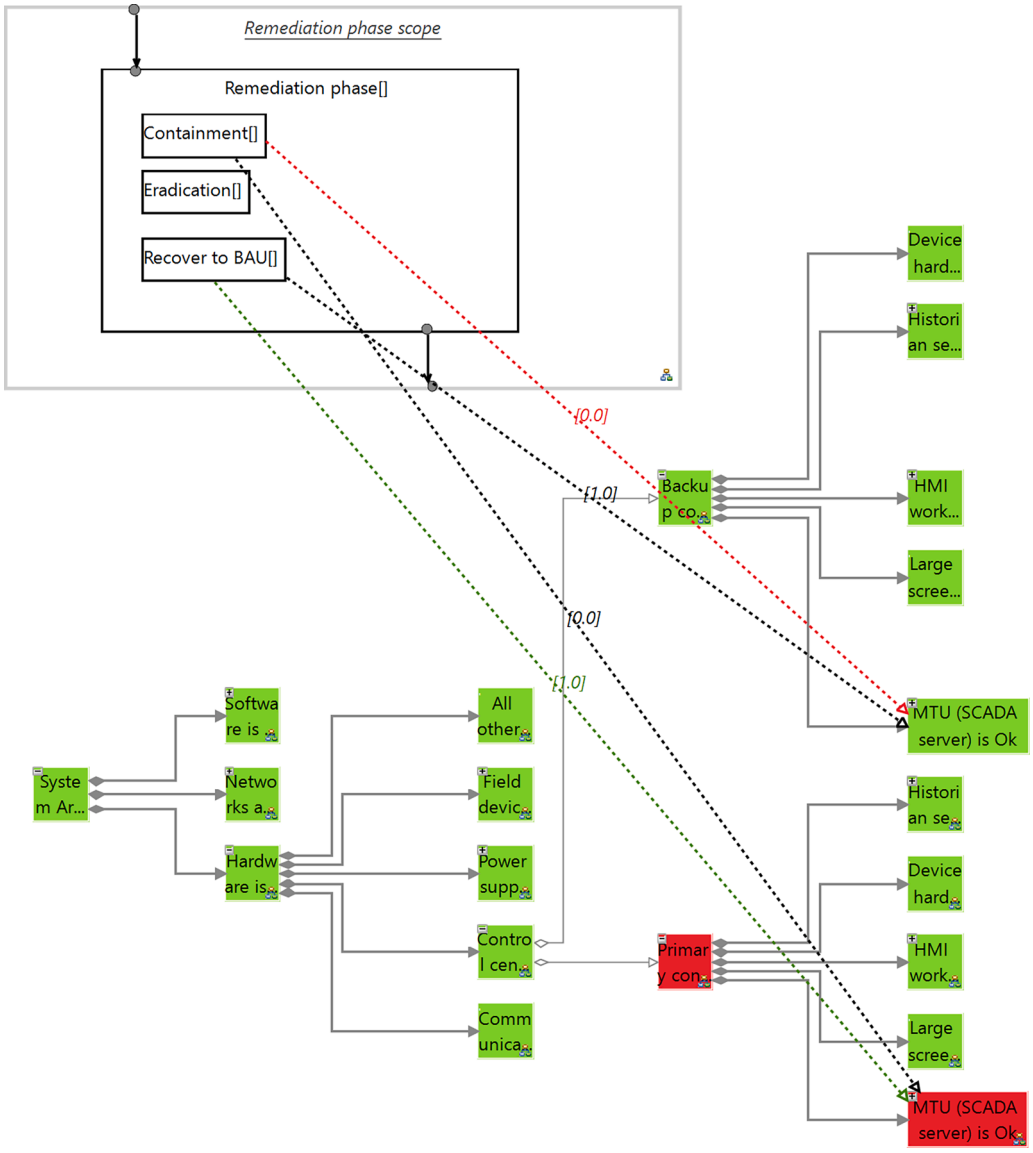

Fig. 10. Operations-informed remediation plan.

DM representations should be read as follows. The shade of each statement element represents its operational status: green for '1' (operational), red for '0' (non-operational). A hollow arrowhead represents an 'or' dependency whereas a filled arrowhead denotes an "and" dependency. The type of dependency is also denoted by an or/and gate attached to the statement element. Uncontrollable statement elements (i.e., statements that have no lower-level dependencies in the model or whose status is directly specified and not computed by lower-level dependencies) do not have a logical gate attached. We assign a CT value with respect the highest hierarchy statement "Secure and safe operation of a SCADA system": CT = 1; denoting that any activity which reduces the operational status of the system should be approved/acknowledged by relevant stakeholders.

Similar to the generic playbook offered by the Scottish Government, the SCADA-DM should also be adapted to the specific system in question, to coincide with organizational and systems structures and dependencies. For example, the dependencies of the "Virtualization and virtual servers are Okay" statement (Fig. 8) can be elaborated to include specific servers. For the sake of brevity and readability, we do not make such adaptations in this paper. Furthermore, relating to a previously established dependency model allows us to reflect on the contribution of our approach to the overall cyber security effort, which we discuss in Section 5. For this case study, we performed a trivial adaptation of the SCADA-DM: the original dependency model identified a primary control center with its lower-level dependency as well as a backup control center with no breakdown of its dependencies; and we extended the SCADA-DM to detail the backup control center's dependencies (currently considered as similar to the primary control's dependencies, i.e., no additional concepts are added). This is shown in Fig. 9, which is further discussed shortly.

The contextualization of the IR process model with respect to the model of operations SCADA-DM is achieved by associating activities in the process model with affected statements in SCADA-DM. This can be done in any relevant hierarchy in both models, as we demonstrate shortly. As a general recommendation, one should aspire to associate each relevant activity with the lowest-level statement available in the dependency model. This will facilitate the most granular assessment of how the incident and the incident response affect the operational status.

Let us now consider a specific case of a Master Terminal Unit (MTU) being compromised with a ransomware as our cyber security incident. Fig. 9 shows the high-level IR process model and the SCADA-DM (filtered for representation purposes). The figure also shows a new conceptual element in the form of a link (graph edge) between a process model activity and a dependency model statement. This link conveys a

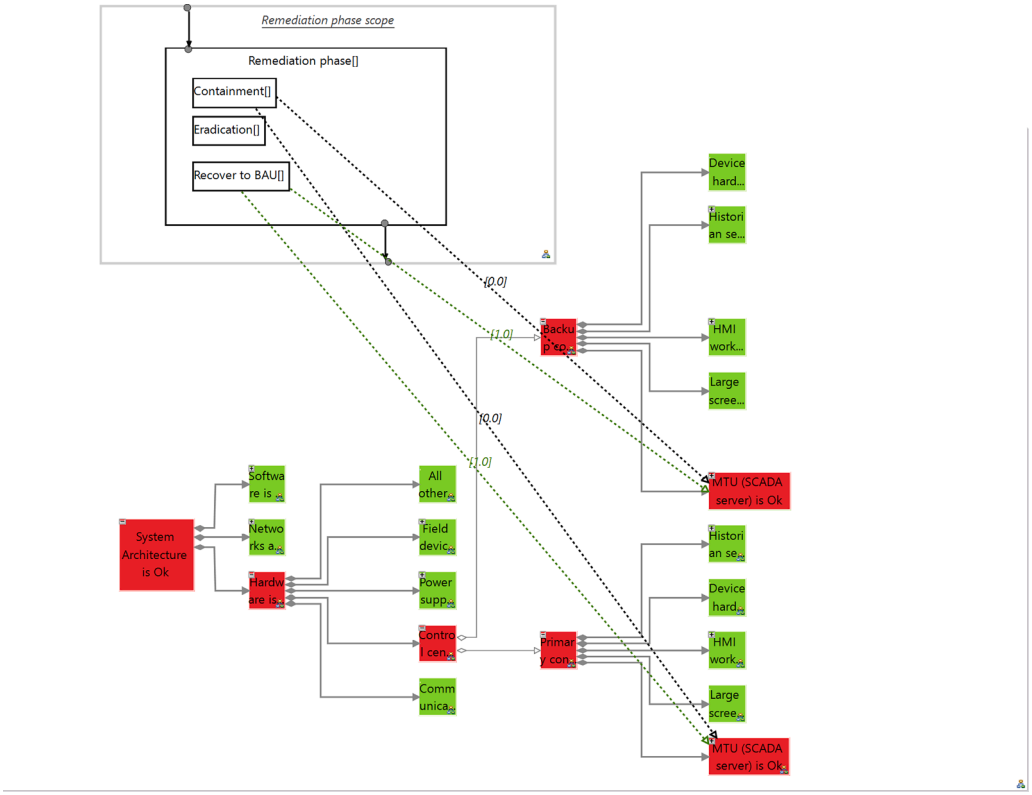

Fig. 11. A what-if analysis of the operations-informed remediation plan.

new operational value for the statement affected by the activity (in this case 0.0, which should be read simply as "0" in our binary ranking). The representation shows the link as red to denote its malign effect. The figure explicitly captures the IR best practice of analyzing the affected entities and impact of the incident (as specified in the Scottish government playbook, for example). In the specific case, the incident analysis resulted in the understanding that only the MTU of the primary control center is compromised, i.e., that specific MTU – which we refer to as Primary-MTU – is identified as the sole affected component. Accordingly, the Primary-MTU operational status is reduced from '1' to '0'. If this analysis is enacted, the impact on the system level operation can be evaluated. In this case, the operational status of the primary control center is automatically updated to '0', based on its "AND" typed dependency on that specific MTU. A CiO metric assigned to that status - $CiO_{Primary\text{-}MTU}$ – is therefore 1. However, the overall system operation is not affected, as "The control center is Ok" statement has "OR" typed dependencies to the two different control centers. A CiO metric assigned to the overall system status – $CiO_{SCADA\text{-}Sys}$ – is therefore 0.

We now proceed to the design of the remediation phase. In general, a best practice is to find the root cause of the incident. Identifying the root cause of a cyber event is important to planning the remediation, as overlooking vulnerabilities may inadvertently leave weaknesses that adversaries may exploit again (Bartock et al., 2016). Ransomware attacks may rely on vulnerabilities, and, accordingly, be fully mitigated by addressing these vulnerabilities (e.g., by applying security patches). The aforementioned WannaCry ransomware exemplifies this (US Department of Homeland Security's National Cybersecurity and Communications Integration Center, 2017). Let us assume that the detected ransomware in Primary-MTU was enabled by a vulnerability which can be solved by applying a patch to the MTU's operating system. If we wish to prevent similar incidents, it is therefore wise to apply the patch to all components that have this vulnerability. An additional immediate candidate for patching – alongside Primary-MTU – is the MTU of the back control center, which we refer to as Secondary-MTU and is an exact replica (bar some software configuration) of Primary-MTU. A resulting plan can be to isolate both components from the network (as part of the Containment activities) and patch them (as part of the Eradication activities) before eventually restoring them to fully operational status (as part of the Recover to BAU activities). Fig. 10 presents the contextualized version of this plan. It explicitly states that the Containment effort impacts the operation statuses of the MTUs, changing them to "0". The color legend, based on the models, may assist the designer: the link to the Primary-MTU operational statement is black, denoting it has no effect on it, as its operational status has already been downgraded by the ransomware, as we noted before; whereas the link to the Secondary-MTU operational statement is red, denoting this might have an adverse effect on the operations. Similarly, the Recover to BAU effort restores the operational status of both components to "1"; with the link to the Secondary-MTU statement appearing in black, thus having no effect with respect to the current situation, and the link to the Primary-MTU statement appearing in green to denote a restorative effect with respect to the current situation. As a side note, we wish to state that the links' color coding may be adapted or revised by practitioners of our approach; this does not affect the generality and applicability of the overall approach.

A what-if analysis of analyzing the execution of the remediation activities is useful in evaluating the effect on the system level operation. Fig. 11 illustrates such an analysis of executing the Containment effort. The execution leads to non-operational status of the "System Architecture is Ok" statement, and in turn, adversely affects the entire system's operational status, which depends on it (Fig. 7). The overall system operational status – represented by the "Secure and safe operation of a SCADA system" statement – drops from "1" to "0" ($CiO_{SCADA\text{-}Sys}$=1), below the CT (of "1"), possibly requiring such a remediation plan to be approved and well-coordinated with stakeholders prior to its execution.

Fig. 12 presents an alternative remediation plan. This design of the remediation involves performing the containment, eradication and recovery separately and serially for each MTU. First, remediation of

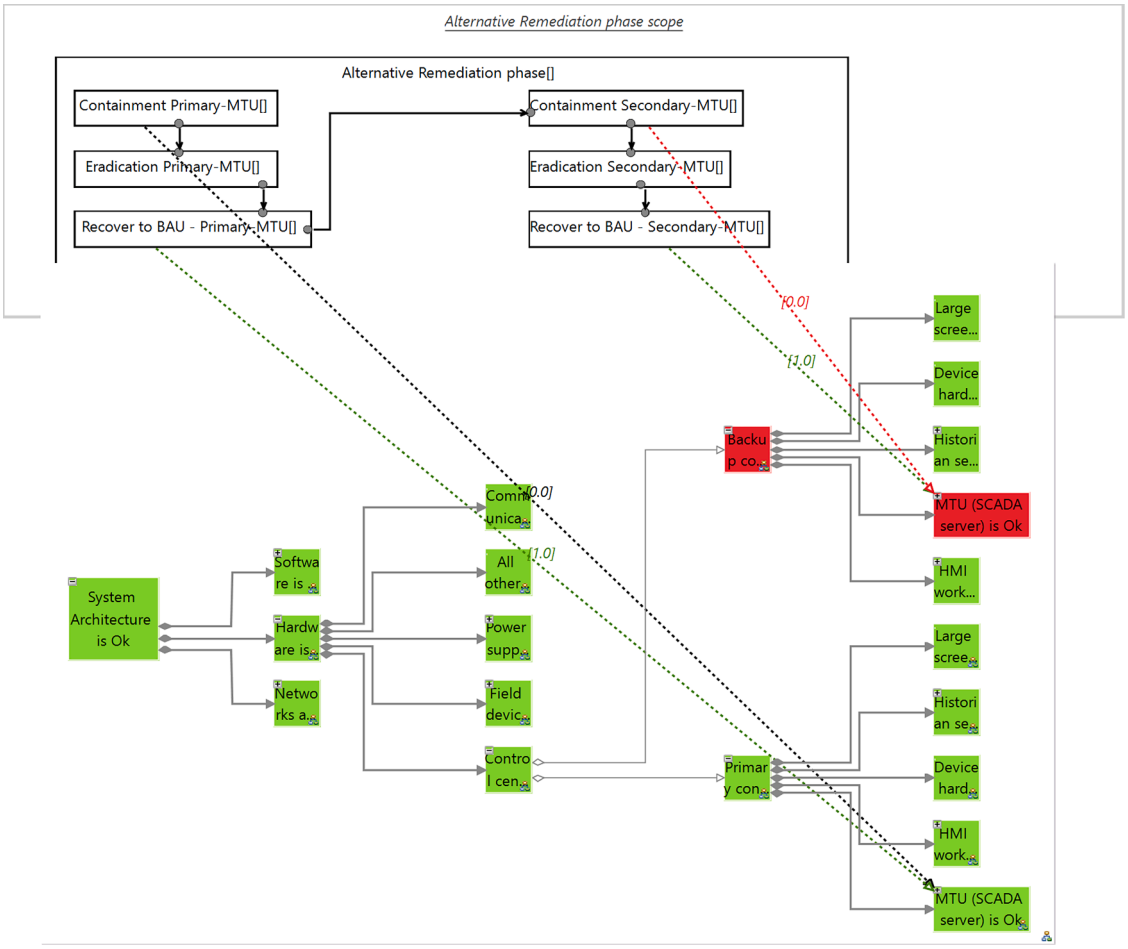

Fig. 12. An alternative remediation plan.

Primary-MTU is addressed, and only then remediation of Secondary-MTU is performed. The figure also details the what-if analysis simulation of the process, up to and including the execution of the "Containment Secondary-MTU" activity. The system's operational status remains "1" throughout the execution of this plan, and, therefore, such a plan can be executed without requiring additional coordination.

5. Discussion

Playbooks are regarded as crucial element for effective incident response (IR). However, there are still significant gaps in establishing their design and effectiveness, especially with respect to possible operational impact. This paper introduces a novel concept of an operations-informed incident response playbook, which integrates a model of operations with an incident response process model. This elaboration of the playbook concept and its realization lay the rigorous foundations for an operations- and business-oriented IR and for relevant decision making.

Our generalized case study implementation shows the value of using our new operations-informed playbooks-based IR approach. We have shown two alternative designs of a playbook process and how each of them may affect the operations by relating the process to a threshold value (CT) which characterizes an operational status. This demonstrates how the new approach promotes the ability to communicate the design of the playbook with different stakeholders, including management. When presented with multiple IR playbook options, for example, executives may prefer a playbook design which is less harmful to the operations.

A new quantitative metric – Change in Operations (CiO) – supports the contextualization of an incident as well as of the incident response with respect to their impact on operations: (1) the metric first indicates the change in operations due to the occurrence of the incident, based on the affected system dependencies; (2) the metric is then used during IR, whenever applicable, to calculate how a response activity can affect the overall operational status, based on association of activities with their respective impact on operational system statements. This can be done in advance, i.e., when prescribing IR activities for different scenarios; or on-the-fly, when responding to an incident.

While our case study only uses a single critical threshold, we stress that multiple critical thresholds may be used. These can be designed to meet the requirements of different stakeholders or to stress that an incident or an IR procedure that has specific effects requires authorization by a designated stakeholder. As an illustration, an additional critical threshold which relates to the "Primary control station is Ok" statement in our case study – denoted CT_2 – may have been introduced to trigger notification to the primary control station manager upon the detection of the incident which affected this operational component, seeking her further involvement. Future research may seek to incorporate additional metrics into playbooks, specifically those associating the model of operations with business and/or performance metrics, such as revenues, reputation and others. This can promote the ability to quantify the impact of an incident and of incident response with respect to organizational objectives.

The lack of an operational statement (in the dependency model) to be associated with an incident or an IR activity may reflect lack of impact (with respect to operations) of the specific incident or IR activity. However, it may also indicate an incomplete/inaccurate risk assessment or poor understanding of operational dependencies. One such example

appears in our case study: the "MTU (SCADA server) is Ok" statement in the SCADA-DM has two lower level "and"-typed dependencies: "Processor and processing power is Ok" and "RAM is Ok." These do not relate to the issue analyzed to affect the MTU operations in our case study (a ransomware compromising the component). Other software related statements also do not relate to the MTU. Eventually, the effect of analyzing the incident was established with respect to the "MTU (SCADA server) is Ok" statement directly. This suggests that the SCADA-DM can be extended to include other dependencies of the MTU's operation. Such indication, facilitated by our novel operations-informed playbook, can play a significant part in establishing the highly desirable feedback loop to support organizational learning aimed to improve the cyber security posture (Ahmad et al., 2020).

Our current effort is limited to integrating dependency models with a flow-chart styled process descriptions as a detailed illustration of the operations-informed incident response playbook. However, the specific selections (in dependency models and in a specific process model) are merely representative, and they do not limit the general applicability of our approach to integrate other forms of operational dependencies and process models. Future research can demonstrate such applicability by integrating other models.

Declaration of Competing Interest

The authors declare that they have no known competing financial interests or personal relationships that could have appeared to influence the work reported in this paper.

Data availability

All data is provided in full in the *Case study evaluation* section of this paper.

Acknowledgments

This work was supported by the Engineering and Physical Sciences Research Council (EPSRC) (Grant number EP/V038710/1).

References

Adamov, A, Carlsson, A, Surmacz, T., 2019. An analysis of lockergoga Ransomware. 2019 IEEE East-West Design and Test Symposium, EWDTS 2019. https://doi.org/10.1109/EWDTS.2019.8884472.

Agrafiotis, I, Nurse, JRC, Goldsmith, M, Creese, S, Upton, D., 2018. A taxonomy of cyber-harms: defining the impacts of cyber-attacks and understanding how they propagate. J. Cybersecur. 4 https://doi.org/10.1093/cybsec/tyy006.

Ahmad, A, Hadgkiss, J, Ruighaver, AB., 2012. Incident response teams—challenges in supporting the organizational security function. Comput. Secur. 31, 643–652. https://doi.org/10.1016/j.cose.2012.04.001.

Ahmad, A, Desouza, KC, Maynard, SB, Naseer, H, Baskerville, RL., 2020. How integration of cyber security management and incident response enables organizational learning. J. Assoc. Inf. Sci. Technol. 71, 939–953. https://doi.org/10.1002/asi.24311.

Ahmad, A, Maynard, SB, Desouza, KC, Kotsias, J, Whitty, MT, Baskerville, RL., 2021. How can organizations develop situation awareness for incident response: a case study of management practice. Comput. Secur. 101, 102122 https://doi.org/10.1016/j.cose.2020.102122.

Akbanov, M, Vassilakis, VG, Logothetis, MD., 2019. WannaCry ransomware: analysis of infection, persistence, recovery prevention and propagation mechanisms. J. Telecommun. Inf. Technol. 113–124. https://doi.org/10.26636/jtit.2019.130218.

Applebaum, A, Johnson, S, Limiero, M, Smith, MJ., 2018. In: . Institute of Electrical and Electronics Engineers Inc., pp. 8–15. https://doi.org/10.1109/NCS.2018.00007

Bartock, M, Cichonski, J, Souppaya, M, Smith, M, Witte, G, Scarfone, K., 2016. Guide for cybersecurity event recovery. NIST Spec. Publ., 800-184 https://doi.org/10.6028/NIST.SP.800-184.

Bodeau D, Graubart R. Cyber Resiliency Engineering Framework 2011. https://dragos.com/blog/crashoverride/index.html (accessed June 22, 2023).

Bodeau D, Graubart R. Structured Cyber Resiliency Analysis Methodology (SCRAM). 2016.

Canadian Centre for Cyber Security. Ransomware playbook. 2021.

Cherdantseva, Y, Burnap, P, Nadjm-Tehrani, S, Jones, K., 2022. A configurable dependency model of a SCADA system for goal-oriented risk assessment. Appl. Sci. 12, 4880. https://doi.org/10.3390/app12104880.

Cichonski, P., Millar, T., Grance, T., Scarfone, K., 2012. Computer security incident handling guide : recommendations of the national institute of standards and technology. NIST Spec. Publ, 800-61. https://doi.org/10.6028/NIST.SP.800-61r2.

Dragos Inc. CRASHOVERRIDE—analysis of the threat to electric grid operations 2017. https://www.dragos.com/resource/crashoverride-analyzing-the-malware-that-attacks-power-grids/(accessed June 22, 2023).

Freas, RL, Adair, HF, Hammad, E, 2022. An engineering process framework for cybersecurity incident response assessment. In: 5th IEEE Conference on Dependable and Secure Computing, DSC 2022 and SECSOC 2022 Workshop, PASS4IoT 2022 Workshop SICSA International Paper/Poster Competition in Cybersecurity. Institute of Electrical and Electronics Engineers Inc. https://doi.org/10.1109/DSC54232.2022.9888795

Ghafur, S, Kristensen, S, Honeyford, K, Martin, G, Darzi, A, Aylin, P., 2019. A retrospective impact analysis of the WannaCry cyberattack on the NHS. NPJ Digit. Med. 2 https://doi.org/10.1038/s41746-019-0161-6.

Huang C-T, Sakib MN, Njilla L, Kamhoua C. A game theoretic approach for making IoT device connectivity decisions during malware outbreak—a game theoretic approach for making IoT device connectivity decisions during malware outbreak. 2019.

Kertzner P, Carter C, Hahn A. Crown Jewels Analysis (CJA) for Industrial Control Systems (ICS). 2022.

Korn, EB, Fletcher, DM, Mitchell, EM, Pyke, AA, Whitham, SM., 2021. Jack pandemus–Cyber incident and emergency response during a pandemic. Inf. Secur. J. 30, 294–307. https://doi.org/10.1080/19393555.2021.1980159.

Martin, G, Ghafur, S, Kinross, J, Hankin, C, Darzi, A., 2018. WannaCry—a year on. BMJ 361. https://doi.org/10.1136/bmj.k2381 (Online).

Microsoft. Microsoft's Incident response playbooks n.d. https://learn.microsoft.com/en-us/security/operations/incident-response-playbooks (accessed June 2, 2023).

Nagaraju, V, Fiondella, L, Wandji, T, 2017. A survey of fault and attack tree modeling and analysis for cyber risk management. 2017 IEEE International Symposium on Technologies for Homeland Security (HST). IEEE, pp. 1–6. https://doi.org/10.1109/THS.2017.7943455.

Nargiza, Akramova, 2022. Ransomware: analysis of 2019 LockerGoga cyber-attack to Norsk Hydro multinational company and its countermeasures. Eur. J. Media Commun. 9.

Naseer, H, Maynard, SB, Desouza, KC., 2021. Demystifying analytical information processing capability : the case of cybersecurity incident response. Decis. Support Syst. 143, 113476 https://doi.org/10.1016/j.dss.2020.113476.

OASIS Open. CACAO Specification 2021. https://docs.oasis-open.org/cacao/security-playbooks/v1.0/cs02/security-playbooks-v1.0-cs02.html (accessed March 13, 2023).

Onwubiko, C., 2018. CoCoa : an ontology for cybersecurity operations center analysis process. In: 2018 International Conference on Cyber Situational Awareness, Data Analytics and Assessment (Cyber SA). https://doi.org/10.1109/CyberSA.2018.8551486.

Rotibi, AO, Saxena, N, Burnap, P, Tarter, A., 2023. Extended dependency modeling technique for cyber risk identification in ICS. IEEE Access 11, 37229–37242. https://doi.org/10.1109/ACCESS.2023.3263671.

Schlette, D, Caselli, M, Pernul, G., 2021. A comparative study on cyber threat intelligence: the security incident response perspective. IEEE Commun. Surv. Tutor. 23, 2525–2556. https://doi.org/10.1109/COMST.2021.3117338.

Scottish Government. Cyber incident response: ransomware playbook. 2020.

Shaked, A, Reich, Y., 2019. Designing development processes related to system of systems using a modeling framework. Syst. Eng. 22, 561–575. https://doi.org/10.1002/sys.21512.

Shaked, A, Cherdantseva, Y, Burnap, P., 2022. Model-based incident response playbooks. In: ACM International Conference Proceeding Series, Association for Computing Machinery. https://doi.org/10.1145/3538969.3538976.

Shaked, A., 2023. A model-based methodology to support systems security design and assessment. J. Ind. Inf. Integr. 33, 100465 https://doi.org/10.1016/j.jii.2023.100465.

Spaulding S. Transportation cybersecurity: protecting planes, trains, and pipelines from cyber threats. 2021.

Stamper, M, Hayslip, G, Bonney, B., 2019. Ten observations on why incident response needs your attention. EDPACS 59, 19–23. https://doi.org/10.1080/07366981.2019.1580409.

Staves, A, Anderson, T, Balderstone, H, Green, B, Gouglidis, A, Hutchison, D., 2022. A cyber incident response and recovery framework to support operators of ICS and critical national infrastructure. Int. J. Crit. Infrastruct. Prot., 100505 https://doi.org/10.1016/j.ijcip.2021.100505.

Stevens, R, Votipka, D, Dykstra, J, Tomlinson, F, Quartararo, E, Ahern, C, et al., 2022. How ready is your ready? Assessing the usability of incident response playbook frameworks. In: CHI conference on human factors in computing systems, New York, NY, USA. ACM, pp. 1–18. https://doi.org/10.1145/3491102.3517559.

Stouffer, K, Pease, M, Tang, C, Zimmerman, T, Pillitteri, V, Lightman, S, 2022. Draft NIST SP 800-82r3, Guide to Operational Technology (OT) Security. https://doi.org/10.6028/NIST.SP.800-82r3.ipd.

The Open Group, 2012. Dependency Modeling (O-DM) Constructing a Data Model to Manage Risk and Build Trust between Inter-Dependent Enterprises.

Tsvetanov, T, Slaria, S., 2021. The effect of the Colonial Pipeline shutdown on gasoline prices. Econ. Lett. 209, 110122 https://doi.org/10.1016/j.econlet.2021.110122.

U.S. Government Accountability Office. SolarWinds Cyberattack Demands Significant Federal and Private-Sector Response (infographic) 2021. https://www.gao.

gov/blog/solarwinds-cyberattack-demands-significant-federal-and-private-sector-response-infographic (accessed March 13, 2023).
US Department of Homeland Security's National Cybersecurity and Communications Integration Center. What is WannaCry/WanaCrypt0r? 2017.
Van der Kleij, R, Kleinhuis, G, Young, H., 2017. Computer security incident response team effectiveness: a needs assessment. Front. Psychol. 8 https://doi.org/10.3389/fpsyg.2017.02179.
van der Kleij, R, Schraagen, JM, Cadet, B, Young, H., 2022. Developing decision support for cybersecurity threat and incident managers. Comput. Secur. 113 https://doi.org/10.1016/j.cose.2021.102535.
Young, W, Leveson, N., 2013. Systems thinking for safety and security. In: ACM International Conference Proceeding Series, pp. 1–8. https://doi.org/10.1145/2523649.2530277.

Avi Shaked is a Senior Research Associate at the University of Oxford's Department of Computer Science. He received the BSc degree in Physics and Computer Science, the MSc degree in Physics and the PhD degree in Systems Engineering, all from Tel Aviv University. Dr. Shaked has over 15 years of experience in research and development leadership roles. His research interests include systems thinking, formal modelling, systems security and decision support systems.

Dr **Yulia Cherdantseva** is a Senior Lecturer at the School of Computer Science & Informatics at Cardiff University. She is the Director of Cardiff University's Academic Center of Excellence in Cyber Security Education (ACE-CSE). Dr Cherdantseva is a co-director of the Digital Transformation University Innovation Institute. She is a member of the Executive Board of the CyBOK project, a national project funded by the National Cyber Security Program focused on codifying the cyber security knowledge.

Pete Burnap is Professor of Data Science & Cybersecurity in the School of Computer Science & Informatics. He is Director of the Cardiff Center for Cyber Security Research, which is recognized as an Academic Center of Excellence in Cyber Security Research (ACE-CSR) by the National Cyber Security Center and EPSRC. He has been involved in research grants worth in excess of £23m, leading large awards from EPSRC, ESRC and industry on the topic of cyber security analytics – the fusion of artificial intelligence, cybersecurity and risk. His work, developed in collaboration with key partners and collaborators, focusses on the development of novel approaches to automated cyber defence.

Peter Maynard is a Research Associate at the School of Computer Science & Informatics at Cardiff University. He has a Ph.D. in Critical Infrastructure Security, From Queen's University Belfast (UK), where he developed and performed novel attacks on Industrial Control System (ICS) networks. He spent a while hunting ICS malware and investigating targeted intrusions e.g. HAVEX and CrashOverride to derive a set of commonalities between intrusions for use in developing future detection systems. Worked on EU FP7 PRECYSE, EU H2020 5G-ENSURE and several EPSRC and DASA projects. He worked in a security start-up company developing a novel Root of Trust mechanisms and lightweight authentication cryptographic protocols for use in machine-to-machine networks.