SOTER: A Playbook for Cyber Security Incident Management

Abstract – SOTER[1], a cyber security incident management playbook, is developed to provide a comprehensive model to manage cyber security incidents, particularly for the cyber security operations centre. The proposed playbook is adaptive, cross-sectorial, and process driven. Each key components of the incident management playbook are outlined and discussed. Further, a lexicon based on equivalence mapping is developed and used to map existing cyber security incident vocabulary and taxonomy into a common and consistent lexicon to aid understanding among incident management stakeholder communities – national, government and private sectors. A versatile workbook model has been explored which proves to be adaptable to serve a wide range of cases for successfully managing government and private sector security operations centre.

Cyber security incident sharing partnership, formalism for metric and measurements of cyber security incident parameters, and cyber security incident classification and prioritisation schemes are presented, and finally, cyber security incident 'plays' and playbook templates are discussed.

Index Terms— *Soter; Cyber Security Operations Centre; Cyber Security; Cyber Incident Management Playbook; Cybersecurity Incident Response; Incident Response Management*

I. Introduction

Cyber incident can be likened to an emergency. It can have serious consequences [1]. The longer it is left unattended or inappropriately controlled, the severe the consequences. For example, if a cyber incident is not swiftly mitigated there is a likelihood the attack will cause further damages, the adversary could delete or destroy evidential data to avoid detection or prosecution, exfiltrate business data, plant backdoors, and stage multi-step attacks leading to exploitation of interconnected services and organisations.

Cyber incident like an emergency is often unannounced, abrupt, urgent and serious; therefore, the key to mitigating, containing and controlling cyber incidents is to be prepared. Even when the incident is foreseen (or foretold) like with severe weather predictions or forecasts, or threat intelligence and vulnerability announcements, or with early warning systems, the preparedness of the institution or mission will determine how quickly the incident can be controlled, contained or/and its impact minimised. Preparedness is an important aspect toward effective cyber incident management. It encompasses, planning, readiness, exercises and rehearsals, policy, detection, reporting, response, recovery and post incident report.

With most emergencies, when not controlled or mitigated immediately could lead to loss, e.g. loss of life, loss of possession (e.g. material loss), loss of service, loss of brand etc. These losses are often exacerbated when the emergency or incident is uncontrolled for a prolonged period. This could be as a result of lack of standard *playbook and operative procedures*. It has been argued that the lack of *standard playbook*, and "poor emergency management governance is a main reason for the increase of natural disasters that are otherwise preventable" [2]. Emergency services, for instance, the fire service, accident and emergency of a hospital, highway patrol etc., are underpinned on prior agreed set of rules, protocols, procedures and actions, that are followed in the event of an emergency. Take the fire service as an example, if there are no prior agreed set of rules to follow in the face of fire outbreak, then firemen will react differently, and their responses are bound to be chaotic, uncoordinated, ineffective and the outcome is likely to be inefficient. Therefore, agreeing prior systematic fire drills, health and safety procedures and protocols to combating fire incidents becomes paramount. The same can be said of Cyber Security Operations Centre (CSOC[2]), or Security Operations Team of an organisation or a mission. When a security incident, data breach, policy violation or compromise occurs, the first people that are contacted is the Security Operations Centre (SOC) of the organisation who provide the audacious task of safeguarding, protecting,

[1] Soter – "is a Greek god personified for safety, preservation and deliverance from harm" – https://en.wikipedia.org/wiki/Soter_%28daimon%29

[2] In this paper we use CSOC, SOC, CyberOps or SecOps interchangeably to mean one and the same thing, and throughout this papers, we will use SOC for all explanations henceforth.

monitoring and managing security incidents for the organisations. This is further compounded by the myriad of assets, systems and services that the SOC are tasked to monitor, their dynamic nature, and the rapid changing situations of these services; maintaining situational awareness of these services in the face of the increasing complexity and frequency of cyber-attacks against these services is challenging in itself [3].

Unfortunately, most SOCs do not have standard incident management playbooks. In cases where a playbook may exist, it is often incomplete, untested, and not fit for purpose. According to Wang J. (2010) of NASA [4], Agency SOCs do not have "accurate incident and threat status from discovery to resolution" or a set of incident response processes; in fact, there is lack of a coordinated operational technical framework to prevention, detection, response and recovery, and this applies to most organisations [6].

Often, *incident management playbooks* are non-existent, inadequate and defective, in some cases, a playbook may have records of individuals who have left the organisation, or who have changed roles and therefore no longer contactable. Imagine an incident occurring 1 o'clock on a Sunday morning and the SOC waking the wrong person up because the playbook entry is not up to date, and worse so, if a *playbook* does not even exist. This means the incident is likely to go on for a prolonged period leading to substantive damages to the organisation. This is terrifying since cyber incidents are unavoidable [5, 6, 7] due to frequent and sophisticated attacks [8] and increasingly common and continuously discovered vulnerabilities in systems, protocols, subsystems and infrastructures [5], causing far more damages and disruptions than ever [8, 9]. It is therefore imperative that standardised *playbooks* of how to appropriately coordinate and manage cyber security incidents exist.

In this paper, we propose ***Soter*** *– a playbook for managing cyber security incidents, especially cyber security operations centre cyber incidents.*

The main contributions of this paper are as follows:

a) Cyber security incident management lexicon based on equivalence mapping is created and discussed.
b) Cyber security incident classification and prioritisation scheme is proposed and discussed.
c) Cyber security incident management playbook is developed and described.
d) Adaptive cyber incident operative playbook and template for managing incident across multiple stakeholders are outlined and explained.

The remainder of the paper is organised as follows: Section II discusses related work, providing definitions to terminologies used in the paper. Section III describes ***Soter*** - our proposed cyber security incident management playbook. Section IV – explains cyber security incident management, including cyber security incident classification, taxonomy and lexicon, and metrics and measurements, while Section V outlines and provides sample playbooks and templates. The paper provides conclusions and future work in Section VI.

I. Related Work

A: Definitions

In [6], we define *playbook* as a "*set of predefined and agreed actions, steps* and *responses* to be carried out by identified stakeholders in a timely manner to successfully manage, contain, counter and recover from an incident the moment it is detected through to resolution and recovery". While in [5], it is defined as an action plan of actionable steps to successfully recover from a cyber incident.

In [10, 6], we define *security operations centre* (SOC) as a capability that comprises **People, Process and Technology.** People monitor business systems, applications and services for intrusions, policy violations and data breaches, and are guided by policies and procedures, while leveraging technology to advance the cause.

According to the UK National Cyber Security Centre (NCSC) [11], a *cyber incident* is defined as "*breach of a system's security policy to affect its integrity or availability, and the unauthorised access or attempted access to a system*"; while in [5], *cyber incident* is defined as a set of related cyber events that lead to successful compromise of one or more systems. We make a distinction between *cyber event* and *cyber incident*.

Cyber events are generated or produced by information systems which may not necessarily result to an incident; events that match certain pre-defined or anomaly-based symptomatic profile will trigger an alert, and one or more alerts may lead to an incident. The recently formed European NIS Directive defines incident in relation to network information systems as "*any event affecting the availability, integrity or confidentiality of networks and information systems (used in the provision of the essential service), that has a significant impact on the continuity of the essential service itself* [12]".

B: Assessment of Related Work

The recently updated NIST Cybersecurity Framework (NIST CSF, 2018) [19] offers a quantitative and measurable risk reduction guide on how organisations can incorporate cybersecurity activities as part of their risk management process. The framework provides guidance that are useful and applicable to any organisation, therefore offers a common, consistent and comparable set of guidelines and practices. While the CSF is a useful guide for setting up and measuring organisation cyber security capability progress and health hygiene, it is not a specific purpose contribution for cyber security incident playbook.

In 2016, the US Homeland Security (US CERT, 2016) [7], directed by the Presidential Policy Directive 41 (PPD-41) [13], developed the United States Cyber Incident Coordination, which stipulates principles guiding the Federal Government's response to any cyber incident pertaining to government, agency and private sectors. The overarching goal of the cyber incident coordination is to form the "national cyber incident response plan (NCIRP) to address cyber security incidents to critical infrastructures and as part of a broader National Preparedness System, establishes the strategic framework and doctrine for a 'whole-of-Nation' approach to addressing, responding to, and recovering from a cyber incident" [7]. The NCIRP is specific to the US, and provides a governance playbook for coordinating national cyber security incidents (pertaining to government, private and citizen) offering guidance, and authority and statutes contacts for each type of cyber incident such as national, provincial, state and private sector communities.

In 2014, MITRE developed a cyber exercise playbook [14]. This playbook is a guide for cyberspace, providing guidance, exercise and Red Team cyber sample event workbook for conducting cyber exercises. Prior, in 2012, they published a cyber defence playbook, focusing on active defence strategies created to leverage the cyber-attack kill chain [15].

A number of other cyber defence playbooks exist, most of which focus on cyber-attack kill chain, adversarial tactics, techniques, and procedures (TTPs), and threat intelligence sharing information methods, such as the MITRE ATT&CK framework [16], a robust framework for assessing control effectiveness for detecting various attacks methods, tactics, techniques and procedures employed by adversarial, and their emerging observable behaviour.

Academic contributions exist, too. Majority of which focus on incident management in natural disasters [2], incident and risk management in SCADA systems [17], human related security incidents [18], and cyber incident response. None of the academic contributions reviewed so far provides a *playbook* for managing cyber incidents, and none provides a *playbook* for managing SOC or strategic cyber incident. To the best knowledge of the authors, our contribution is original and inceptive in this respect.

II. SOTER: Cyber Security Incident Management Playbook

SOTER is our proposed cyber security incident management playbook, a framework that allows SOCs, government departments and private sectors to systematic and consistently manage cyber security incidents, and possibly other types of incidents. The playbook is developed using Business Process Modelling Network (BPMN).

The rationale for BPMN is because, as a process-based modelling tool, it lends itself perfectly well to creating a robust process driven artefact.

The aim of a playbook is to embed standardised repeatable processes and procedures and to provide a comprehensive set of actionable collaterals for SOCs, government departments, and private sector incident responders and managers to follow when an incident is detected.

SOTER (see Figure 3) is composed of three key aspects, namely:

- Cyber Security Incident Governance Command,
- Cyber Security Incident Sharing, Escalations and Reporting, and finally,
- Cyber Security Incident Management.

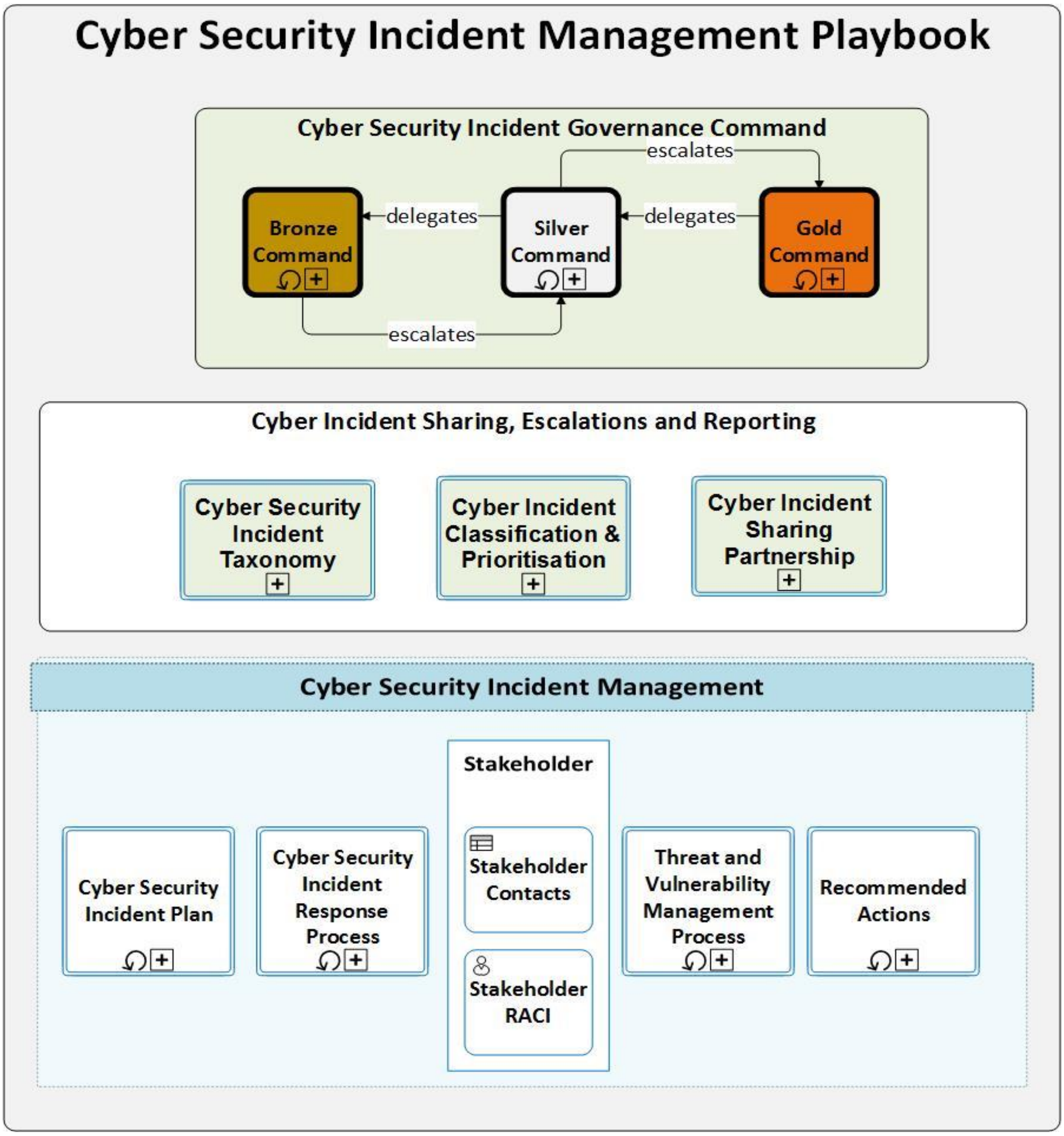

Cyber Security Incident Management Playbook
Cyber Security Incident Governance Command
escalates
Bronze Command
delegates
Silver Command
delegates
Gold Command
escalates
Cyber Incident Sharing, Escalations and Reporting
Cyber Security Incident Taxonomy
Cyber Incident Classification & Prioritisation
Cyber Incident Sharing Partnership
Cyber Security Incident Management
Stakeholder
Cyber Security Incident Plan
Cyber Security Incident Response Process
Stakeholder Contacts
Stakeholder RACI
Threat and Vulnerability Management Process
Recommended Actions

Figure 1: SOTER – A Playbook for Managing Cyber Incidents

A: Cyber Security Incident Governance Command

A robust cyber security incident governance command must be established to manage cyber incident escalations, reporting and authorisation. The governance command must have executive powers in their organisations, agency or government departments to make decision with respect to the approach to cyber incident response, containment and management.

Three hierarchical command structures have been proposed: BRONZE, SILVER and GOLD.

A1: BRONZE Command – is a Board accountable for 'Operational' cyber incident management. We classify 'operational' cyber incident incidents with respect to *priority* or/and *severity*. 'Operational level cyber incidents are usually classified as ***Priority 2*** and/or **Severity 2** Cyber Incidents (see Section 0-B). These are cyber incidents affecting a Service or multiple Services of a singular Business Area, or multiple Business Areas of a particular Service. The membership to this Board should be Heads and Leads of Service Areas, Third-Party Suppliers, the SOC Manager/Head and their Cyber Incident Responder (CIR) Provider.

A2: SILVER Command – is a Board accountable for 'Tactical' ***Priority 1*** and/or **Severity 1** Cyber Incidents (see Section III-B). These are cyber incidents affecting the Entire Organisation, Department, or majority of the organisation, and a number of critical services. Membership to this Board are Business Senior Responsible Owners (SROs), or Service SROs, SOC Capability Director.

A3: GOLD Command – is a Board accountable for 'Strategy', that is, Nation-wide ***Priority 1*** and/or **Severity 1** Cyber Incidents or *Significant Cyber Incidents* (as defined in Table 1), which may include Critical National Infrastructure (CNI) services. Membership to this Board are Chief Technology Officer (CTO), SRO, Director and Director Generals of the Organisation or Government Department.

Note: As shown in Figure 1, a cyber incident could easily be escalated or downgraded from one Command level to the other, as more information become available and as the categorisation, priority and severity ratings change.

B: Cyber Security Incident Sharing, Escalations and Reporting

The second key component of SOTER is the Cyber Security Incident Sharing, Escalations and Reporting layer. It comprises:

- Cyber security incident taxonomy,
- Cyber security incident classification and prioritisation, and
- Cyber incident sharing partnership.

Cyber security incident taxonomy is discussed in detail in Section 0-A, while Cyber security incident classification and prioritization is described in Section 0-B.

B1: Cyber Security Incident Sharing Partnership

The purpose of the *cyber security incident sharing partnership* is to establish specific cyber incident sharing framework that allows for consistency in sharing cyber security incident among appropriate cyber incident management stakeholders to enable incident response and management swiftly. In this paper, we emphasise the importance of cross-government (X-Govt), cross-sector and cross-vertical incident sharing partnerships that allow nation-wide, sector-wide and across-vertical cyber incidents, especially *significant cyber incident* to be shared so that cyber incidents can be mitigated, and services restored as quickly as possible.

One of the mandates for the incident sharing partnership is the adoption and use of a common and consistent cyber security incident lexicon (as defined in Section 0-B), this allows for common understanding among stakeholders when dealing with cyber incident so that appropriate cyber incident responses and containment measures are applied. We strongly recommend this partnership to include all sectors, such as finance and insurance, telecommunications, health, utilities, government, academia etc. This is particularly essential, especially when dealing with significant cyber incidents affecting CNI and public services.

It is pertinent to note that our proposed cyber incident sharing partnership is different to the existing threat intelligence sharing frameworks, such as the Cyber Security Information Sharing Partnership (CiSP[3]), whose mission is to exchange threat intelligence and information. The difference is that our proposed *cyber security incident sharing partnership* is a coordination centre for ensuring that all sectors impacted or 'would be impacted' in the event of *significant cyber incidents* are swiftly notified, to the appropriate contacts of the different sectors, and following prior agreed common and consistent notification framework. We are not also precluding that the existing CiSP cannot be used for such purposes, but it would mean the mission/purpose of the existing sharing partnership will need to be expanded to include this goal.

Another important function of the incident sharing partnership is the role of an *escalation and reporting* centre, accountable for ensuring significant cyber incidents are escalated and reported upstream to the relevant sectors and respective commands.

[3] CiSP – UK Cyber Security Information Sharing Partnership for the purposes of exchanging threat intelligence and information to aid situational awareness – https://www.ncsc.gov.uk/cisp

III. Cyber Security Incident Management

SOC remains an essential part of any robust cyber programme [6], focusing on monitoring, detecting and responding to cyber incidents [19, 10, 20].

Cyber incident management is a complex and wide-reaching task requiring cooperation and collaboration of many stakeholders regardless whether the incident management is for a nation, mission or industry. To successfully manage a cyber incident, one must seek the support and cooperation of multiple teams, such as the infrastructure and networking teams, systems administration and management teams, business continuity and disaster recovery teams, communications and press office, and designated senior management teams etc. Therefore, for cyber incident management to be successful it must seek and gain the support of appropriate and delegated stakeholders. At a national level, for example, the NCIRP [7] or NCSC [11], offers a platform for collective effort from multiple government bodies, private sector and international partners to cooperate and collaborate in managing significant cyber incidents. At organisation levels, organisations need to form their own cyber incident management forums or boards, and a starting point could be to adopt our proposed framework as baseline to guiding them to both the composition of the memberships and also the structure (see Figure 1).

The success of any cyber incident management effort is built upon the planning, preparedness and readiness predicated on a framework on which to collaborate, share and communicate cyber incidents. This audacious task becomes even harder if the lexicon for sharing and coordinating cyber incident mitigation and management activities is ambiguous. Therefore, a common and consistent taxonomy and vocabulary is required for cyber security incident management.

A: Cyber Security Incident Taxonomy

The importance of a common and consistent taxonomy to share, communicate, escalate, report and disseminate cyber incidents cannot be over emphasised. Cyber incident information must be clear and unambiguous. This can only be achieved by agreeing and using a common and consistent body of knowledge.

The problem is that a review of the many authoritative manuals for cyber incident management and government directives on handling cyber incidents e.g. [1, 7-8, 11, 13, 15, 19, 21, 23-25] shows that many vocabularies and terminologies are used for the same thing. This is a cause for confusion, and no wonder why many cyber security subject matter experts argue among themselves expressing the same things.

To address this problem, the terminologies and vocabularies used in describing cyber incidents and cyber incident management need to be grouped into a common and consistent body of knowledge.

One of the contributions of this paper is to map and rationalise known cyber incident vocabulary into a common and consistent taxonomy (see Table 1 and Figure 2); and we have accomplished this using equivalence mapping. *Equivalence mapping* is a relationship that shows the interchangeability and similarity of the cyber security incident vocabulary. It allows us to map (a.k.a. group) the various terminologies that have been used in the literature and notable national CERTs and Standards Organisations (e.g. ISO/IEC) guidance and standards to their equivalencies in order to express cyber security incidents concisely using a common vocabulary.

The *equivalence mapping* as a tool can be used to convert, map or group data from one lexicon to another, and hence provide the commonality and consistency needed for sharing and managing cyber security incidents. As often, the confusion in the use of terminology may mean that cyber incidents are incorrectly prioritised or classified, which could lead to varying degree of consequences.

The rationale for the equivalence mapping is to provide a bridge to existing cyber security incident vocabulary and taxonomy. We believe the lexicon is a significant tool in creating a holistic body of knowledge across all cyber security incident management stakeholder communities including nation, agency, public and private sectors.

To the best of our knowledge, it is the first time such a taxonomy based on *equivalence mapping* has been used to demonstration the relationship among cyber security incident vocabularies.

A mapping of cyber security incident vocabularies to their ‘equivalence’ is presented in Table 1-16. Each Table maps existing cyber incident vocabularies into a lexicon that offers consistent and common understanding among stakeholders involved in cyber incident response and management; for example, cyber incident responders, government agencies responsible for supporting or coordinating national cyber incidents such as the NCSC, US-CERT and NCIRP.

Our contribution in this paper, in our opinion is the beginning of an area of research that requires deeper investigation to produce an authoritative comprehensive lexicon for national and multilateral usage.

Table 1**: Defining equivalences for cyber security incident taxonomy**

Description	Cyber incident is described as "an event occurring on or conducted via a computer network that actually or imminently impacts the integrity, confidential or availability of computers, information or communications systems or network, physical or virtual infrastructure controlled by computers or information systems, or information resident thereon." The PPD-41 includes "vulnerability in an information system, system security procedures, internal controls, or implementation that could be exploited by a threat source. [13]"
Taxonomy	**Equivalences**
Cyber Incident [7, 13, 11]	Information Security Incident [21, 22] Cyber Event [5] Security Incident [12] NISD Incident [12] CSIRT Incident [23] Computer Security Incident [23] Crypto Incident []

Table 2**: Defining equivalences for significant cyber incident taxonomy**

Description	This relates to "Cyber incident that is likely to result in demonstrable harm to the national security interests, foreign relations, or economy of the Nation or to the public confidence, civil liberties, or public health and safety of the citizens. [13]"
Taxonomy	**Equivalences**
Significant Cyber Incident [7, 13]	Major Incident [5] Major Cyber Incident [24] Significant Incident [12] Critical Incident [21] Demonstrable Harm [13] Significant Cyber-harm [25]

Table 3**: Defining equivalences for severity of cyber security incident taxonomy**

Description	Severity and priority are used synonymously e.g. [8], with the connotation that 'very severe' incidents are 'prioritised'. We see this with the interchangeable use of phrases such as *Severity 1* to mean *Priority 1* incident.
Taxonomy	**Equivalences**
Severity [7]	Priority [8]

Table 4**: Defining equivalences for priority of cyber security incident taxonomy**

Description	Incidents are prioritised based on three factors – *functional impact* (now or happening in the future), *informational impact* (e.g. effect on C, I & A), and *recoverability* from the incident (e.g. time and resource required). Note: priority may be related to three impact factors, but 'Impact' is computed using four impact variables (See Impact) below.
Taxonomy	**Equivalences**

Priority [7]	Severity [21]

Table 5**: Defining equivalences for urgency of cyber security incident**

Description	The immediacy of the incident. Urgency may be a direct relation with functional impact.
Taxonomy	**Equivalences**
Urgency [7]	Functional Impact [8]

Table 6**: Defining equivalences for seniority level in relation to managing cyber security incident**

Description	This relates to the hierarchy of the stakeholders coordinating the incident response effort. E.g., incident management governance command – Bronze, Silver and Gold commands (see Section II - SOTER).
Taxonomy	**Equivalences**
Seniority Level [7]	Incident Governance Command

Table 7**: Defining equivalences for impact in relation to managing cyber security incident**

Description	This describes the level of associated impact resulting from an incident. It's a.k.a. business impact level (BIL), a computation of functional impact, informational impact, socio-economic impact and recoverability impact.
Taxonomy	**Equivalences**
Impact [7]	Business Impact [21] Functional Impact [8] Informational Impact [8] Recoverability [8]

Table 8**: Defining equivalences for impact in relation to managing cyber security incident**

Description	*functional impact* is related to what 'impact' the incident is having 'now' or it may have in the 'future', measured as 'None', 'Low', Medium' or 'High'. None, means no impact to the organisation's ability to provide all services [8].
Taxonomy	**Equivalences**
Functional Impact [8]	Functional Impact

Table 9**: Defining equivalences for informational impact in relation to managing cyber security incident**

Description	*informational impact* (e.g. effect on C, I & A), measured as 'None', 'Privacy breach', 'Proprietary breach, and 'Integrity loss' [8].
Taxonomy	**Equivalences**
Informational Impact [8]	Informational Impact

Table 10**: Defining equivalences for informational impact in relation to managing cyber security incident**

Description	This relates to *recoverability* from an incident (e.g. time and resource required) to successfully mitigate the incident, measured as 'Regular', 'Supplemented', 'Extended' and 'Not Recoverable'. E.g. 'Extended' means that time to recover from the incident is unpredictable; additional resources and outside help are required [8].
Taxonomy	**Equivalences**
Recoverability Impact [8]	Recoverability Impact

Table 11**: Defining equivalences for informational impact in relation to managing cyber security incident**

Description	This relates to the detrimental impact of the incident on activities of users, which generate either economic or social damages. This seems to be one part of the 'Impact' in general, therefore, may be regarded as a subset of Business Impact.
Taxonomy	**Equivalences**
Economic Impact [12]	Economic Impact

Table 12**: Defining equivalences for level of investments required in relation to managing cyber security incident**

Description	This relates to the commitment required to respond and successfully mitigate the incident, which is often associated to time and resource. Resource encompassing people, process and financial resources.
Taxonomy	**Equivalences**
Level of Investment Required [7]	Level of Investment Required

Table 13**: Defining equivalences for observed actions in relation to managing cyber security incident**

Description	This relates to the perceived state of the incident, such as 'preparation', 'engagement', 'presence', and 'effect' [8]. Observed action is proportionate to 'intended consequences'
Taxonomy	**Equivalences**
Observed Actions [7]	Effects [8] Intended Consequences [8]

Table 14**: Defining equivalences for intended consequence in relation to managing cyber security incident**

Description	These are the effects or outcomes of the incident, such as *functional*, *informational* and *socio-economic* impacts.
Taxonomy	**Equivalences**
Intended Consequence [7]	Potential Impact [7] Functional Impact [8] Consequential Impact [6] Cyber-harm [25, 26]

Table 15**: Defining equivalences for demanded immediate action in relation to managing cyber security incident**

Description	This relates to the *time and resources* required to successfully recover from the incident.
Taxonomy	**Equivalences**
Demanded Immediate Action [8]	Potential Impact [7] Functional Impact [8] Consequential Impact [6]

Table 16**: Defining equivalences for threat level in relation to managing cyber security incident**

Description	A coarse indication of the likelihood of a terrorist attack. This indication is drawn from a counter-terrorist perspective. The UK national levels are Low, Moderate, Substantial, Severe and Critical [21].
Taxonomy	**Equivalences**
Threat Level [7]	Threat Level

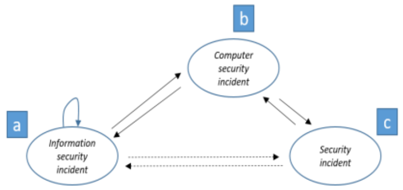
Table 17**: Defining equivalences for threat level in relation to managing cyber security incident**

Description	This relates to severity levels associated to a disaster, usually based on many factors, such as severity, size, impact on life or public health and urgency. It's rated as Level 1, 2, 3 & 4. Disaster levels are inversely proportional to cyber security incident levels. For example, the highest disaster level (Emergency = Level 1), while the lowest = level 4). The highest cyber incident severity level 'Critical' equals disaster level 1 (a.k.a. 'Emergency').
Taxonomy	**Equivalences**
Disaster Level [7]	Cyber Security Incident Severity Level [7]

A1: How to interpret Table 1:

An equivalence relation (denoted by "~") is a relationship on a set that is reflexive, symmetric, and transitive for everything in the set [27]. This means, for all the terminologies that have been mapped to a lexicon, we can show that the equivalence properties preserve. Equivalence properties are reflexive, symmetry and transitivity. For example, we consider the terms grouped together per row as the objects, and if these terms are denoted as objects a, b and c, then they can be mapped to a common lexicon if we can show that for each lexicon (per row in Table 1) that:

1. $a = a$ (reflexive property)
2. If $a = b$ then $b = a$ (symmetric property), and
3. If $a = b$ and $b = c$, then $a = c$ (transitive property.



The following terms have been used in various literatures to describe a cyber incident (see, Table 1):

- Information Security Incident [28, 29]
- Cyber Event [5]
- Security Incident [12]
- NISD Incident [12]
- CSIRT Incident [30]
- Computer Security Incident [23]

Therefore, we show that:

1. If an *Information security incident* ~ *Computer security incident*, and
2. If a *Computer security incident* ~ *Security incident*, then it means we can establish that:
   a) An *information security incident* is an *incident* (reflexive). This is true since an information security incident is indeed an information security incident, and therefore an incident.
   b) Secondly, since an *Information security incident* ~ *Computer security incident*, then it is also true that an *Information security incident* is a type of *incident*, and so is a *Computer security incident*, therefore, a *Computer security incident* ~ an *Information security incident* (symmetric).

c) Finally, since an *Information security incident* ~ *Computer security incident*, and a *Computer security incident* ~ *Security incident*, and having shown that a *Computer security incident* is equally ~ an *Information security incident*, it is therefore true that an *Information security incident* ~ *Security incident* (transitive).

d) Hence, information security incident, cyber event, security incident, NISD incident, CSIRT incident and computer security incident are all equivalent and hence mapped to cyber security incident taxonomy (see Figure 2).

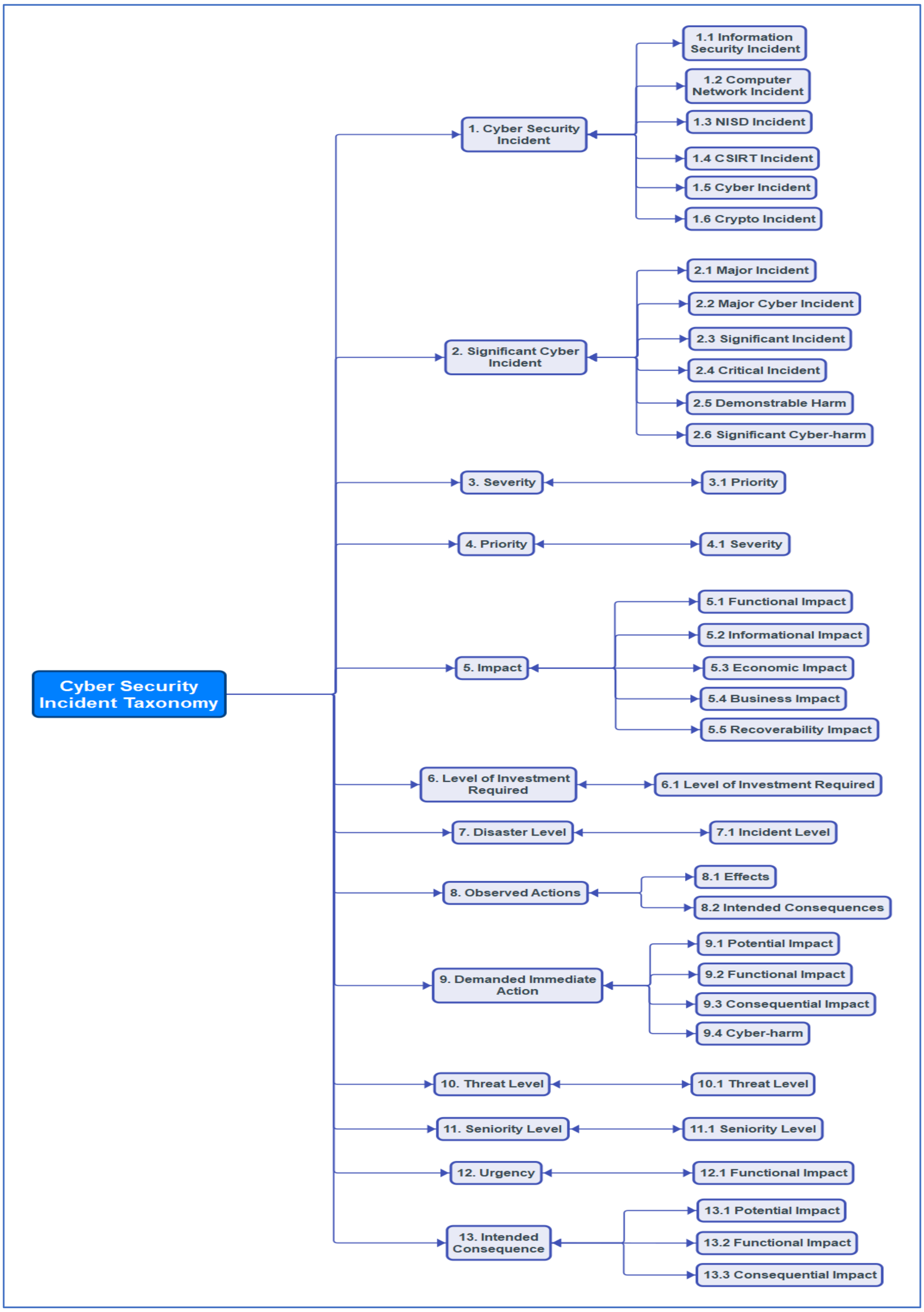


Figure 2: Equivalence Mapping of Cyber Security Incident Vocabulary

A.2 How to Use the Lexicon

As shown in Figure 2:

- **Cyber Security Incident (1.)** is equivalent to:
    - *Information Security Incident* (1.1), *Computer Network Incident* (1.2), *NISD Incident* (1.3), *CSIRT Incident* (1.4), *Cyber Incident* (1.5) and *Crypto Incident* (1.6), (also, see Table 1.0).

- **Significant Cyber Incident (2.)** is equivalent to:
    - *Major Incident* (2.1), and Major *Cyber Incident* (2.2), Significant Incident (2.3) and Critical Incident (2.4)

- **Impact (5.)** is equivalent to:
    - *Functional Impact* (5.1), *Informational Impact* (5.2), *Economic Impact* (5.3), *Business Impact* (5.4) and *Recoverability Impact* (5.5).

Similarly, we see that **Intended Consequence (13.)** is equivalent to *Potential Impact* (13.1), *Functional Impact* (13.2) and *Consequential Impact* (13.3).

B: Cyber Security Incident Classification and Prioritisation

Cyber security incident classification and prioritisation is a schema to classify and prioritise cyber incidents based on a common lexicon discussed in Section 0-A (See Table 18).

In this paper we examine two notable classification schemes namely, the US National Response Coordination Centre [7] and the GovcertUK (now part of the NCSC) incident response classification [31] in conjunction with UK Her Majesty's Government (HMG) Business Impact Assessment (BIA) Classification Standard [21, 28 33]. Cyber security incidents are classified in terms of *priority* or *severity*, driven by a number of factors such as the impact on critical and/or public services, urgency, scale etc. According to the US Federal Incident Notification Guidelines [24], impact and severity assessment of cyber incidents, regardless of those it is affecting, e.g., national-level, government and private sectors, need to be assessed based on a number of factors such as information impact, recoverability, information impact, etc.

One important contribution of our incident classification and prioritisation is the concept of the '**Target Detection Time**' (TDT).

We describe the TDT as the mean time it takes the SOC, or Security Monitoring Supplier (or their analysts) to initially identify or detect an incident. In other words, it is the time it takes the SOC to detect or spot an alert. It may be a single alert or correlated alerts (displayed on their monitoring dashboard). It should include the time it takes for them to raise a ticket for the incident (in their ticketing systems) and ensure that incident triage of the alert or event is started. **Note**. The TDT does not include the *triage time*, neither does not it include the *MTTF*, as shown in Figure 3.

While our measurements of TDT (in Table 18) is not scientific, however, we believe, based on experience that a 'mature and well-resourced SOC' should be able to meet these targets. On the contrary, if a SOC is unable to detect a cyber-attack or incident within the set targets, then it is arguable to assess the maturity model of that SOC.

Table 18: Cyber Security Incident Prioritisation

Priority Level	Severity Level	Description	Target Detection Time
Priority 1	**Critical**	*Significant cyber incidents* which may impact CNI services, or critical services for a large number of users, or serious security breach affecting a mission, or nation critical services or damage public confidence in the Government.	≤ 30Mins

Priority 2	**Major**	*Major incidents* which may impact an organisation users, or disrupt essential business services, or breach network security policy or affect the reputation of Government Departments and key Government services.	≤ 60Mins
Priority 3	**Minor**	Incidents which are neither Critical nor Major and which can be handled by the organisation's SOC or Infrastructure teams. These incidents typically have minimal impact on IT or business services. For example, unsuccessful denial-of service attacks or Phishing campaign, network monitoring alerts.	≤ 120Mins
Priority 4	**Negligible**	Incidents, which are neither Critical, Major nor Minor and are in general considered to be part of normal IT support operations. These include an isolated case of SPAM email or failure of a single endpoint or use device, loss of network connectivity to a peripheral device or loss of access to an external, non-essential service.	≤ 48 hours
Priority 5	**Advisory**	These are Threat Advisories (TA), Vulnerability Announcements, or CERT Notifications, which are not manifested on the organisation but that needs to be tracked, assessed, investigated and actioned.	≤ 72 hours

C: Metrics and Measurements

C1: Mean Time To Detect (MTTD)

The *mean time to detect* a cyber incident is the average time it takes a monitoring system or its subsystems to detect an incident. The incident could manifest in a number of forms, such as an alert, intrusion, attack or a trigger to an event or message which is flagged onto the monitoring dashboard.

Note: An alert may or may not be triggered for a cyber incident to be realised. This is because some systems may not be capable of triggering an alert, instead they only generate logs, events or messages, which are rather sent to the systems buffer or short-term subsystem storage facility. There are systems that are capable of triggering alerts and these may be reported straight as an incident to the monitoring system. Further, other systems may produce a sequence of other notifications, such as alerts, alarms, and events.

MTTD, a.k.a. *mean time to identify* (MTTI), can be affected by a number of factors such as, monitoring systems configuration, e.g. if the monitoring systems is configured to receive events or messages in realtime (as opposed to receiving in batch, which is non-realtime), the 'sensitivity' or tuning of the monitoring systems, processing power of both the sensors and their underlying computers or servers, if the events are correlated or not, if the underlying network infrastructure has delays or quality of services enabled, and the location and distance between the monitored infrastructures and the monitoring systems (WAN coverage, and Round Trip Times) etc.

We calculate the MTTD as follows:

$$MTTD = \frac{1}{n}\sum_{t=1}^{n} DE_t \qquad\qquad Equ.\ (C1)$$

Where, DE_t is detection time, *t* is time, and *n* is a finite number of times it takes the monitoring system to detect an incident (see Figure 3).

For SOC monitoring systems, we expect the MTTD to be in seconds, and would strongly recommend that the monitoring system and its subsystems are configured to process events in realtime.

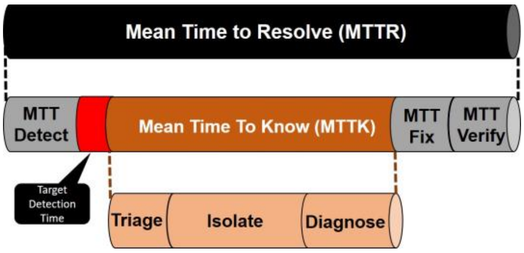


Figure 3: Incident and Fault Measurement Metrics [32]

C2: Mean Time To Know (MTTK)

The MTTK comprises *triage*, *isolation* and *diagnosis* (see Figure 3). *Triage* is the initial check/assessment conducted to determine whether the alert is a false positive or true negative, the perceived coverage and potential severity of the incident. *Isolation* refers the correct identification of the teams that have ownership of the source of the problem, incident or attack, that is, from where the incident originates. This is important because correct identification of the owner eliminates substantial delays due to redundant investigations [32]. **Note**: Isolation in this case, is different from taking systems off the network or quarantine of infected systems in a sandbox as a means of isolating the systems, and therefore reducing the spread of the incident, for instance, in the case of a network worm, or virus, in order to minimise the incident spreading or affecting other systems and networks.

Diagnosis follows isolation, it means once ownership of the fault or attack is identified, then a task is assigned to the rightful team or group to conduct further analysis to determine the root cause and recommend appropriate fixes/remedies.

We define MTTK as average time required to triage, isolate and diagnose the incident, as follows:

$$MTTK = \frac{1}{n}\sum_{t=1}^{n}(T_t) + \frac{1}{n}\sum_{t=1}^{n}(I_t) + \frac{1}{n}\sum_{t=1}^{n}(D_t) \qquad Equ.C2$$

Where *Tt* is triage time, *It* is isolation time, and *Dt* is diagnosis time. *t* is time, and *n* is the finite number of times it takes for each process to be successfully completed.

Since MTTK encompasses three specific activities, we believe that MTTK can take several **minutes to hours** to be determined, and in some circumstances, could take days to be determined. That said, it is important that with cyber incident that the MTTK is kept to minutes or hours rather than days, and where this is untenable, then, we strongly recommend that the incident is contained during the isolation phase in order that the business can still operate while the incident is being investigated to resolution.

C3: Target Detection Time (TDT)

TDT asks the question – "how long would it take a SOC human operator (SOC Analyst) to spot an incident on their monitoring dashboard? It is about the responsiveness and reactiveness of the SOC analysts that are being adjudged here. How quickly can the SOC spot or detect an inflight or potential incident. If they are monitoring the service, and are dedicated, and that the monitoring dashboard is reporting incidents and events in realtime, then you would expect the SOC to identify an incident as quickly as possible.

We define the TDT as the responsiveness of the SOC human operators (e.g. SOC Analysts, Administrators, Incident Responders, Threat Hunters etc.). It is the difference between MTTK and MTTD.

We calculate the TDT as follows:

$$TDT = MTTK - MTTD \qquad Equ.(C3)$$

We expect the TDT to be in **seconds**, especially if the SOC has dedicated analysts monitoring the service, and within their operational hours.

C4: Mean Time To Fix (MTTF)

MTTF (a.k.a. *mean time to remedy - MTTRem*), is the average time it requires to apply the fix to remedy an incident, a fault or an issue. It is the average time required to apply the right fixes once the 'corrective actions' is known. We expect the MTTF to be in **seconds to minutes**, this is because, once the fix is known, applying it to remedy the incident is a matter of minutes. It is believed that some fixes are tested, say in a test environment before being applied in a production environment. As shown in Figure 3, the MTTF does not include the MTTK, therefore, once the fix is known, its application to remedy the incident should be significantly shorter than the MTTK.

We calculate the MTTF as follows:

$$MTTF = \frac{1}{n}\sum_{t=1}^{n}F_t \qquad Equ.(C4)$$

Where F_t is the time required to fix or remedy an incident, and *t* is time, and *n* is a finite number of time trials.

C5: Mean Time To Verify (MTTV)

MTTV is the average time it takes to check, verify and validate that the countermeasure or remedy applied to the incident has caused it to stop or successfully mitigated the incident.

We expect the MTTV to be in **seconds**, this is because, the verification should be instantaneous, and if it works, then the incident should stop or immediately reduce. As shown in Figure 3, the MTTV does not include post incident reporting, lessons learned and documentation of post incident reports, therefore, once the fix is known, and applied, the verify time should be in seconds, and in most cases, is included within the MTTF. This is because, when the fix is applied, it is believed to be tested and verified, otherwise a backout procedure or roll-back may be required. While the two may be separate in this paper, it may be the case that both MTTF and MTTV are combined in practice.

We calculate the MTTV as follows:

$$MTTV = \frac{1}{n}\sum_{t=1}^{n} V_t \qquad\qquad Equ.(C5)$$

Where V_t is the time required to verify that the applied patch has remedied the incident, *t* is time, and *n* is a finite number of verifications.

C6: Mean Time To Resolve (MTTR)

MTTR is the average time it takes from detection to root cause analysis (RCA) through to resolution (see Figure 3). MTTR does not include the post incident report, this is because including the post incident report will skew the MTTR since post incident reports are not often prioritised and in actual fact may take longer to complete.

We calculate the MTTR as follows:

$$MTTR = \frac{1}{n}\sum_{t=1}^{n}(DE_t) + TDT + \frac{1}{n}\sum_{t=1}^{n}(T_t) + \frac{1}{n}\sum_{t=1}^{n}(I_t) + \frac{1}{n}\sum_{t=1}^{n}(D_t) + \frac{1}{n}\sum_{t=1}^{n}(F_t) + \frac{1}{n}\sum_{t=1}^{n}(V_t)\ (C6)$$

Where DE_t is detection time, *TDT* is target response time, *Tt* is triage time, *It* is isolation time, *Dt* is diagnosis time, *Ft* is fix time and *Vt* is verify time. *t* is time, while *n* is finite number of times required to accomplish each task or exercise.

We believe MTTR should be in **several hours**, and occasionally in days, but for cyber incident, it is best to ensure that the MTTR is in hours rather than days. This is because the longer the incident is prolonged the higher the chances that the attacker may destroy any evidential information, such as logs, events, data etc that could be used to attribute the source of the attack, equally, the longer the incident, also the higher the probability that the attacker may plant backdoor and may use those to re-launch an attack at a later time. This is one of the reasons why most companies who have suffered a breach end up suffering subsequent breaches. Further, it is challenging for a company to ensure that their systems have been absolutely cleansed after an attack. This is because, one of the goals of the business is to continue to provide services to their customers, and this means that thorough cleansing, e.g. building the systems from ground-up may not happen, in which case, any of the remnants of the attack may still exist, e.g. in memory, databases, codes or registry. This could therefore provide the attacker a backdoor and a foothold to re-launch an attack.

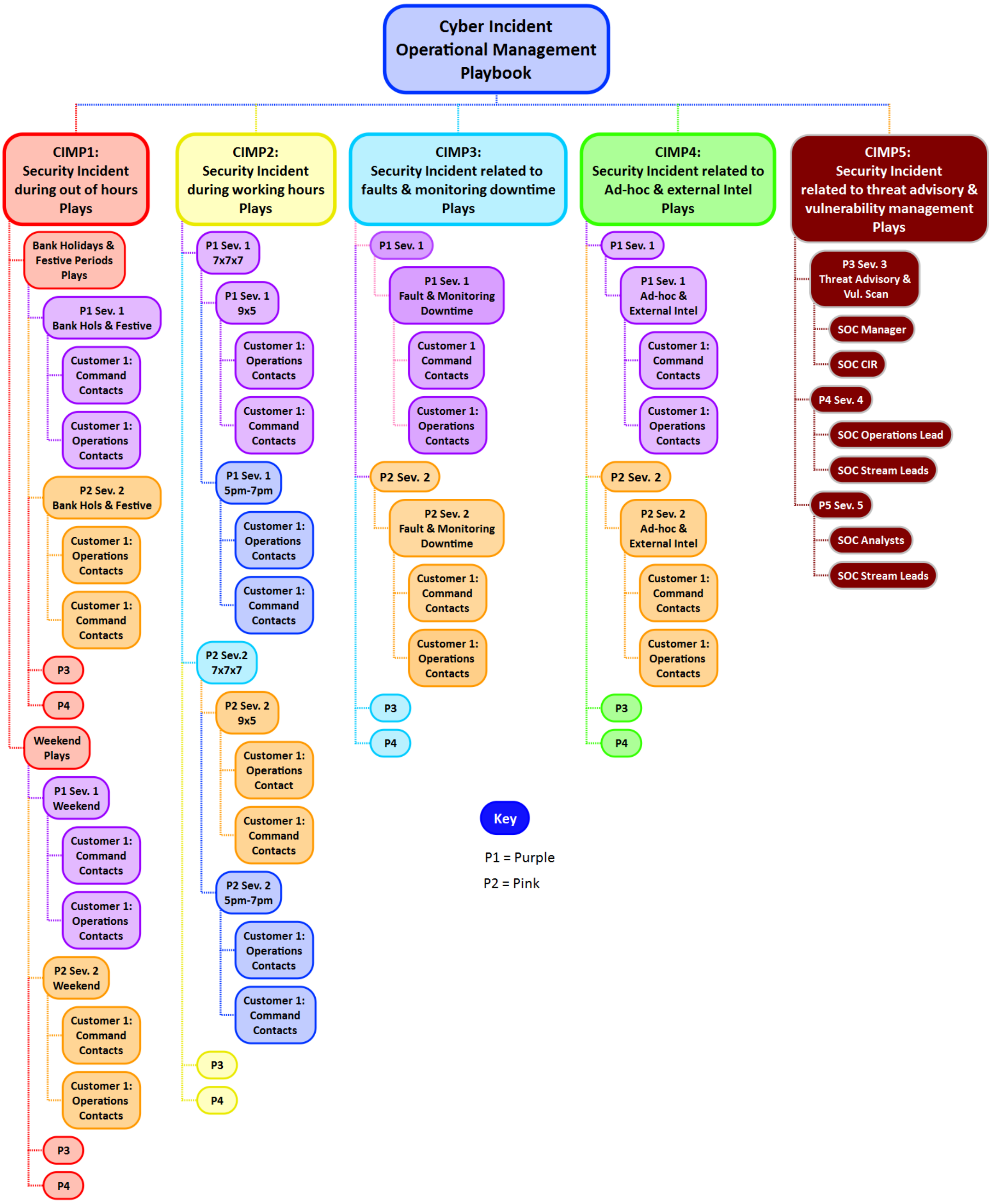
IV. CSOC Cyber Security Management Playbook and Templates

The essence of the playbook is to provide a set of “plays” to guide organisation’s cyber security programmes, especially the SOCs on how cyber incidents should be managed from detection to recovery and through to post incident reporting.

According to the UK HMG Security Policy Framework, the main objective of the SOC is to coordinate stakeholder activity including UK CERTs, NCSC etc. into providing a satisfactory, coherent incident management [33]. Therefore, the principle function of the SOC is hinged on incident management in as much as detection and monitoring are essential.

In this section, we discuss our proposed playbook template (as shown in Figure 4), which shows five cyber incident playbook templates, namely:

- **Play 1**: Cyber Incident Management Playbook (CIMP 1) for handling and managing *cyber incidents that occur during non-operational hours of the SOC*.
- **Play 2**: Cyber Incident Management Playbook (CIMP 2) for handling and managing *cyber incidents that occur during working hours of the SOC*.
- **Play 3**: Cyber Incident Management Playbook (CIMP 3) for handling and managing *cyber incidents relating to faults and monitoring downtime of the SOC*.
- **Play 4**: Cyber Incident Management Playbook (CIMP 4) for handling *cyber incidents that relates to Ad-hoc and external threat intelligence*.
- **Play 5**: Cyber Incident Management Playbook (CIMP 5) for handling and managing *cyber incidents relating to threat advisory and vulnerability management*.


Cyber Incident Operational Management Playbook
CIMP1: Security Incident during out of hours Plays
Bank Holidays & Festive Periods Plays
P1 Sev. 1 Bank Hols & Festive
Customer 1: Command Contacts
Customer 1: Operations Contacts
P2 Sev. 2 Bank Hols & Festive
Customer 1: Operations Contacts
Customer 1: Command Contacts
P3
P4
Weekend Plays
P1 Sev. 1 Weekend
Customer 1: Command Contacts
Customer 1: Operations Contacts
P2 Sev. 2 Weekend
Customer 1: Command Contacts
Customer 1: Operations Contacts
P3
P4
CIMP2: Security Incident during working hours Plays
P1 Sev. 1 7x7x7
P1 Sev. 1 9x5
Customer 1: Operations Contacts
Customer 1: Command Contacts
P1 Sev. 1 5pm-7pm
Customer 1: Operations Contacts
Customer 1: Command Contacts
P2 Sev.2 7x7x7
P2 Sev. 2 9x5
Customer 1: Operations Contact
Customer 1: Command Contacts
P2 Sev. 2 5pm-7pm
Customer 1: Operations Contacts
Customer 1: Command Contacts
P3
P4
CIMP3: Security Incident related to faults & monitoring downtime Plays
P1 Sev. 1
P1 Sev. 1 Fault & Monitoring Downtime
Customer 1 Command Contacts
Customer 1: Operations Contacts
P2 Sev. 2
P2 Sev. 2 Fault & Monitoring Downtime
Customer 1: Command Contacts
Customer 1: Operations Contacts
P3
P4
CIMP4: Security Incident related to Ad-hoc & external Intel Plays
P1 Sev. 1
P1 Sev. 1 Ad-hoc & External Intel
Customer 1: Command Contacts
Customer 1: Operations Contacts
P2 Sev. 2
P2 Sev. 2 Ad-hoc & External Intel
Customer 1: Command Contacts
Customer 1: Operations Contacts
P3
P4
CIMP5: Security Incident related to threat advisory & vulnerability management Plays
P3 Sev. 3 Threat Advisory & Vul. Scan
SOC Manager
SOC CIR
P4 Sev. 4
SOC Operations Lead
SOC Stream Leads
P5 Sev. 5
SOC Analysts
SOC Stream Leads
Key
P1 = Purple
P2 = Pink

- **Figure 4: Cyber Incident Operational Management Playbook**

Each play has a number of sub-plays. Plays can be triggered by the occurrence of a cyber incident, identification of a threat or the discovery of a vulnerability (see Figure 4).

- First, CIMP1 to CIMP4 do not have P5, as discussed previously (see Table 2) P5 are threat advisories, notifications and vulnerability scan information, and these are captured in play CIMP5.
- Secondly, P3 and P4 are not expanded in CIMP1 to CIMP4 plays because they are SOC specific plays which do not require governance command escalations, however, should follow the SOC run book (that is, already existing knowledge articles and operating procedures or local working instructions). It is also the same reason why P3 to P5 for CIMP5 play involve only the SOC, e.g. SOC Manager, SOC CIR, Stream Leads etc.

Note: Cyber incidents are dynamic in nature and as more information pertaining to an incident becomes available, it is possible, too that the severity of the incident may change. So, there will be cases where a P3 incident is escalated to a P2 or even to a P1 as new evidence of the incident are uncovered. Likewise, there will be cases where an incident that started off as a P1 or P2 may be downgraded to a P3 following an initial triage or further investigations.

CIMP1 is a collection of plays for managing cyber incidents occurring during non-operational hours of the SOC. As a template, this play can be adapted by a SOC to fit into their operating hours. In this play, we capture two sub-plays, namely – *festive period plays* and *weekend plays*. Festive period play is the cyber incident playbook that governs the SOC when a cyber incident occurs during festive periods, e.g. Christmas, Easter, and Independence Day, Thanksgiving Day and all majority holidays. The rationale for creating plays for managing cyber incident during festive periods is multiple fold:

a) SOC resource may be scant during festive periods, in which case appropriate handling measure should be in place to counter,
b) SOC may resolve to On-Call procedure to cover shortage in workforce during this period,
c) Attacker may exploit the theme of the festive period to launch crafted attacks, and also,
d) Incident escalation may be challenging as the designated senior authorities may be hard to reach. Therefore, agreeing a set of plays and knowing who to contact during such situations in advance have proved invaluable.

CIMP2 is a collection of plays for managing cyber incidents during the operational working hours of the SOC. It consists of two sub plays, one for a 9x5 SOC service, this is the case where the SOC works 9 hours, five days a week. Most SOCs work 24x7, which means 24 hours, 7 days a week. A SOC that operates 24x7 will have to adapt this play template to fit its working hours. This can be straightforward to do. You will notice also that there is a 7x7x7 play and a 5x7 play for the CIMP2 plays. This is the case where the SOC may have a working pattern of covering extended days and including weekends, that is, the SOC starts at 7am, closes at 7pm and works 7 days a week. The 6pm-7pm is the case where a special arrangement has been provisioned, for example, using on call service to between 6pm to 7pm after the normal 9x5 working hours.

CIMP3 is a collection of plays covering faults that impact the SOC monitoring platform, while CIMP4 is about ad hoc and external threat intelligence, threat advisory and vulnerability notification and announcement. It also covers when a significant cyber incident may have been uncovered by an external agency which are not still in the wild.

CIMP1-4 has two key stakeholder communities across the various plays -these are operations stakeholder contacts and command contacts. The operations stakeholder contacts are the people that the SOC must contact to collaborate with mitigating a cyber incident related to that particular customer, agency or mission, while the command contacts are the governance commands that the SOC must escalate the cyber incident to, such as the GOLD, SILVER and BRONZE commands, as discussed in Section 0.

IV-A: An Example of how our Framework can be used to manage a Significant Cyber Incident

This section presents a scenario that uses the guidelines provided in earlier section of this document to effectively demonstrate the application of the proposed framework to manage a significant cyber incident.

Table 19: Cyber Security Incident Management Playbook - Example

Incident Type, Classification and Prioritisation

Incident Type:	Ransomware
Incident Classification	Major Cyber Incident
Definition	*Major incidents* which may impact an organisation users, or disrupt essential business services, or breach network security policy or affect the reputation of Government Departments and key Government services.
Incident Prioritisation	P2

Cyber Security Incident Governance Command

Cyber Incident Governance Command	The organisation understood the importance of cyber incident preparedness, readiness and management. Hence, they had formed their internal cyber incident governance command. The have Bronze Command, Silver Command and Gold Commands. Members of the various Commands are known within the organisation, so that the appropriate teams know who to contact in the event of cyber incident. Since the current incident is a Significant Cyber Incident of severity P2, then this incident is escalated to the Silver Command of the organisation.
	The Silver Command The Silver Command convenes an urgent Cyber Incident Call using secure phone lines (e.g. Brent) in accordance with guidelines and as stipulated in the Cyber Security Incident Management Protocol. The Silver Command will ensure that details of the cyber incident are only shared with member of the Silver Command. The Silver Command Call is chaired by the designated Senior Responsible Officer (SRO) or the Deputy. The Security Operations Manager is invited to the Silver Command Call to provide low level details of the Cyber Incident, and to answer any questions that the Silver Command may have in respect of the incident as follows: a) When was this incident detected? b) How many services are impacted? c) A list of affected services or lines of business or stakeholders d) What measures are available to contain the incident? e) What measures have been put in place already? f) How quickly can the incident spread? g) Are there recovery processes and plans in place? h) What are the financial impacts (high level at this stage)? i) What are the reputational impacts (high level at this stage)? j) Has this type of incident occurred before (e.g. Ransomware, Hacking, Intrusion, Data Exfiltration etc.)? k) Can the incident be attributed to any parties, (e.g. 3rd parties, supplier community or foreign intelligence services)? l) What authorisations is required from the Silver Command with regards to mitigating the incident? m) Regular briefings must be provided by the Security Operations Manager to the Silver Command Conference Bridge every 10 minutes

	Escalation to Gold Command or Downgrade to Bronze Command Depending the answers to the questions above, the Silver Command Chair may decide to either escalate the incident to the Gold Command or downgrade the incident priority or severity so that it can be dealt by the Bronze Command. Note that each Command has its own Rule Books, which dictates how cyber incidents are managed from start to finish. An important note is that if the incident is escalated to Gold Command, then a CORBA (which is the highest level of emergency security forum) may be convened and external Agencies may be invited, especially if the incident impacts National Security.

Cyber Incident Sharing, Escalations and Reporting

Cyber Security Incident Taxonomy	The organisation has 'Defined Terms' a.k.a. Acronyms which map or uses industry standard taxonomy. As discussed in the paper, since there is yet a standard cyber security incident taxonomy in the extant literature, it is likely that the organisation used incident terminologies that are used frequently in the organisation, which they may have defined prior.
Cyber Incident Classification and Prioritisation	The organisation follows a well-defined cyber incident classification and prioritisation scheme. It is this scheme that has allowed them to determine the severity and priority of the incident. Hence, they have used to identify the incident as a 'Major Cyber Incident' and a priority of P2 was assigned.
Cyber Incident Sharing Partnership	The organisation has a cyber incident sharing partnership memorandum of understanding (MoU) with a National Cyber Incident Coordination Centre, or a 3rd Cyber Incident Responder e.g. FIRST [34] and have access to their incident response information sharing portal. Based on this MoU the organisation is able have a callout with FISRT who provides incident response and security management to them in the event of the ransomware attack. Note: that our discussion in this paper on cyber incident sharing partnership exceeds beyond current incident-to-response capabilities, such offered by forums like FISRT (as discussed in Section II-B) of this paper.

Cyber Security Incident Management

Cyber Security Incident Plan	The organisation understood the importance to be ready and prepared in the event of a ransomware incident. The organisation had conducted planning to operate in a reduced capacity (or diminished level of services). The organisation has conducted prior stakeholder assessment to determine who is response for what, and who to contact in the event of an incident. The organisation has compiled a list of all stakeholders, both internal and external, and including service providers and national cyber incident responders, e.g. NCSC, Department of Homeland Security (DHS) etc. The organisation has a plan of the sequences of how services might be restored if an event happens, knowing that if the sequences are not followed in a particular order, this might cause fatal consequences. For example, if the management LAN (local area network) is not restored first, then administrator may not have access to reach and manage the devices and/or network, and this will mean that they are further faced with a denial of service to its own administrative staff, which then compounds their restoration or service remediation activities. A stakeholder RACI (Response, Accountable, Consulted, and Informed) matrix is kept so that the organisation knows who to contact, inform and take instructions and authority from (see below as these are needed artefacts).
Cyber Security Incident Response Process	The organisation understood the importance to be ready and prepared in the event of a ransomware incident. The organisation had conducted planning to operate in a reduced capacity scale in the event of a significant cyber incident, such as a ransomware. The ransomware playbook includes the following critical elements: • Detailed set of formal recovery processes to use if the organisation experiences a ransomware attack [5].

	• A stakeholder contacts and list of stakeholder RACI, who will be contacted in the event of a Ransomware incident. • A dependency map that explains the order of restoration priority and sequence • Priori metrics that have been documented against all the systems, and this will be used after restoration to compare if the recovered systems are optimal and functioning as they were prior to the incident. • Repository of previous backups, which will then be used to restore service. • A comprehensive recovery communications plan. This plan comprises both internal and external communications contacts. It is pertinent to note that external communications must go via the designated response owners, for example through the Organisation's Press Office or Communications Office as stipulated in the organisation's Cyber Incident Management Protocol or Playbook.
Stakeholder Contacts	The organisation has up-to-date stakeholder contacts database, repository or list, which it uses in the event of a Cyber security incident to expedite its response activities.
Stakeholder RACI	The organisation has well defined the roles and responsibilities of its stakeholder community, whether internal or external stakeholders. This comprises internal stakeholders, external stakeholders including service providers, 3rd party organisations, external agencies, other government departments and national cyber incident responders and incident managers, such as the NCSC, DHS etc.
Threat and Vulnerability Management Process	The organisation has well-defined threat and vulnerability management process, which helps them identify threats and vulnerabilities that may exist within and around their assets. The organisation's threat and vulnerability management process stipulates the process around continuous vulnerability assessment and management. For example, • it states how frequently the organisation's ecosystems are scanned for vulnerability, e.g. daily. • It also stipulates what happens if a critical or major vulnerability is identified in its systems/assets. • It outlines the remedial processes including raising expedite (a.k.a. Emergency change requests) change controls in order to mitigate/address the identified vulnerability. • It describes when an external IT Health Check (ITHC) or Deep Penetration Testing may be conducted, and the conditions in which exploitation may not be required in the ITHC exercise. • It outlines the various vulnerability repositories it will use for vulnerability assessment and discoveries, e.g. National Vulnerability Database (NVD), Common Vulnerability Exploit (CVE), and Vendor vulnerability repositories such as Microsoft, Linux, Cisco etc based on the number of asset types in the estate that are of these types. • It stipulates how threat intelligence sources will be engaged in order to receive threat advisories. • It stipulates how threat intelligence will be ingested into its ecosystems, and outlines if any pre-processing may be required. For example, aggregation of multiple threat intelligence sources, de-duplication, curation, normalisation, and ingestion
Recommended Actions	The organisation has a well-defined recommended actions policy that determines what recommended actions may be required. For example, the policy will define: • when containment is recommended, and the conditions in which these are recommended. • When controls are required to be applied, and the consequential impacts, e.g. active defence controls that could denial service based on perceived impacts of the attack. • When countermeasures are required to be applied. • When legal investigation and prosecution are required and the conditions for which these are requested. • When the incident may be closed as deemed resolved.
Post Incident Report	The organisation has created a template for post incident management report, which must be completed per incident. Finally, a post incident report is completed for the ransomware incident upon resolution.

V. Conclusion

We have provided a comprehensive cyber security incident management playbook and discussed the various components of the playbook, showing how this can be applied to many institutions, such as nation, government department or private sector. We introduced an equivalence mapping and used it to group cyber security incident management vocabulary into a common and consistent lexicon, which we believe is useful for providing a common taxonomy framework among incident responders and incident sharing partnerships.

We introduced cyber security incident response classification, defining the various tiers of the prioritisation and providing a target response time against each. We provided a formalism for each of the parameters of cyber incident stages, namely detection, triage, mitigation, remedy and resolution, showing how the various associated or recommended mean time to detect, know, fix, verify and resolve are deduced.

Finally, we provided a comprehensive cyber incident operational playbook template for SOC and showed how these are applied. As a template, we believe this can be easily adapted to assist national, agency, government and private sector SOCs in successfully managing cyber incident from start to finish.

A: Future work

Our research has uncovered gaps that exist in the cyber security incident management, which need to be pursued as future research either by the authors or other researchers and may form a PhD piece of work in some respects. As follows:

- Our work has shown that the exist cyber incident management vocabulary is neither comprehensive nor consistent, and we argue for a common and consistent lexicon. This piece of work requires deeper investigation beyond what we have provided in this paper. We believe a common body of knowledge should be created, and our work provides both a starting point and a steppingstone.
- The authors also believe that cyber incident metrics and measurements require further investigations, for example, how does one distinguish between MTTD in respect to MTTD of the subsystems, and associated systems in the ecosystem.
- Can standardisation help with determining a consensus around the following: 'cyber incident target response time', 'cyber incident resolution target time' and 'cyber incident RCA' etc.
- Finally, while the proposed SOTER playbook is innovative, specifically for SOC environment, it still needs to be validated, at least in applying it to an organisation in order to measure its effectiveness for coordinating cyber incident response and management. In this respect, it is recommended that future work will focus on the applicability of SOTER to different organisations and across multiple verticals, e.g. Government (e.g. Local Government, Central Government, Agency etc), Industry (Retail, Banking, Finance, Telecommunications, and Health) and Academia (e.g. Universities, Colleges).

References

[1] DHS (2016), "Cyber Incident Reporting: A Unified Message for Reporting to the Federal Government", US Department of Homeland Security, 2016

[2] J. Raikes and G. McBean (2016), "Responsibility and liability in emergency management to natural disaster: A Canadian example", *International Journal of Disaster Risk Reduction*, 16 (2016) 12-18

[3] C. Onwubiko (2016), "Understanding Cyber Situation Awareness. *International Journal on Cyber Situational Awareness*, Vol. 1, No.1, pp11-30.

[4] J. Wang (2010) "Anatomy of a Security Operations Center", GFirst 2010, NASA, [Accessed 31st Jan. 2018] https://ntrs.nasa.gov/archive/nasa/casi.ntrs.nasa.gov/20110011188.pdf

[5] NIST (2016) Special Publication 800-184, "Guide for Cybersecurity Event Recovery", 10.6028/NIST.SP.800-184

[6] C. Onwubiko (2018), "CoCoa: An Ontology for Cybersecurity Operations Centre Analysis Process" published in 2018 International Conference on Cyber Situational Awareness, Data Analytics and Assessment (CyberSA), 10.1109/CyberSA.2018.8551486

[7] US CERT (2016), "National Cyber Incident Response Plan", Homeland Security.

[8] NIST (2012), Special Publication 800-61r2, "Computer Security Incident Handling Guide", 10.6028/NIST.SP.800-61r2

[9] C. D. McDermott, W. Haynes and A. V. Petrovski (2018), "Threat Detection and Analysis in the Internet of Things using Deep Packet Inspection", *International Journal on Cyber Situational Awareness*, Vol. 3, No. 1, pp. 61-83. **10**.22619/IJCSA.2018.100118

[10] C. Onwubiko (2017), "Security Operations Centre: Situation Awareness, Threat Intelligence and Cybercrime" published in 2017 International Conference on Cyber Situational Awareness, Data Analytics and Assessment (CyberSA), 10.1109/CyberSA.2017.8073384

[11] NCSC (2018), "Incident Management", https://www.ncsc.gov.uk/incident-management

[12] EU NIS Directive (2018), "Reference document on Incident Notification for Operators of Essential Services, NIS Cooperation Group, Feb 2018

[13] PPD-41 (2016), “Annex for Presidential Policy Directive – United States Cyber Incident Coordination”, July 26, 2016

[14] J. Kick (2014), “Cyber Exercise Playbook”, MITRE

[15] MITRE (2012), “Threat-Based Defense – A New Cyber Defense Playbook”, MITRE Public Release Case Number 12-2919.

[16] MITRE ATT&CK (2018), “MITRE ATT&CK”, https://attack.mitre.org/

[17] Y. Cherdantseva, P. Burnap, A. Blyth, P. Eden, K. Jones, H. Soulsby and K. Stoddart (2016), “A Review of Cyber Security Risk Assessment Methods for SCADA Systems”, *Computer & Security* 56 (2016) 1-27

[18] M. Evans, Y. He, L. Maglaras and H. Janicke (2019), “HEART-IS: A Novel Technique for Evaluating Human Error-Related Information Security Incidents”, *Computer & Security* 80 (2019) 74-89

[19] NIST (2018), “Framework for Improving Critical Infrastructure Cyber Security”, Version 1.1, April 16, 2018, 10.6028/NIST.CSWP.04162018

[20] C. Onwubiko (2015), “Cyber Security Operations Centre: Security Monitoring for Protecting Business and Supporting Cyber Defense Strategy, published in 2015 International Conference on Cyber Situational Awareness, Data Analytics and Assessment (CyberSA)

[21] UK HMG IA Standard No. 1(2009), “Technical Risk Assessment Part 1: Risk Assessment”, Issue 3.5, October 2009.

[22] ISO/IEC 27035-1:2016 (2016), “Information Technology – Security Techniques – Information security incident management – Part 1: Principles of incident management

[23] US CERT (2017), “US-CERT Incident Reporting System”, us-cert.gov/forms/report

[24] US CERT (2017), “Federal Incident Notification Guidelines”, https://www.us-cert.gov/sites/default/files/publications/Federal_Incident_Notification_Guidelines.pdf

[25] I. Agrafiotis, J. R.C. Nurse, M. Goldsmith, S. Creese and D. Upton(2018), “A taxonomy of cyber-harms: Defining the impacts of cyber-attacks and understanding how they propagate”, Journal of Cybersecurity, 2018, 1-15 doi: 10.1093/cybsec/tyy006, Oxford University Press.

[26] Agrafiotis I., Bada M., Cornish P. et al (2016), “Cyber harm: concepts, taxonomy and measurements”. Said Business School Working Paper 2016, University of Oxford, UK, 23. Doi: http://dx.doi.org/10.2139/ssrn.2828646

[27] Wikipedia (2019), “Equivalence Relation”. Retrieved October 2019. https://en.wikipedia.org/wiki/Equivalence_relation

[28] UK HMG IA Standard No. 1(2009), “Technical Risk Assessment Part 1: Risk Assessment”, Issue 3.5, October 2009.

[29] ISO/IEC 27035-1:2016 (2016), “Information Technology – Security Techniques – Information security incident management – Part 1: Principles of incident management

[30] US CERT (2017), “US-CERT Incident Reporting System”, us-cert.gov/forms/report

[31] NCSC GovCERTUK Incident Response Classification Scheme – https://www.ncsc.gov.uk

[32] C. Priddy (2016), “Time To Know is the Most Critical Factor to Accelerate MTTR”. Accessed 7th Dec. 2018 https://itmonitor.zenoss.com/time-know-critical-factor-accelerate-mttr/

[33] UK HMG SPF (2013), “HMG Security Policy Framework”, Version 10.0, April 2013, pp.6

[34] FIRST (2019), “Forum of Incident Response and Security Teams”. Accessed 4th November 2019. https://www.first.org/