A Case Study for Cyber Incident Report in Industrial Control Systems

By

Kim Whatt Gary Ang

M.Sc Management of Technology
National University of Singapore, 2013

SUBMITTED TO THE SYSTEM DESIGN AND MANAGEMENT PROGRAM IN PARTIAL FULFILLMENT OF THE REQUIREMENTS FOR DEGREE OF

MASTER OF SCIENCE IN ENGINEERING AND MANAGEMENT
AT THE
MASSACHUSETTS INSTITUTE OF TECHNOLOGY

SEMPTEMBER 2022

Signature of Author ____
Department of System Design and Management
August 15, 2022

Certified by ____
Thesis Supervisor, Professor Stuart Madnick
John Norris Maguire Professor of information Technologies, MIT Sloan School of Management
Professor of Engineering Systems, MIT School of Engineering

Accepted by ____
Joan S Rubin
Executive Director, System Design and Management Program, MIT

(This page left intentionally blank)

A Case Study for Cyber Incident Report in Industrial Control Systems

By
Kim Whatt Gary Ang

SUBMITTED TO THE SYSTEM DESIGN AND MANAGEMENT PROGRAM on AUGUST 15 2022
IN PARTIAL FULFILLMENT OF THE REQUIREMENTS FOR DEGREE IN
MASTERS OF SCIENCE IN ENGINEERING AND MANAGEMENT

ABSTRACT

In recent times, Cyber Incidents[1] have increased in frequency and complexity. These incidents have come from a wide range of sources, from lone individuals to complex state-sponsored teams. In particular, these cyber-crime organizations have used a variety of tactics, techniques, and procedures (TTP) from exploiting well-known vulnerabilities to navigating highly sophisticated zero-day pathways in order to attack systems, sabotage critical services, commit financial crimes, and gather sensitive information for political gain.

Industrial Control Systems (ICSs) have been used in critical infrastructure sectors such as nuclear reactors for power generation. These ICSs have evolved to connect with the enterprise systems for centralized management, opening up new risks. The risks of ICS Cyber Incidents have been increasing, some of which have brought severe consequences. Although governments have classified these risks as a matter of national security, the successful prevention and mitigation of such incidents will increasingly depend on the ability of organizations to share cyber threat information and use it to improve their security posture.

New regulations, such as the Cyber Incident Reporting for Critical Infrastructure Act 2022 (CIRCIA), emphasize the need and urgency of reporting relevant details of a Cyber Incident. These reports will allow the relevant authorities (e.g. Cybersecurity and Infrastructure Security Agency (CISA)) to spot trends and quickly share critical information with network defenders to warn other potential victims. Can organizations that rely on ICSs improve their cybersecurity posture through Cyber Incident Reports? What are the necessary ingredients for Cyber Incident Reports to be effective?

This research aims to answer these questions by studying the current state of Cyber Incident Reporting in terms of definition, purposes, regulations and more. This research also seeks to

[1] With reference to the United States Code for Bills and Statues, Title 44, Chapter 35, Sub-Chapter II, and Section 3552[1], the term "Incident" means an occurrence that:
(1) actually or imminently jeopardizes, without lawful authority, the integrity, confidentiality, or availability of information or an information system; or
(2) constitutes a violation or imminent threat of violation of law, security policies, security procedures, or acceptable use policies.

understand the current Cyber Incident Reports formats available to the public and map out their advantages and disadvantages based on National Institute of Standards and Technology (NIST) Cybersecurity recommendations on Cyber Incident Reporting. In addition, this research evaluates the use of the MITRE ATT&CK (Adversarial Tactics, Techniques & Common Knowledge) Framework for ICS in a Cyber Incident report. This research could help ICS organizations improve their process of Cyber Incident reporting.

Thesis Supervisor
Stuart Madnick
John Norris Maguire Professor of Information Technologies, MIT Sloan School of Management & Professor of Engineering Systems, MIT School of Engineering

THIS PAGE INTENTIONALLY LEFT BLANK

ACKNOWLEGDEMENTS

This work would not have been possible without the help and support of several people. I would like to thank Professor Stuart Madnick for his guidance and support as my thesis supervisor. I also would like to thank Dr. Raphael Yahalom and Shaharyar Khan for their encouragement and feedback, which has been essential in shaping this work.

I would also like to thank the Cybersecurity at MIT Sloan Consortium (CAMS) for providing me a platform to share my research and providing valuable feedback. This work would not have been possible without the valuable input and feedback from the CAMS partners, in particular FM Global.

Finally, I would like to thank my family for their unwavering support and encouragement.

THIS PAGE INTENTIONALLY LEFT BLANK

Table of Contents

List of Figures

List of Tables

Introduction

This chapter provides a study on the current status of Cyber Incident Report. It starts with the background on the increased in Cyber Incidents and evolution of ICSs that explains why this topic is of such great interest. The discussion moves on to the definition, purposes and types of data, regulations and current statistics on Cyber Incident Report. Finally, primary research questions are posted that will guide the remainder of the thesis.

1.1 Background

In recent times, Cyber Incidents have increased in frequency and complexity. These incidents have come from a wide range of sources, from lone individuals to complex state-sponsored teams. In particular, these cyber-crime organizations have used a variety of tactics, techniques, and procedures (TTP) from exploiting well-known vulnerabilities to navigating highly sophisticated zero-day pathways in order to attack systems, sabotage critical services, commit financial crimes, and gather sensitive information for political gain (Johnson et al. (2016) [1]).

As defined by Lokus (2015) [2], Cyber-Physical incidents adversely affect physical space by targeting the computational and communication infrastructure that monitors and controls sensors and actuators. An example of a Cyber-Physical incident would be an attack that targets ICSs. ICSs are typically used in industrial control sectors such as electric, water and wastewater, oil and natural gas, transportation, chemical, pharmaceutical, pulp and paper, food and beverage, and discrete manufacturing (e.g., automotive, aerospace, and durable goods.)

These ICSs are vital to the operation of U.S. critical infrastructures that are often highly interconnected and mutually dependent. That being said, a Cyber-Physical incident in a critical infrastructure sector can cause considerable damage to a large number of people over a vast geographical area. With these severe consequences, it is a matter of national security to prevent such incidents on ICSs.

1.2 Evolution of Modern ICSs

Stouffer et al. (2015) [3] describes ICSs, which include Supervisory Control and Data Acquisition (SCADA) systems, Distributed Control Systems (DCS), and other control system configurations such as Programmable Logic Controllers (PLC), which are typically found in industrial control sectors. SCADA systems are generally used to control dispersed assets using centralized data acquisition and supervisory control. DCS are typically used to control production systems within a local area, such as a factory using supervisory and regulatory control. PLCs are often used for discrete control for specific applications and generally provide regulatory control.

Stouffer et al. (2015) [3] also noted that ICSs traditionally had little interaction with Information Technology (IT) systems as ICSs were isolated systems running proprietary control protocols using specialized hardware and software. Hence, many ICS components used to be in physically secured areas and the components were not connected to IT networks or systems. However, with the widely available, low-cost Internet Protocol (IP) devices now replacing proprietary solutions, ICS systems are no longer isolated from IT Systems in cyberspace even though it is physically located in different areas.

Furthermore, Stouffer et al. (2015) [3] also noted that the modern ICSs are adopting IT solutions to promote corporate business systems connectivity such as remote access capabilities. ICSs are designed and implemented using industry standard computers, operating systems (OS) and network protocols so much that they are starting to resemble IT systems. While this integration supports new IT capabilities, it provides significantly less isolation for ICSs from the outside world than predecessor systems, creating a greater need to secure these systems.

There have been many reported Cyber Incidents whilst previously predominately present in traditional IT systems, are now also prevalent in the ICSs environment amidst TTPs derived from IT System attack methodologies. Hence, ICSs inevitably inherit the possibility of cyber vulnerabilities by becoming connected with IT systems.

1.3 Definition of Cyber Incident

With reference to the United States Code for Bills and Statues, Title 44, Chapter 35, Sub-Chapter II, and Section 3552, the term "*Incident*" means an occurrence that:

1. actually or imminently jeopardizes, without lawful authority, the integrity, confidentiality, or availability of information or an information system; or
2. constitutes a violation or imminent threat of violation of law, security policies, security procedures, or acceptable use policies.

In short, there should be reasonable grounds to indicate malicious intent of the attempts or actual unauthorized access to the systems or data. The types of occurrences that are classified as *Cyber Incidents* should be exhaustive and the corresponding consequences of causing a *Cyber Incident* should be commensurate with the level of risk it carries. This is to deter potential cyber criminals from committing the act. Some examples are discussed as follows:

1. Tricking users into opening a document sent via email that is malware; running a document which infected their computers and establishing connections with an external host.
2. A user who provides or exposes sensitive information to others through peer-to-peer file sharing services.
3. User A who accesses User B's account intentionally by correctly guessing the password to User B's account but did not cause any damage.

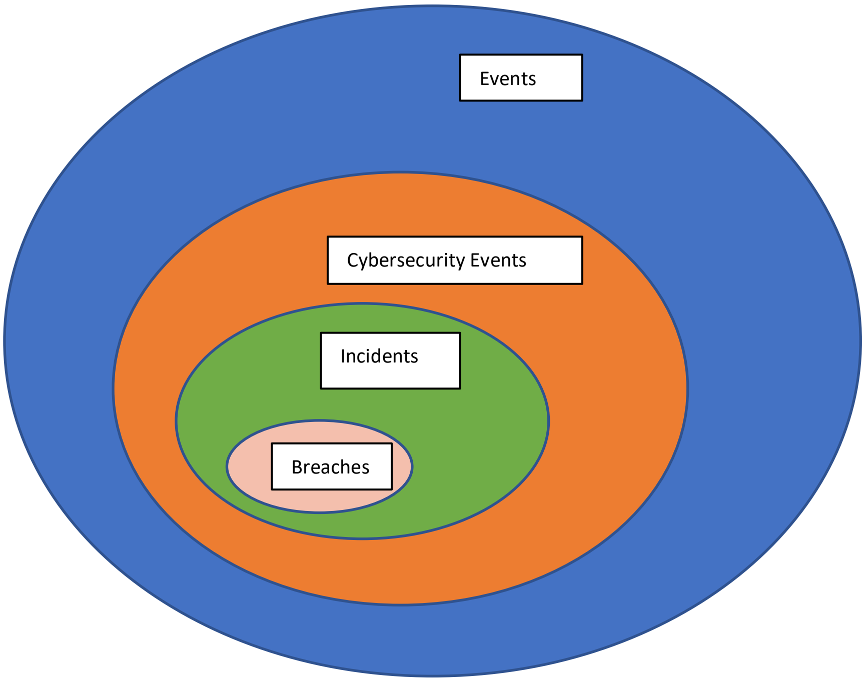


Figure 1: Relationships between Incidents and other occurrences in ICSs

As indicated in Figure 1, a Cyber Incident could lead to Breach or non-Breach of data and systems. A Breach[2] is defined as confirmed – not just potential - access of data or system to an unauthorised party. One example could be customers' sensitive information exposure when hackers compromise an organization's network and release stolen data on the web. An example of a Cyber Incident without Breach would be where an organization successfully stops a cyber-attack before the adversary had any success in gaining access or causing harm to data or system.

Cichonski et al. (2012) [4] defines an *event* as any observable occurrence in a system or network. There are many types of events, including *Cybersecurity Events*. Ross et al. (2021) [5] defines a *Cybersecurity Event* as a cybersecurity change that may have an impact on organizational operations (including mission, capabilities, or reputation). One example of a Cybersecurity Event that is non-Incident could be a planned system update. Another example

[2] 2020 Data Breach Investigations Report (DBIR), Verizon, https://www.verizon.com/business/resources/reports/dbir/2020/cheat-sheet/

could be User A who accesses User B’s account unintentionally as the session for User B was not logged off on a shared computer and did not cause any damage.

Boer and Idler (2021) [6] proposed standardization of key terminology that includes *Cyber Incident*. Boer and Idler defined a “Cyber Incident” as:

“The occurrence of actual harm to the confidentiality, integrity, or availability of an information system or the information that the system processes, stores, or transmit.”

Whereas a “Cyber Event” is defined as:

“The occurrence of actual and potential harm to the confidentiality, integrity, or availability of an information system or the information that the system processes, stores, or transmit or that constitutes a violation or imminent threat of violation of security procedures or acceptable use polices.”

Boer and Idler (2021) [6] and this research have the same approach in defining the relationships between the terms even though the actual terms used were different. However, Boer and Idler (2021) [6] does differ with this research in proposing to leave out the inclusion of “potential harm” and “imminent threat” to reduce the universe for potential reporting. For the sake of discussion, this research maintains the definition that both actual and imminently occurrences should be reported for two reasons as follows:

1. Emphasize on the seriousness of the action to attempt and criminalize this action. Every attempt to prob or scan someone else’s network or system should be made accountable by regulations.
2. Not all organisation can successfully fend off the attempt and some will not even be aware that the cyber-attack had been carried out. Hence, there may be corelated information of the same threat actor using similar TTPs.

Therefore, *Cyber Incident* should continue to include all actual and attempts of unauthorized access of system and network.

1.4 Purpose of Cyber Incident Report

Cyber Incidents happen every day and some are major while others are minor, but most of them are never reported. A recent U.S. Senate report [7], published by the Homeland Security and Government Affairs, concluded that there is a lack of comprehensive data on the amount of ransomware attacks and use of cryptocurrency as ransom payments in these attacks due to under-reporting. This fragmented and incomplete data regarding the breadth and dept of the ransomware threat was the reason for introducing the CIRCIA of 2021.

While the needs and benefits are obvious for the federal government to encourage and even regulate Cyber Incident reporting, the benefits are not clear for ICS organizations that are victims themselves. Hennin et al. (2008) [8] cited an analogy in the practice of mutual aid that are well established in the first responder community, such as municipal fire departments. He also mentioned that ICS organizations should recognize that the "health" of the wider industrial community is also in their own interest because of the complex system inter-dependencies that exist. Hence, there is more value in a cooperative rather than go-it-alone mentality. However, when the victim is recovering from the consequences of the incident, mandated Cyber Incident reporting will likely result in minimum information being provided to be compliant with the regulation.

The purpose of Cyber Incident reporting can be for a variety of reasons that would determine the type of details to be reported, some examples are listed in Table 1.

Types of Purpose	Example	Types of Details Required
Creating awareness	Alerting others that a certain type of attack exists	1. Type of Incident 2. Description of Incident 3. Technical details for detection 4. Measures for mitigation after incident Source: National Cyber Awareness System Alerts - https://www.cisa.gov/uscert/ncas/alerts/aa22-137a
Reporting a crime	Ransomware	1. Victim Information 2. Description of Incident 3. Financial Transaction such as ransom amount demanded, actual ransom paid, type of currency used, etc. 4. Perpetrator Information Source: Complaint Referral Form Internet Crime Complaint Center - https://ransomware.ic3.gov/default
Complying with Regulations	General Data Protection Regulation (GDPR)	1. Type of Incident 2. Description of Incident 3. Impact of Incident 4. Existing measures 5. Technical details for detection 6. Measures for mitigation after incident 7. Correspondences with Authorities Source: 72 Hours: Understanding the GDPR Data Breach Reporting Timeline - https://www.imperva.com/blog/72-hours-understanding-the-gdpr-data-breach-reporting-timeline/
Insurance Claims	Cyber Insurance Claims	1. Type of Incident 2. Description of Incident 3. Contact of relevant employees 4. Impact of Incident

		5. Existing measures 6. Measures for mitigation after incident 7. Perpetrator Information (For ransomware only) 8. Confirmation if Incident has become public 9. Correspondences with Authorities 10. Other Insurance coverage Source: Edge underwriting Cyber Claim Form - https://edgeunderwriting.com.au/cyber-claim-form
Instilling an internal company culture	Develop habit of incident reporting similarly to safety culture in workplace	1. Type of Incident 2. Description of Incident 3. Impact of Incident 4. Existing measures 5. Technical details for detection 6. Measures for mitigation after incident

Table 1: Purposes for Cyber Incident Report and its required information

With these examples, there are both push and pull factors for *Cyber Incident* Reporting. Once the benefits of reporting are assimilated, organizations will be able to recognize the significance and step-up efforts to implement Cyber Incident reporting accordingly. Otherwise, it would end up having regulations to enforce the need of incident reporting.

1.5 Types of Data for Cyber Incident Report

The types of data required for Cyber Incident reporting are important to derive meaningful information about the trend of attacks and help decision makers make informed choices. Other than the fundamental technical details that most Cyber Incident reports require, such as precursors, indicators and TTPs of the incident to detect similar incidents, other data are valuable in building a bigger picture of the problem. Some examples for the types of data to report are:

1. What are the controls to the vulnerability that were exploited? This is to identify if there are controls that exist or the vulnerability (e.g., Zero-days attacks) was not known in the first place. For an unknown vulnerability, a different control measure would be required compared to a known vulnerability with controls that exist such as an advanced heuristic-based detection system.
2. For ransomware, what is the amount of ransom demanded and the amount of ransom actually paid? This data could be used to understand the negotiation mentally and identify the threat actors using the behavior trades.
3. For ransomware, did the victim recover their data when ransom was paid? This could be a good indication if ransom should have been paid in the first place.

4. For ransomware, what was the form of currency requested for the ransom? This could indicate which currency needs to be regulated more strictly.

Varga et al. (2020) [9] evaluated information elements in Cyber Incident reporting to support time-critical and high mental workload situation for incident management. The research team conducted an experiment with the Swiss Military in a Cyber Range environment where cyber defence analysts responded to Cyber Incidents simulated in a closed environment. The paper shared their findings using Cyber Incident report templates with five sections: (1) About the report, (2) What happened, (3) Consequences, (4) Impact, and (5) Actions. The cyber defence analyst rated the respective sections in terms relevancy to defend their systems against similar attacks. Their evaluation concluded that except for the section on (4) Impact, all other sections were relevant for a technical cyber defence team. It was noted that the category (4) Impact was mainly used to update relevant stakeholders, specifically management reporting. The section on (5) Actions was the most? relevant as it included control measures already taken or planned. This further emphasized that control measures are critical in detecting and mitigating vulnerabilities. However, there was no information on whether there were any controls to prevent the vulnerability in the first place. We will further explore other guides and formats of Cyber Incident reports in Chapter 3.

1.6 Regulations on Cyber Incident Report

In March 2022, the U.S. Congress passed a significant new cybersecurity law, The Strengthening American Cybersecurity Act 2022 [10], that includes the following three regulations:

1. The Federal Information Security Modernization Act of 2022
2. Cyber Incident Reporting for Critical infrastructure Act (CIRCIA) of 2022 (H.R. 5440)
3. Federal Secure Cloud Improvement and Jobs Act of 2022

This work will focus on (2) CIRCIA of 2022, which seeks to establish a Cyber Incident Review Office (refer to as “Office”) in the CISA of the Department of Homeland Security (DHS). The Office is empowered to coordinate and enforce matters regarding Cyber Incident reported by entities in the critical infrastructure sector. This includes requiring critical infrastructure entities to report material cybersecurity incidents within 72 hours and ransomware payments within 24 hours to the CISA from the time the entity reasonably believes the incident occurred. This regulation has also defined “Incident” according to United States Code for Bills and Statues, Title 44, Chapter 35, Sub-Chapter II, and Section 3552.

1.6.1 Types of Critical Infrastructure Entities

Under Section 2242 on the Required Reporting of Certain Incidents [10], the Office is also responsible for determining the critical infrastructure entities that are required to comply with CIRCIA. In determining this, the entities will need to have one or more of the following types[3]:

1. the consequences that disruption to or compromise of such an entity could cause to national security, economic security, or public health and safety;
2. the likelihood that such an entity may be targeted by a malicious cyber actor, including a foreign country;
3. the extent to which damage, disruption, or unauthorized access to such an entity will disrupt the reliable operation of other critical infrastructure assets; and
4. the extent to which an entity or sector is subject to existing regulatory requirements to report cybersecurity incidents and the possibility of coordination and sharing of reports between the Office and the regulatory authority to which such entity submits such other reports.

The reporting requirements for CIRCIA will cover 16 sectors of the economy detailed in the [4]Presidential Policy Directive 21 (PPD-21).

1.6.2 Format Requirements of a Cyber Incident Report

Under Section 2242 on the Required Reporting of Certain Incidents, the Office is also responsible in determining the format of report for the covered entities' compliance. In addition, under Section 2244, the Office can obtain the required information about the Cyber Incident or ransom payment by engaging the relevant organization directly if the organization fails to comply with the requirement to report and the authority will issue a subpoena if the organization fails to cooperate. The required information for the report includes the following:

1. A description of the covered Cyber Incident, including affected functions, impact to operations and relevant timeline.
2. A description of the vulnerabilities exploited and the security defences that were in place, as well as the tactics, techniques, and procedures used to perpetrate the covered Cyber Incident.

[3] H.R.5440 Cyber Incident Reporting for Critical Infrastructure Act of 2021, https://www.congress.gov/bill/117th-congress/house-bill/5440/text

[4] Presidential Policy Directive – Critical Infrastructure Security and Resilience, https://obamawhitehouse.archives.gov/the-press-office/2013/02/12/presidential-policy-directive-critical-infrastructure-security-and-resil

3. Any identifying or contact information related to each actor reasonably believed to be responsible for such Cyber Incident.
4. Identification of the category or categories of information that were, or are reasonably believed to have been, accessed or acquired by an unauthorized person.
5. Information to identify affected entity
6. Contact information for liaising with the Office

Notably, it is required to report the security defences that were in place and it should include the details on the failure of these defences. This is critical as many incidents were caused by control measures that exist but were not implemented correctly. For example, to reduce the likelihood of password guessing, one of the control measures would be to implement complex password requirement. However, if the administrator of the system did not correctly implement this control, it will not be effective. Other examples such as the Capital One Data Breach by Neto et al. (2020) [11], also discussed about the Cyber Incident caused by failure to implement proper security controls. It was also reported[5] by DHS in 2021 that systemic cybersecurity failures persist across federal agencies that are putting American's personal information at risk. Hence, it is evident that documenting failed controls is critical in a Cyber Incident report.

1.6.3 Finalizing the CIRCIA of 2022

Under Section 2242 on the Required Reporting of Certain Incidents [10], the Office must promulgate a proposed implementing regulation within 24 months from final enactment date of March 15, 2022, and a final regulation no later than 18 months thereafter. The effective date of the act's reporting requirements will be set by the final rule.

CIRCIA of 2022 is intended to provide the federal government with a better understanding of the nation's cyberthreats that includes ransomware and facilitate a coordinated national response to them. The FBI currently provides an avenue for *voluntarily* sharing information about Cyber Incidents. This avenue contributed to FBI's yearly report on the trend of Cyber Incidents to help the public make informed decisions on security policies. However, it is estimated that only a quarter[6] of Cyber Incidents are actually reported to the FBI.

Separately, current Department of Home Security (DHS) Transportation Security Administration (TSA) directives[7] impose cybersecurity and reporting requirements for designated transportation operators and pipelines. Existing directives require select

[5] New Bipartisan Portman-Peters Report Shows Federal Agencies' Cybersecurity Failures Leaving Americans' Personal Information at Risk, https://www.hsgac.senate.gov/media/minority-media/new-bipartisan-portman-peters-report-shows-federal-agencies-cybersecurity-failures-leaving-americans-personal-information-at-risk

[6] Congress Passes Cyber Incident Reporting for Critical Infrastructure Act of 2022, https://datamatters.sidley.com/congress-passes-cyber-incident-reporting-for-critical-infrastructure-act-of-2022

[7] DHS Announces New Cybersecurity Requirements for Critical Pipeline Owners and Operators, https://www.dhs.gov/news/2021/07/20/dhs-announces-new-cybersecurity-requirements-critical-pipeline-owners-and-operators

transportation and pipeline entities to report to CISA, within 24 hours, cyber events that have been confirmed or have the potential to disrupt operations.

The CIRCIA OF 2022 further emphasizes the importance of Cyber Incident Reporting and the critical component in the success would be the ease of complying with this law. This would require specific guidelines for respective organizations to report relevant and timely information such as the specific classification of *Cyber Incidents* for this regulation. In addition, the question remains for the Office if the information to be shared can help other organizations learn, detect and mitigate similar attacks.

1.6.4 Other Similar Regulations – U.S. Securities and Exchange Commission

In March 2022, the U.S. Securities and Exchange Commission (SEC) proposed new rules on cybersecurity for public companies. These amendments come four years after the SEC's previous guidance back in 2018. The proposed rules require reporting of ongoing cybersecurity breaches, updates on previously reported incidents, and detailing of the policies and procedures a company is implementing to identify and manage cybersecurity threats. The rules also explain in detail what Form 8-K[8] should contain when reporting incidents. These rules are intended to keep investors informed about the risk management strategies of the companies they are involved with, as well as increase corporate accountability.

Although the SEC does not expect a public company to disclose technical information about its cybersecurity systems, potential vulnerabilities or response to a cybersecurity incident, disclosure of the following information[9] for each material cybersecurity incident are required:

1. when the incident was discovered and whether it is ongoing
2. a brief description of the nature and scope of the incident
3. whether any data was stolen, altered, accessed or used for any other unauthorized purpose
4. the effect of the incident on the company's operations
5. whether the company has remediated or is currently remediating the incident

In particular, the triggering event for disclosure is *not* the date of the cybersecurity incident. Rather, disclosure would be within four days after the company "determines that a cybersecurity incident it has experienced is material."[10] Notwithstanding allowing the exercise of discretion (which effectively codifies the longstanding concept of "ripeness" in determining materiality), the SEC expects public companies "to be diligent in making a

[8] Form 8-K is the "current report" companies must file with the SEC to announce major events that shareholders should know about.

[9] SEC Proposes Cybersecurity Incident and Governance Disclosure Obligations for Public Companies, Scott M., Shardul D, and Ira R., March 14, 2022, Holland & Knight Law: https://www.hklaw.com/en/insights/publications/2022/03/sec-proposes-cybersecurity-incident-and-governance-disclosure

[10] Cybersecurity Risk Management, Strategy, Governance and Incident Disclosure Proposed Rule ("Proposed Rule"), at 22

materiality determination."[11] "Materiality is to be determined under longstanding precedent of whether there is a substantial likelihood that a reasonable shareholder would consider the information as important or as having significantly altered the total mix of information made available. The SEC acknowledged that this materiality analysis "is not a mechanical exercise" but rather would require the company to "thoroughly and objectively evaluate the total mix of information…"

In summary, the four days' timeline stated in the CIRCIA and new SEC cybersecurity regulations did not give companies any pressure, given that there was no stated timeline to determine the materiality of the C*yber Incident.* And Cyber Incidents such as the Ukraine Power Grid Attack 2015 showed that adversaries remains undetected in the network for several months so the time from initial compromise to detection could add up.

1.7 Statistics on Cyber-physical Incidents

In 2021, Skybox Security (2021) [12] reported 83% of organizations that manage critical infrastructure experienced a Cyber Incident. Yet, the biggest concern comes from the responses from company leadership as that same study found that 73% of CISOs and CIOs (Chief Information Security Officer and Chief Information Officer) indicated a high level of confidence that their company would not be victims of a breach in the coming years. This is in stark comparison to only 37% of plant managers, who have more first-hand experience with the repercussion of attacks. This result prompted Skybox Security to summarize the report by stating that overconfidence foreshadows future breaches. This considerable disparity between the perception and the reality of threats in the company leadership has prompted regulators to make certain changes. Regulators have begun to instil stricter regulations, holding companies and therefore CISOs accountable for ethical and timely disclosure of cyber breaches, such as Cyber Incident Reporting for Critical Infrastructure Act 2022 (CIRCIA).

In June 2021, the FBI began tracking reported ransomware incidents where the victim was a member of a critical infrastructure sector (FBI (2022) [13]). Ransomware is a type of malicious software, or malware, that encrypts data on a computer, making it unusable. A malicious cyber-criminal holds the data hostage until the ransom is paid. If the ransom is not paid, the victim's data remains unavailable. Cyber criminals may also pressure victims to pay the ransom by threatening to destroy the victim's data or to release it to the public.

There are 16 critical infrastructure sectors as mentioned in Section 1.6.1 whose assets, systems, and networks, whether physical or virtual, are considered so vital to the United

[11] Proposed Instruction 1 to Item 1.05 states that "a registrant shall make a materiality determination regarding a cybersecurity incident as soon as reasonably practicable after discovery of the incident." Proposed Rule, at 22; Proposed Instruction 1 to Proposed Item 1.05 of Form 8-K.

States that their incapacitation or destruction would have a debilitating effect on the security, national economy, public health or safety, or any combination thereof. The FBI received 649 reports of ransomware attacks where victims belong. Of the 16 critical infrastructure sectors, FBI reported that 14 sectors (Figure 2) had at least one member that fell victim to a ransomware attack in 2021, with the Healthcare and Public Health, Financial Services, and Information Technology sectors registering the most victims. The FBI anticipates an increase in critical infrastructure victimization in 2022.

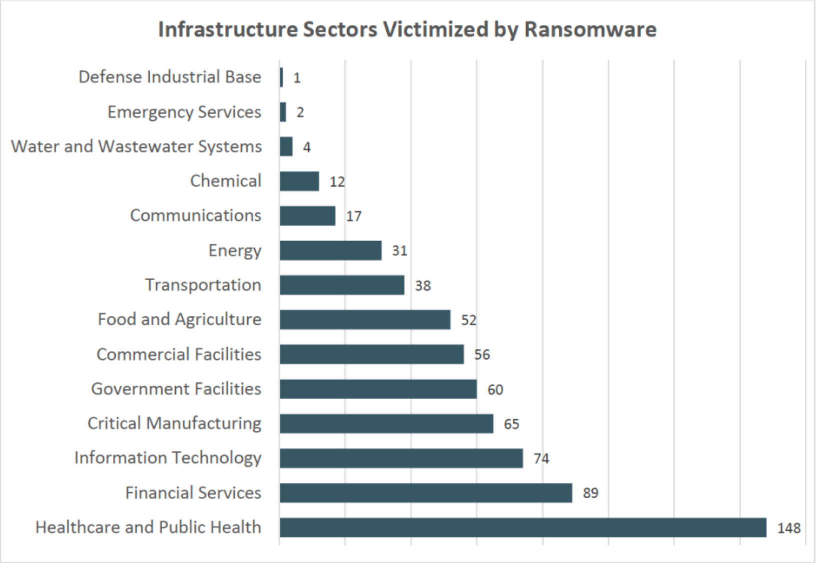


Figure 2: Infrastructure Sectors victimized by Ransomware

The FBI does not encourage paying a ransom to criminal actors as it does not guarantee that a victim's data will be recovered. Other government security agencies such as the CISA (CISA [14]) also encourages reporting of Cyber Incidents so that victims can receive assistance from government agencies if necessary. The agencies are able to assist in investigating the incident, mitigate its consequences and help prevent future incidents. For example, the DHS has highly trained investigators who specialize in responding to Cyber Incidents for the express purpose of disrupting threat actors who caused the incident and preventing harm to other potential victims.

Mediating actions and follow ups steer the future course of the organization. And this largely hinges of the accuracy, relevancy and completeness of a Cyber Incident Report, which is imperative to an organisation.

1.8 Objectives and Research Questions

With the need and urgency for Cyber Incident Reporting in Critical Infrastructure, this work aims to evaluate the current Cyber Incident Report formats available to the public from cybersecurity federal agencies and vendors. This study aims to understand the current Cyber Incident formats, map out their advantages and disadvantages based on National Institute of Standards and Technology (NIST) Cybersecurity recommendations on incident reporting, and identify the necessary changes and benefits if the format adopts the MITRE ATTACK Framework for ICS. The MITRE ATT&CK Framework is a widely adopted knowledge base of TTP by cybersecurity teams to understand adversary behaviour and tradecraft. The results of this research could help ICS organizations improve their Cyber Incident Report formats for the improvement of cybersecurity posture. Specifically, the questions that would be asked throughout this analysis are:

1. What are the advantages and disadvantages of the current publicly available Cyber Incident Report formats/templates from cybersecurity federal agencies and vendors?
2. Can Cyber Incident Report format adopting the MITRE ATTACK Framework for ICS be beneficial in improving Cybersecurity posture?

1.9 Thesis Structure

This section maps out the following sections with the research plans:

Chapter 2 – Literature Review: Contains a literature review covering the current community research on Cyber Incident reports for both industrial and academic sectors.

Chapter 3 - Evaluation of Existing Cyber Incident Report Format: Provides an evaluation of current Cyber Incident Report Formats that are available to the public by organizations like the federal government and security vendors. The evaluation includes the advantages and disadvantages of their formats for the intended purpose of reporting.

Chapter 4 – MITRE ATTACK Framework for ICS: Provides the overview on MITRE ATT&CK Framework that covers its background, possible use cases and types of information sharing it facilitates.

Chapter 5 – Evaluation of Proposed Cyber Incident Report Format: Provides an evaluation on the use of MITRE ATT&CK Framework for ICS in a Cyber Incident Report Format. The evaluation compares three different Cyber Incident Cases that occurred in three different periods to derive potential learning points.

Chapter 6 – Conclusion: Summarizing the lessons learned in this research on Cyber Incident Reports, limitations of this research and the possible future research paths are proposed.

Literature Review

This chapter discusses a variety of approaches currently used in industry as well as those found in academic literature for Cyber Incident reporting in ICSs.

2.1 Information Technology Based Approaches

NIST guides have been internationally regarded as the “gold” standard that the Cybersecurity industry refers to for guidance in managing their security posture. This section discusses the various NIST developed guides that are relevant to Cyber Incident reporting in ICSs.

2.1.1 Guide to Industrial Control Systems (ICSs) Security, SP 800-82 R2 (Stouffer et al. [3])

Stouffer et al. [3] indicated an effective cybersecurity program for an ICS should apply a strategy known as “defense-in-depth,” a layering security mechanism such that the impact of a failure in any one mechanism is minimized. This “defense-in-depth” strategy is based on practices and design principles prevalent in the IT system security world. One example is to implement security controls such as intrusion detection software, antivirus software and file integrity checking software, where technically feasible, to prevent, deter, detect, and mitigate the introduction, exposure, and propagation of malicious software to, within, and from the ICS.

Stouffer et al. [3] refers to the NIST Framework for Improving Critical Infrastructure Cybersecurity for ensuring that the organization develops the core competencies to manage cybersecurity risk.

2.1.2 Framework for Improving Critical Infrastructure Cybersecurity, v1.1 **(NIST 2018 [15])**

This framework (NIST 2018 [15]) advises having five essential functions as the Framework Core to organize basic cybersecurity activities at their highest level. These five functions are Identify, Protect, Detect, Respond, and Recover. They aid an organization in expressing its management of cybersecurity risk by organizing information, enabling risk management decisions, addressing threats, and improving by learning from previous activities.

The specific area that is relevant to this work would be the Respond function where there is a category on Communications with a Unique Identifier (RS.CO). This is a category where response activities are coordinated with internal and external stakeholders. Furthermore, there is a subcategory within the Unique Identifier of RS.CO-2 where Incidents reported are consistent with established criteria developed by the organisation. This subcategory of incident response corresponds to other forms of cybersecurity informative references that are available as IT systems guides.

Function	Category	Subcategory
RESPOND (RS)	**Communications (RS.CO):** Response activities are coordinated with internal and external stakeholders (e.g. external support from law enforcement agencies).	**RS.CO-2:** Incidents are reported consistent with established criteria

Table 2: NIST Cybersecurity Framework on Incident Response (NIST 2018 [6])

This guide (NIST 2018 [15]) further advises its readers to refer to the guide (Cichonski et al. 2012 [7]) for further guidance on incident handling.

2.1.3 Computer Security Incident Handling Guide, SP 800-61 R2 **(Cichonski et al. [4])**

Cichonski et al. [4] initially developed this guide primarily for IT Systems but it has become relevant to ICSs. This guide recommends the incident response team document information such as the status of the incident, a summary of the incident, indicators related to the incident, actions taken by incident handlers, chain of custody, impact assessments, contact information of involved parties, evidence gathered during investigation, and follow-up action to improve the security posture.

Section 3.4 Post-Incident Activity of this guide emphasizes the importance of learning and improving incident response by conducting “lessons learned” meeting with all involved parties after a major incident. The involved parties should consist of respective stakeholders who were appointed in the initial Cyber Incident response plans. This meeting provides a platform to achieve closure with respect to an incident by reviewing what occurred, what was done to intervene, and how well the intervention worked. The meeting should be held within several days of the end of the incident. The questions to be answered in the meeting include:

1. Exactly what happened, and at what times?
2. How well did staff and management perform in dealing with the incident? Were the documented procedures followed? Were they adequate?
3. What information was needed sooner?
4. Were any steps or actions taken that might have inhibited the recovery?
5. What would the staff and management do differently the next time a similar incident occurs?
6. How could information sharing with other organizations have been improved?

7. What corrective actions can prevent similar incidents in the future?
8. What precursors or indicators should be watched for in the future to detect similar incidents?
9. What additional tools or resources are needed to detect, analyse, and mitigate future incidents?

2.1.4 Security and Privacy Controls for Information Systems and Organisations, SP 800-53 R5 **(NIST 2020 [16])**

This guide (NIST 2020 [16]) on security and privacy controls was initially developed for IT systems and it has become relevant for ICS. The section on the control to track and document incidents (IR-5) discusses documenting incidents that includes maintaining records about each incident, the status of the incident, and other pertinent information necessary for forensics, as well as evaluating incident details, trends, and handling. Incident information can be obtained from a variety of sources, including network monitoring, incident reports, incident response teams, user complaints, supply chain partners, audit monitoring, physical access monitoring, and user and administrator reports.

Loukas [2] mentioned that the traditional protection mechanisms in cyberspace are largely applicable to cyber-physical systems although differences exist in implementation and effectiveness. Table 2 below summarizes some examples on the similarities and differences between protection mechanisms application in IT Systems and ICSs.

Type of Control Measures	Similar deployments between IT and ICS	Differing deployments between IT and ICS
Authentication	Password-based authentication is often the first line of defence	ICS often has no implementation of multiple factors of authentication such as “what you know” or “what you have”
Access Control	Attribute-based access control is widely used	Attribute-based access control works more effectively for ICS due to the highly automated routine environment.
Firewall	Commercial firewalls increasingly support ICS communication protocols	Not all types of firewalls can support ICSs such as Stateless firewalls as they are not effective with its current filtering system

Intrusion Detection	Knowledge-based and Behaviour-based mechanisms works effectively for ICSs	Behaviour-based mechanisms work more effectively for ICSs due to the highly automated and routine environment. There are currently no widely available knowledge-based mechanisms for ICSs due to its rather short period of new developments.

Table 3: Examples on the type of control measures for IT and ICS

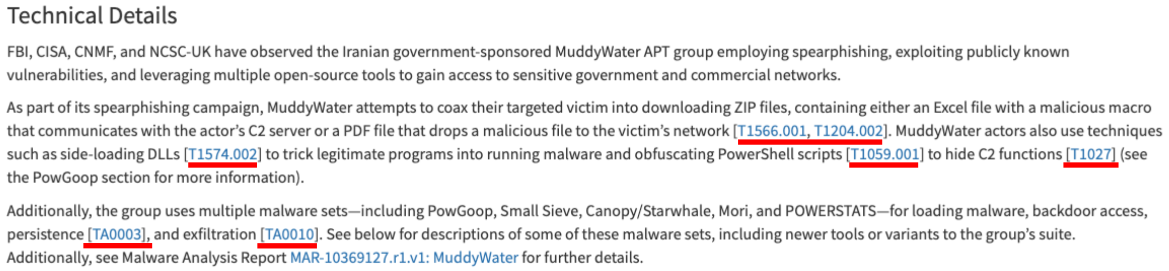
This opinion was supported by *Stouffer et al.* [3], “While security solutions have been designed to deal with these security issues in typical IT systems, special precautions must be taken when introducing these same solutions to ICS environments.”

Center for Internet Security (CIS) also supported the view that it is not uncommon for an ICS Incident Response plan to require an augmentation of IT plans and procedures already in place for an enterprise IT system in order to be relevant, applicable and complete for Operational Technology where ICS is a subset under this category of technology (CIS Controls v7, 17]). Many others (Homeland Security 2009 [18] and Pauna, A. et al. [19]) also discussed that security solutions needed to be tailored to the ICS environment as they differs significantly from traditional IT systems.

2.2 Incident Response using MITRE ATT&CK Framework

Many cybersecurity vendors promote the use of the MITRE ATT&CK Framework in incident response. One of the cybersecurity vendors, Huntsman, published a blog [20] on how the MITRE ATTACK matrix can be used to complement the work of the incident response team in the Security Operations Centre (SOC). It details how the MITRE ATT&CK Framework can help incident responders structure and streamline their investigations in IT Systems. By referring to the MITRE ATT&CK Framework, the Cybersecurity Incident Response Team (CSIRT) can match their stage of attack at present moment and work backwards for initial access or to predict the attackers’ next move. This can help save precious time in containing the attack and use it on recovering from the attack instead. Trend Micro [21] also supports the optimization of incident response planning using the MITRE ATT&CK Framework as their cybersecurity analysts shared that it helped them build on the full chain of attack during an incident.

CISA and CIS also actively promoted the use of the MITRE ATT&CK Framework through security advisories that tag TTPs to their IDs in the MITRE ATT&CK Framework. Examples from CISA (Figure 3) and CIS (Figure 4) can be seen below showing that the technical details of their security alerts, (AA22-055A) for CISA and (MS-ISAC 2022-084) for CIS, tags the TTPs to the IDs in the MITRE ATT&CK Framework.



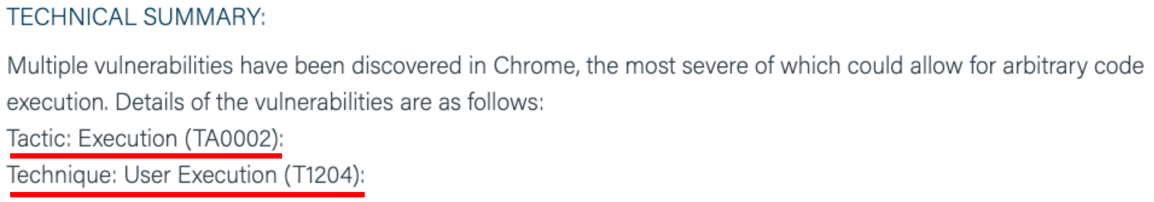
Technical Details

FBI, CISA, CNMF, and NCSC-UK have observed the Iranian government-sponsored MuddyWater APT group employing spearphishing, exploiting publicly known vulnerabilities, and leveraging multiple open-source tools to gain access to sensitive government and commercial networks.

As part of its spearphishing campaign, MuddyWater attempts to coax their targeted victim into downloading ZIP files, containing either an Excel file with a malicious macro that communicates with the actor's C2 server or a PDF file that drops a malicious file to the victim's network [T1566.001, T1204.002]. MuddyWater actors also use techniques such as side-loading DLLs [T1574.002] to trick legitimate programs into running malware and obfuscating PowerShell scripts [T1059.001] to hide C2 functions [T1027] (see the PowPoop section for more information).

Additionally, the group uses multiple malware sets—including PowGoop, Small Sieve, Canopy/Starwhale, Mori, and POWERSTATS—for loading malware, backdoor access, persistence [TA0003], and exfiltration [TA0010]. See below for descriptions of some of these malware sets, including newer tools or variants to the group's suite. Additionally, see Malware Analysis Report MAR-10369127.r1.v1: MuddyWater for further details.

Figure 3: CISA security alert (AA22-055A) [22] that refers to MITRE ATT&CK Framework



TECHNICAL SUMMARY:

Multiple vulnerabilities have been discovered in Chrome, the most severe of which could allow for arbitrary code execution. Details of the vulnerabilities are as follows:
Tactic: Execution (TA0002):
Technique: User Execution (T1204):

Figure 4: CIS security alert (MS-ISAC 2022-084) [23] that refers to MITRE ATT&CK Framework

The use of the MITRE ATT&CK Framework helps in identifying known TTPs and aids the investigator on possible routes that the Threat Actors might come from or move onto in IT Systems. However, it is only based on the technical aspect of the incident and does not include the human or organizational controls that failed played a part in this hazard. In addition, the security advisories on ICSs are not tagged to the MITRE ATT&CK Framework for ICSs. It would be an opportunity for this work to explore the use of MITRE ATT&CK Framework in an ICS' Cyber Incident Report.

2.3 Summary

This chapter presented a variety of approaches currently used in the Cybersecurity industry and academic literature for reporting Cyber Incidents. The chapter started by presenting traditional IT-security biased approaches prevalent in the industry. It was noted that multiple researchers view that it is common to extend IT Incident Response Plans to ICS but it there is a need to further tailor them to ensure that it is relevant and applicable for ICS. For the next chapter, this work will focus on the current Cyber Incident Report format that are used by various regulators and vendors.

3. Evaluating Cyber Incident Report Formats

This chapter provides an evaluation of current Cyber Incident Report Formats that are available to the public by organizations like the federal government and security vendors. The evaluation includes the advantages and disadvantages of their formats for the intended purpose of reporting.

3.1 Methodology for Evaluation

This research reviewed 30 Cybersecurity guides, listed in Table 3, relating to Cybersecurity Incident Reports for ICSs from major cybersecurity regulatory agencies and vendors. The majority of these guides provide strategies in developing a full plan to respond to cybersecurity incidents. However, as there is no official standard Cyber Incident Report format, most of these cybersecurity guides advised organizations to develop their own format.

No	**Title**	**Author/Publish**
1	National Association of Secretaries of State (NASS) Cybersecurity Resource Guide	National Association of Secretaries of State (NASS)
2	Cybersecurity Capability Maturity Model (C2M2) Version 2.0 July 2021.pdf	U.S. Department of Energy
3	NIST Cybersecurity Framework SANS Policy Templates	Multi-State Information Sharing & Analysis Center (MS-ISAC)
4	OE-417 Electric Emergency Incident and Disturbance Report	U.S. Department of Energy
5	Public Power Cyber Incident Response Playbook	American Public Power Association
6	Ransomware Guide	Multi-State Information Sharing & Analysis Center (MS-ISAC)
7	Computer Security Incident Handling Guide Special Publication 800-61 Revision 2	National Institute of Standards and Technology (NIST)
8	Guide to Cyber threat Information Sharing Special Publication 800-150	National Institute of Standards and Technology (NIST)
9	Enhanced Security Requirements for Protecting Controlled Unclassified Information Special Publication 800-172	National Institute of Standards and Technology (NIST)
10	Cyber Incident Reporting Law	Indiana Office of Technology
11	Security Lifecycles in the ISA/IEC 62443 Series Security of Industrial Automation and Control Systems	Global Cybersecurity Alliance
12	Cyber Security Incident Response Guide Version 1	CREST
13	Department of Health and Human Services (DHHS) Cybersecurity Program	Department of Health and Human Services (DHHS)
14	US-CERT Federal Incident Notification Guidelines	US-Computer Emergency Response Team (CERT)

15	CIP-008-6 Cyber Security Incident Reporting and Response Planning	North America Electric Reliability Corporation (NERC)
16	Reliability Guideline Cyber Intrusion Guide for System Operators	North America Electric Reliability Corporation (NERC)
17	Example Incident Response Plan	Michigan State Police
18	Incident Handling Annual Testing and Training	K. Holland, SANS Institute
19	National Cyber Incident Response Plan	Department of Homeland Security (DHS)
20	Customizable Incident Response Plan	Cynet
21	Cybersecurity Incident & Vulnerability Response Playbooks	Cybersecurity and Infrastructure Security Agency (CISA)
22	Best Practices for Victim Response and Reporting of Cyber Incidents	U.S. Department of Justice
23	Incident Response Checklist	Cybersecurity Agency of Singapore (CSA)
24	Framework for Improving Critical Infrastructure Cybersecurity	National Institute of Standards and Technology (NIST)
25	Guide to Industrial Control System (ICS) Security Special Publication 800-82 Revision 2	National Institute of Standards and Technology (NIST)
26	Security and Privacy Controls for Information Systems and Organizations Special Publication 800-53 Revision 5	National Institute of Standards and Technology (NIST)
27	Cyber Security Metrics and Measures	National Institute of Standards and Technology (NIST)
28	Cyber Resilience Supplemental Resource Guide – Volume 5 Incident Management Version 1.1	Carnegie Mellon University
29	Cyber Incident Management	Swedish Civil Contingencies Agency
30	Enhancing Resilience Through Cyber Incident Data Sharing and Analysis	Department of Homeland Security (DHS)

Table 3: List of Cybersecurity Incident Reporting Guides reviewed for recommended formats

Most of these guides further recommend that organizations seeking to develop their own Cyber Incident format to reference the NIST Cybersecurity Framework (NIST 2018 [15]) for guidance. Hence, this research assumes the need to develop a baseline *Cyber Incident* Report format using NIST Cybersecurity Framework recommendation for Incident Response.

3.2 Baseline Cyber Incident Report Format

With the assumption that the NIST Cybersecurity Framework (NIST 2018 [15]) has been unanimously regarded as the "gold standard", this research seeks to establish a baseline Cyber Incident Report format using the NIST Cybersecurity Framework principles on Incident Response. As reviewed in Section 2.1, NIST Cybersecurity Framework (NIST 2018 [15]) recommends a Response function to ensure reporting of incidents consistently with established criteria. More guidelines (NIST 2020 [16]) were given in terms of documenting incidents, which includes maintaining records about each incident, the status of the incident, and other pertinent information necessary for forensics as well as evaluating incident details, trends, and handling.

Cichonski et al. [4] emphasized the importance of learning and improving after the incident for the incident response teams and proposed nine specific questions on required information during post incident reviews session. Using the nine specific questions, this work established 18 *Information Elements* corresponding to the questions to use as a baseline as shown in the Table 3. This baseline will be used to compare with other existing Cyber Incident Report formats upon a total score of 18. Half a score will be indicated if the questions are not specific in indicating the established criteria but covers the category it is in.

No	**Questions on required information**	**Corresponding *Information Elements***
1	Exactly what happened, and at what times?	1. Incident description that includes the TTPs and timeline 2. Impact description and timeline
2	How well did staff and management perform in dealing with the incident? Were the documented procedures followed? Were they adequate?	3. Time from attack to detection 4. Time from detection to isolation 5. Time from isolation to recovery 6. Details on stakeholder reporting
3	What information was needed sooner?	7. Investigation description and timeline
4	Were any steps or actions taken that might have inhibited the recovery?	8. Recovery description that includes containment and timeline 9. Reflection on redundant recovery plans
5	What would the staff and management do differently the next time a similar incident occurs?	10. Details on each stage of incident response (to be compared with similar stages in other incidents)
6	How could information sharing with other organizations have been improved?	11. Platform for sharing cyber threat 12. Structure data inputs for analytics
7	What corrective actions can prevent similar incidents in the future?	13. Control failure for incident 14. Add new or modify existing control to prevent incident
8	What precursors or indicators should be watched for in the future to detect similar incidents?	15. Indicators of Compromise (IOC)[12] 16. Indicators of Attacks (IOA)[13] 17. Indicators of Interest (IOI)[14]
9	What additional tools or resources are needed to detect, analyze, and mitigate future incidents?	18. Gap in capabilities to manage cyber risk

Table 4: Using NIST guiding principles (Cichonski et al. [4]) to derive Information Element

[12] Forensic artifacts or remnants of an intrusion that can be identified on a host or network

[13] a series of actions that an adversary must conduct in order to succeed in the Cyber attack, defined by CrowdStrike and Intel/McAfee in 2014

[14] Information that acts in a supporting role to the identification and definition of an IOC.

This research also uses another NIST Incident Handling checklist (Cichonski et al. [4]) to verify if the 18 *Information Elements* covers all major steps in an NIST Incident Handling Plan. The 18 *Information Elements* should guide the reporter in avoiding ambiguous answers and creating a systematic flow to ease the documentation process. Table 5 shows that all the questions required in the NIST Incident Response checklist were fulfilled by the 18 *Information Elements* to ensure that the final report would be structured properly.

Stage	**Description of Action**	**Proposed Format with 18 *Information Element***
Detection and Analysis		
1.	Determine whether an incident has occurred	1. Incident description that includes the TTPs and timeline
1.1	Analyze the precursors and indicators	2. Indicators of Compromise (IOC) 3. Indicators of Attacks (IOA) 4. Indicators of Interest (IOI)
1.2	Look for correlating information	5. Investigation description and timeline 6. Time from attack to detection 7. Time from detection to isolation 8. Details on Stakeholder reporting 9. Impact description and timeline
1.3	Perform research (e.g., search engines, knowledge base)	
1.4	As soon as the handler believes an incident has occurred, begin documenting the investigation and gathering evidence	
2.	Prioritize handling the incident based on the relevant factors (functional impact, information impact, recoverability effort, etc.)	
3.	Report the incident to the appropriate internal personnel and external organizations	
Containment, Eradication, and Recovery		
4.	Acquire, preserve, secure, and document evidence	10. Time from isolation to recovery 11. Recovery description that includes containment and timeline 12. Reflection on redundant recovery plan 13. Details on each stage of incident response
5.	Contain the incident	
6.	Eradicate the incident	
6.1	Identify and mitigate all vulnerabilities that were exploited	
6.2	Remove malware, inappropriate materials, and other components	
6.3	If more affected hosts are discovered (e.g., new malware infections), repeat the Detection and Analysis steps (1.1, 1.2) to identify all other affected hosts, then contain (5) and eradicate (6) the incident for them	
7.	Recover from the incident	
7.1	Return affected systems to an operationally ready state	

7.2	Confirm that the affected systems are functioning normally	
7.3	If necessary, implement additional monitoring to look for future related activity	
Post-Incident Activity		
8.	Create a follow-up report	14. Platform for sharing cyber threat 15. Structure data inputs for analytics 16. Control failure for incident 17. Add new or modify existing control to prevent incident 18. Gap in capabilities to manage cyber risk
9.	Hold a “lessons learned” meeting (mandatory for major incidents, optional otherwise)	

Table 5: Using NIST Incident Handling Checklist (Cichonski et al. [4]) to verify if the 18 Information Element

The description for each of the *Information Element* is shown in Table 6 and the specific data with its possible uses are also discussed. This work assumes that for a *Cyber Incident* Report to be complete, all 18 *Information Element* needs to be fulfilled. This work did not further explore the priority of importance of each *Information Element*. Further work is recommended in Chapter 6 on verifying the priority of importance of each *Information Element* for different purposes of *Cyber Incident Reporting*

No	*Information Element*	Description	Possible uses
1.	Incident description that includes the TTPs and timeline	Factual incident details that include but not limited to workflows, timeline, TTPs used in terms of access, vulnerabilities exploited, movement routes, tools used, what systems were target, exfiltration, and eradication method.	This is the “what”, “who”, “where”, “when”, and “how” of the incident. Understanding the adversary’s entire chain of attack can be used to work on defence to prevent future incidents.
2.	Impact description and timeline	Functionality in terms of current and future impact, Information in terms of confidentiality, integrity and availability. Recoverability in terms of size of incident and resources affected to determine resources in terms of time and cost required. Information regarding ransom payment should also be documented for cases involving ransomware	This is to report to stakeholders, especially management, for making decisions on immediate or future plans on budget and manpower.
3.	Time from attack to detection	Time difference between detection and successful adversary access to network so that amount of potential damage can be estimated	This is to assess the detection capability performance and sophistication of adversary’s attack.
4.	Time from detection to isolation	Time difference to assess capability to stop further damages to system	This is to assess the containment capability performance to reduce further impact.
5.	Time from isolation to recovery	Time difference to assess capability to continue business operations	This is to assess the continuity of operations to resume business requirements.
6.	Details on stakeholder reporting	What must be reported to whom, timeliness of this, and the approvals to obtain to proceed with plans.	This is to improve incident response plans.
7.	Investigation description and timeline	Details on how evidence, including compromised systems has been collected and preserved to meet applicable laws and regulations.	This is to comply with applicable laws and regulations.

8.	Recovery description that includes containment and timeline	Details on the resolution of issues that includes containment, eradication and recovery.	This is to understand the chain of events that occurred for recovery.
9.	Reflection on redundant recovery plans	Details on validation of effectiveness on existing recovery plans during actual incident.	This is to improve incident response plans.
10.	Details on each stage of incident response	Details on actions taken in Detection, Analysis, Containment, Eradication, Recovery and post incident activity.	This is to categorize specific actions in the full process of incident response framework in order to find any gaps between each stage of the framework.
11.	Platform for sharing cyber threat	Sharing of pre-approved details on approved platform for other organizations as early warning.	This applies to the entire eco-system of the sector as the inter-dependencies are tightly coupled.
12.	Structure data inputs for analytics	Format of report to allow tagging for easy export to other data structure forms	This is to derive further insights using advance analytic tools.
13.	Control failure for incident	Details of failed or lack of controls that resulted in the incident	This is the “why” of the incident. This will explain the actual vulnerability of the organization.
14.	Add new or modify existing control to prevent incident	Details of new or modification of controls to prevent similar incident	This is the follow up of the incident to prevent future similar incidents.
15.	Indicators of Compromise (IOC)	Forensic artifacts or remnants of an intrusion that can be identified on a host or network	This is to form signatures to identify threat actors or detect future incidents.
16.	Indicators of Attacks (IOA)	A series of actions that an adversary must conduct in order to succeed in the Cyber Incident	This is to form signatures to identify threat actors or detect future incidents.
17.	Indicators of Interest (IOI)	Information that acts as a supporting role in the identification and definition of an IOC	This is to form signatures to identify threat actors or detect future incidents.
18.	Gap in capabilities to manage cyber risk	Specific Cyber security capabilities that are lacking or absence that resulted in the incident	This is to address specific gaps in technical cyber security capabilities.

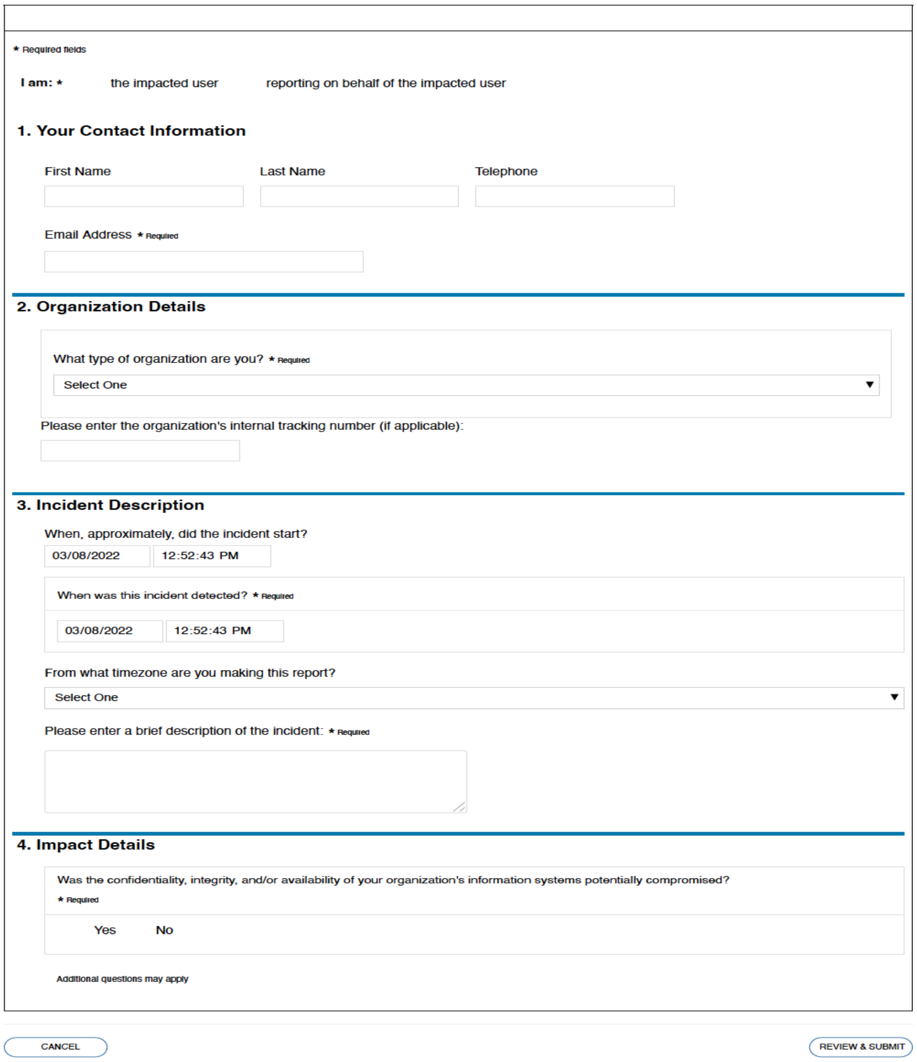
Table 6: Description of each Information Element and its possible use

3.3 Evaluation of Existing *Cyber Incident* Report Formats

In this section, we will use four *Cyber Incident* Report formats available to the public to compare with the baseline Cyber Incident Report format derived in Section 3.2. The four formats selected for evaluation were chosen due to their availability to public as two (CISA and FBI) of them were online web forms while the other two were images of the form. This research did not verify the authenticity and design considerations with the relevant owners of the formats and are using them for discussion only.

3.3.1 CISA *Cyber Incident* Report Format

The current format for a CISA Cyber Incident Report is shown in Figure 5. It compromises of four categories of information *(1) Contact Information, (2) Organization Details, (3) Incident Description* and *(4) Impact Details*.



* Required fields

I am: * the impacted user reporting on behalf of the impacted user

1. Your Contact Information

First Name

Last Name

Telephone

Email Address * Required

2. Organization Details

What type of organization are you? * Required

Select One ▼

Please enter the organization's internal tracking number (if applicable):

3. Incident Description

When, approximately, did the incident start?

03/08/2022 12:52:43 PM

When was this incident detected? * Required

03/08/2022 12:52:43 PM

From what timezone are you making this report?

Select One ▼

Please enter a brief description of the incident: * Required

4. Impact Details

Was the confidentiality, integrity, and/or availability of your organization's information systems potentially compromised?

* Required

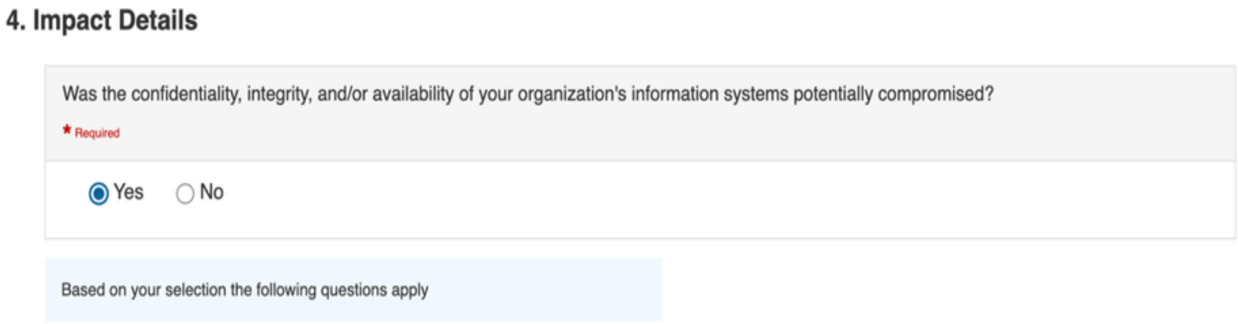
Yes No

Additional questions may apply

Figure 5: CISA Cyber Incident Report Format

While categories *(1) Contact Information* and *(2) Organization Details* are generic information necessary for the authorities to follow up with the reporter, the rest of the form focuses mostly on getting the impact details. Category *(3) Incident Description* component is a short section where there is a free text space as shown in Figure 5. There were no instructions given to guide the person reporting as to what level of details are required. The answer may vary widely with the person's level of experience. In addition, there is no option to select types of Incidents which suggest that there are no categories that CISA had preconceived or prioritized to be attended.

Furthermore, only upon indicating that the systems' CIA (Confidential, Integrity and Availability) was compromised as shown in Figure 6, more questions (Figure 7 to Figure 10) will apply about the incident. This seems to suggest that incident that did not lead to a breach should be reported in the free text space in Figure 6 before category *(4) Impact details*.



4. Impact Details

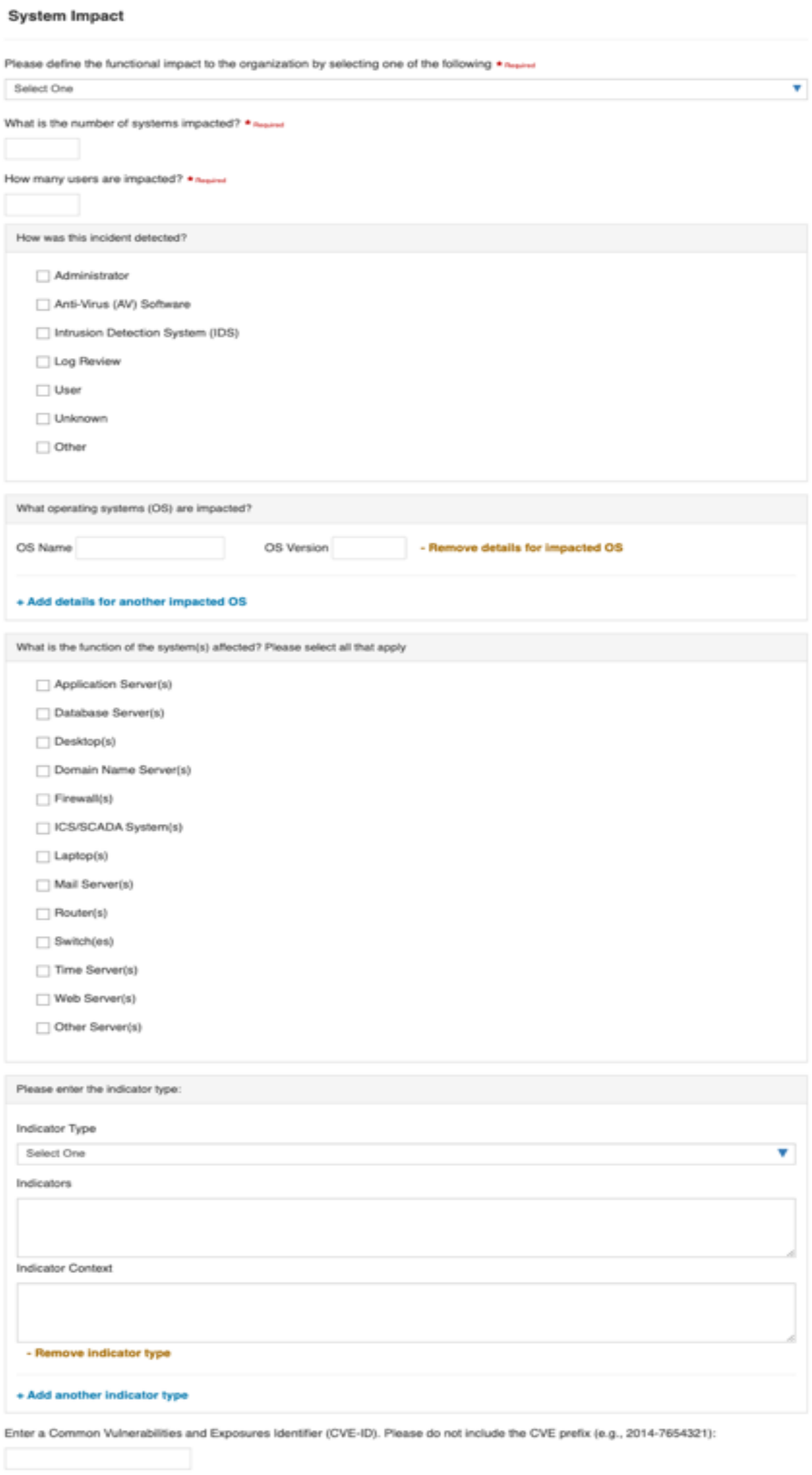
Was the confidentiality, integrity, and/or availability of your organization's information systems potentially compromised?

* Required

● Yes ○ No

Based on your selection the following questions apply

Figure 6: Only upon choosing "yes" option, more questions will apply



System Impact

Please define the functional impact to the organization by selecting one of the following • Required

Select One ▼

What is the number of systems impacted? • Required

How many users are impacted? • Required

How was this incident detected?

□ Administrator
□ Anti-Virus (AV) Software
□ Intrusion Detection System (IDS)
□ Log Review
□ User
□ Unknown
□ Other

What operating systems (OS) are impacted?

OS Name ____ OS Version ____ - Remove details for impacted OS

+ Add details for another impacted OS

What is the function of the system(s) affected? Please select all that apply

□ Application Server(s)
□ Database Server(s)
□ Desktop(s)
□ Domain Name Server(s)
□ Firewall(s)
□ ICS/SCADA System(s)
□ Laptop(s)
□ Mail Server(s)
□ Router(s)
□ Switch(es)
□ Time Server(s)
□ Web Server(s)
□ Other Server(s)

Please enter the indicator type:

Indicator Type

Select One ▼

Indicators

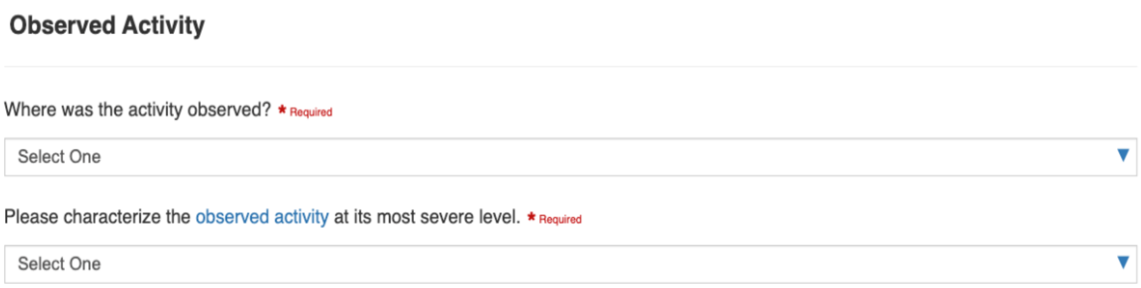
Indicator Context

- Remove indicator type

+ Add another indicator type

Enter a Common Vulnerabilities and Exposures Identifier (CVE-ID). Please do not include the CVE prefix (e.g., 2014-7654321):

Figure 7: More questions apply after indicating that CIA of System was compromise



Observed Activity

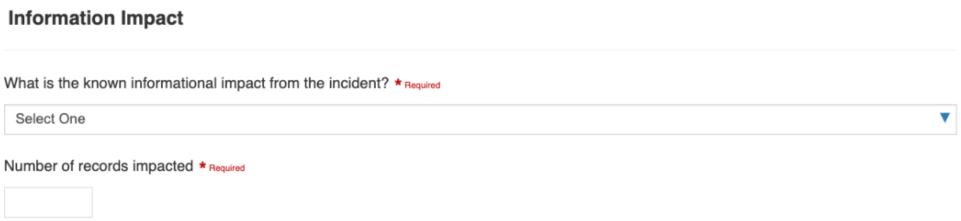
Where was the activity observed? * Required

Select One ▼

Please characterize the observed activity at its most severe level. * Required

Select One ▼

Figure 8: More questions on Observed Activity if system was compromised



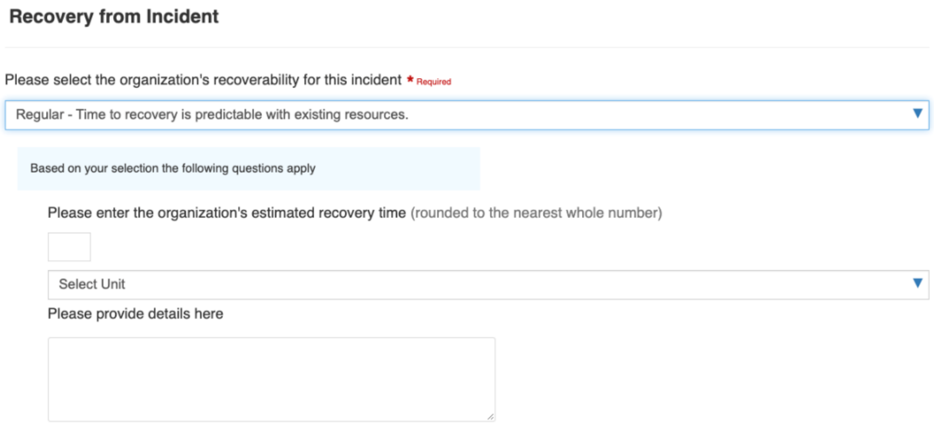
Information Impact

What is the known informational impact from the incident? * Required

Select One ▼

Number of records impacted * Required

Figure 9: More questions on Information Impact if system was compromised



Recovery from Incident

Please select the organization's recoverability for this incident * Required

Regular - Time to recovery is predictable with existing resources. ▼

Based on your selection the following questions apply

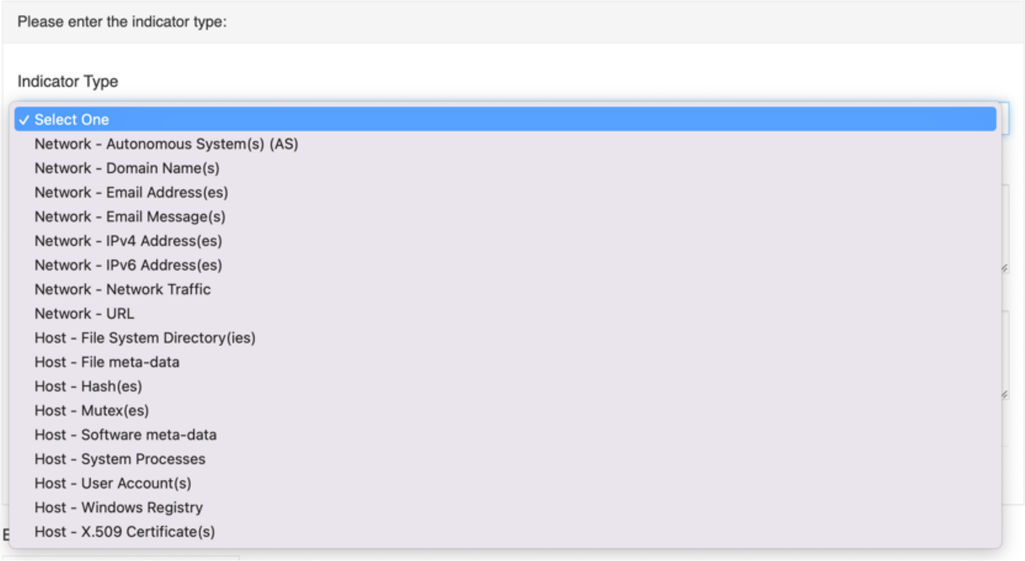
Please enter the organization's estimated recovery time (rounded to the nearest whole number)

Select Unit ▼

Please provide details here

Figure 10: More questions on Recovery if system was compromised

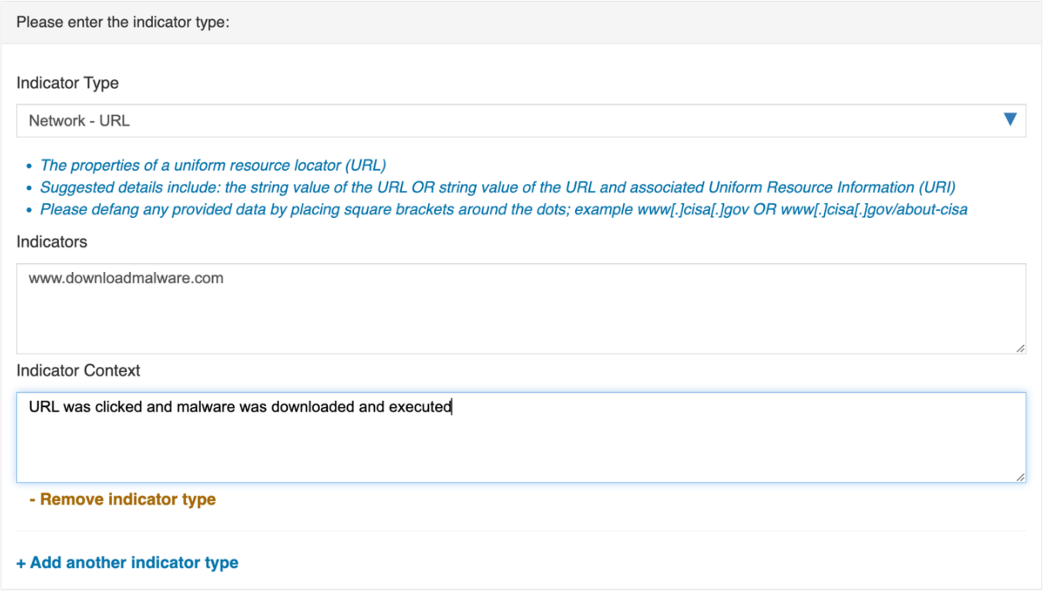
For the category *(4) Impact details*, the indicator type options are limited to the selections as seen in Figure 11. The indicator type options are specific components of the systems that are suspected to be causing the incident. An example of selecting indicator type as network URL is shown in Figure 12 to illustrate how to report such findings. This list should not be limited as there might be other unknown indicator type and the reporter would not be able to report accordingly.


Please enter the indicator type:

Indicator Type

✓ Select One
Network - Autonomous System(s) (AS)
Network - Domain Name(s)
Network - Email Address(es)
Network - Email Message(s)
Network - IPv4 Address(es)
Network - IPv6 Address(es)
Network - Network Traffic
Network - URL
Host - File System Directory(ies)
Host - File meta-data
Host - Hash(es)
Host - Mutex(es)
Host - Software meta-data
Host - System Processes
Host - User Account(s)
Host - Windows Registry
Host - X.509 Certificate(s)

Figure 11: Options for Indicator of Compromise


Please enter the indicator type:

Indicator Type: Network - URL

- *The properties of a uniform resource locator (URL)*
- *Suggested details include: the string value of the URL OR string value of the URL and associated Uniform Resource Information (URI)*
- *Please defang any provided data by placing square brackets around the dots; example www[.]cisa[.]gov OR www[.]cisa[.]gov/about-cisa*

Indicators: www.downloadmalware.com

Indicator Context: URL was clicked and malware was downloaded and executed

Figure 12: Example of selecting one option of the Indicator of Compromise

This format can be completed with minimum information so the person at the receiving end will likely need to follow up to gather more specific information for the incident. Some suggestions for improving the format are as follows:

1. Allow some options on the type of incident so that data can be categorize upfront. For example, Denial-of-Service (DOS) can be one option.
2. Allow the option of “Others” in the Indicator of Compromise
3. Allow more options for components in ICS/SCADA Systems as this seems to cater more towards IT Systems
4. Add more instructions to advise the level of details required for description of incident, especially for attempts that was successful defended.

5. Collect the failure of existing control measures if applicable to learn the reason of the Cyber Incident

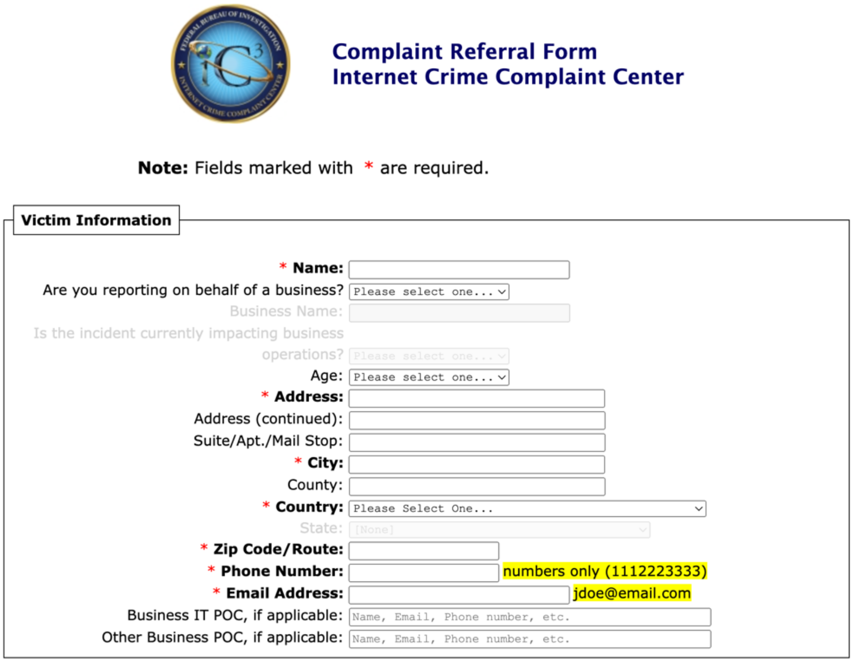
Comparing to the baseline Cyber Incident Report format, the score for CISA Cyber Incident Report Format is 5.0/18.0 and can be seen in Table 7.

No	Criteria	CISA Score	Comments
1.	Incident description that includes the TTPs and timeline	0.5	No mention of TTP
2.	Impact description and timeline	0.5	No mention of timeline
3.	Time from attack to detection	1	
4.	Time from detection to isolation	0	
5.	Time from isolation to recovery	0	
6.	Details on stakeholder reporting	0	
7.	Investigation description and timeline	0.5	Limited options
8.	Recovery description that includes containment and timeline	0.5	Generic options
9.	Reflection on redundant recovery plans	0	
10.	Details on each stage of incident response	0	
11.	Platform for sharing cyber threat	0	
12.	Structure data inputs for analytics	0.5	Web form that is structured
13.	Control failure for incident	0	
14.	Add new or modify existing control to prevent incident	0	
15.	Indicators of Compromise (IOC)	0.5	Generic mention of indicator
16.	Indicators of Attacks (IOA)	0.5	
17.	Indicators of Interest (IOI)	0.5	
18.	Gap in capabilities to manage cyber risk	0	
	Total Score	5.0/18	

Table 7: Score for Cyber Incident Report – CISA

3.3.2 FBI Cyber Incident Report Format

A format of FBI Cyber Incident Report is shown in Figure 9 (A to G). It compromises of 6 information categories that are *(1) Victim Information, (2) Financial Transaction (s), (3) Description of Incident, (4) Information about the subject who victimized you, (5) Other information* and *(6) Who filed the complaint?.*



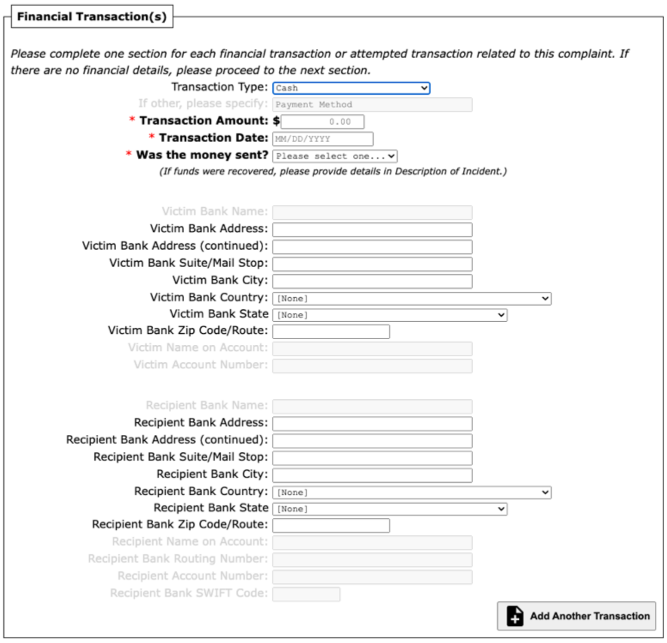
Complaint Referral Form
Internet Crime Complaint Center

Note: Fields marked with * are required.

Victim Information

* **Name:**
Are you reporting on behalf of a business? Please select one...
Business Name:
Is the incident currently impacting business operations? Please select one...
Age: Please select one...
* **Address:**
Address (continued):
Suite/Apt./Mail Stop:
* **City:**
County:
* **Country:** Please Select One...
State: [None]
* **Zip Code/Route:**
* **Phone Number:** numbers only (1112223333)
* **Email Address:** jdoe@email.com
Business IT POC, if applicable: Name, Email, Phone number, etc.
Other Business POC, if applicable: Name, Email, Phone number, etc.

Figure 13: FBI Cyber Incident Report Form – Victim Information



Financial Transaction(s)

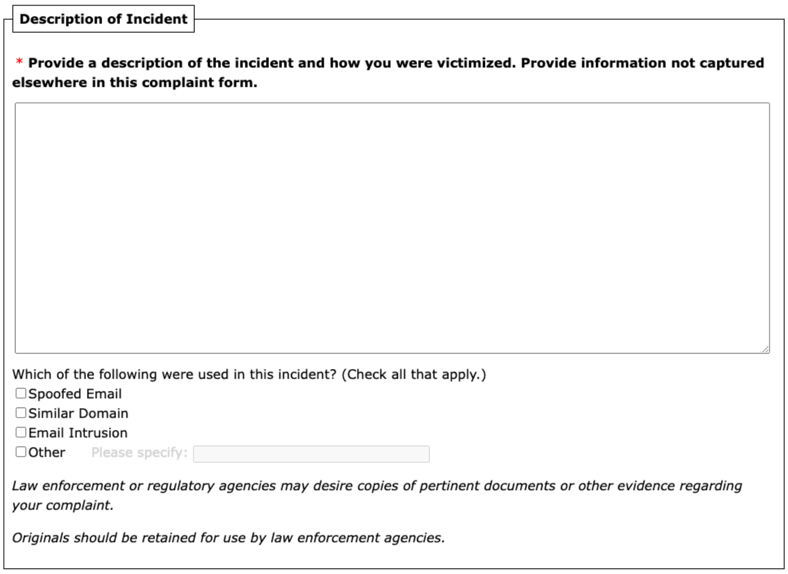
Please complete one section for each financial transaction or attempted transaction related to this complaint. If there are no financial details, please proceed to the next section.

Transaction Type: Cash
If other, please specify: Payment Method
* **Transaction Amount: $** 0.00
* **Transaction Date:** MM/DD/YYYY
* **Was the money sent?** Please select one...
(If funds were recovered, please provide details in Description of Incident.)

Victim Bank Name:
Victim Bank Address:
Victim Bank Address (continued):
Victim Bank Suite/Mail Stop:
Victim Bank City:
Victim Bank Country: [None]
Victim Bank State [None]
Victim Bank Zip Code/Route:
Victim Name on Account:
Victim Account Number:

Recipient Bank Name:
Recipient Bank Address:
Recipient Bank Address (continued):
Recipient Bank Suite/Mail Stop:
Recipient Bank City:
Recipient Bank Country: [None]
Recipient Bank State [None]
Recipient Bank Zip Code/Route:
Recipient Name on Account:
Recipient Bank Routing Number:
Recipient Account Number:
Recipient Bank SWIFT Code:

Figure 14: FBI Cyber Incident Report Form – Financial Transaction (s)



Description of Incident

*** Provide a description of the incident and how you were victimized. Provide information not captured elsewhere in this complaint form.**

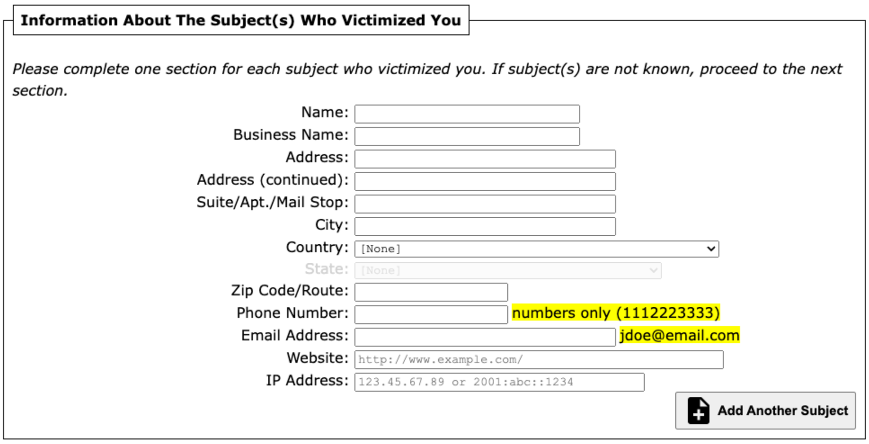
Which of the following were used in this incident? (Check all that apply.)

□ Spoofed Email
□ Similar Domain
□ Email Intrusion
□ Other Please specify:

Law enforcement or regulatory agencies may desire copies of pertinent documents or other evidence regarding your complaint.

Originals should be retained for use by law enforcement agencies.

Figure 15: FBI Cyber Incident Report Form – Description of Incident

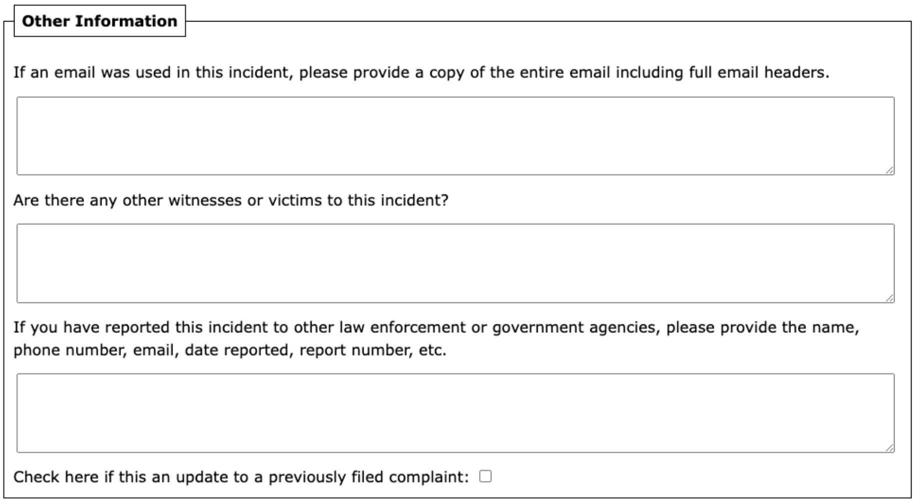


Information About The Subject(s) Who Victimized You

Please complete one section for each subject who victimized you. If subject(s) are not known, proceed to the next section.

Name:
Business Name:
Address:
Address (continued):
Suite/Apt./Mail Stop:
City:
Country: [None]
State: [None]
Zip Code/Route:
Phone Number: numbers only (1112223333)
Email Address: jdoe@email.com
Website: http://www.example.com/
IP Address: 123.45.67.89 or 2001:abc::1234

Figure 16 : FBI Cyber Incident Report Form – Information about the Perpetrator



Other Information

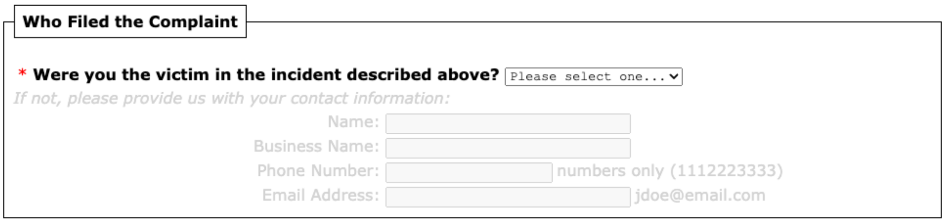
If an email was used in this incident, please provide a copy of the entire email including full email headers.

Are there any other witnesses or victims to this incident?

If you have reported this incident to other law enforcement or government agencies, please provide the name, phone number, email, date reported, report number, etc.

Check here if this an update to a previously filed complaint: □

Figure 17: Information on available evidences



Who Filed the Complaint

* **Were you the victim in the incident described above?** Please select one...

If not, please provide us with your contact information:

Name:

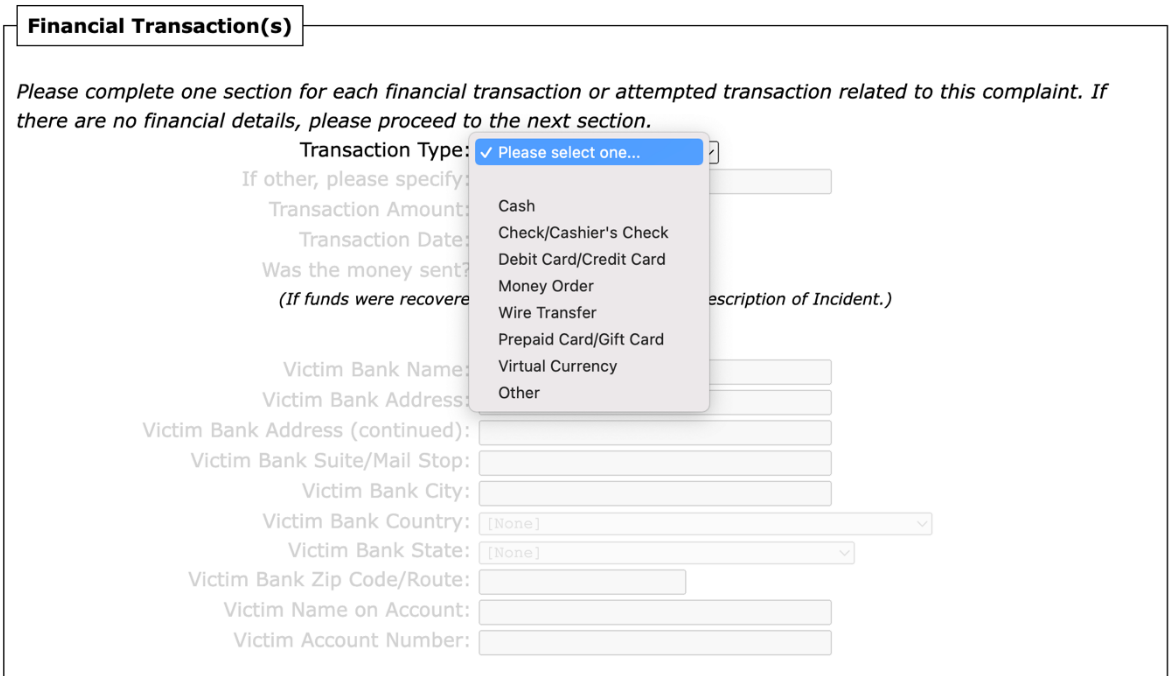
Business Name:

Phone Number: numbers only (1112223333)

Email Address: jdoe@email.com

Figure 18: Information on the reporter

This format prioritizes *(2) Financial transaction* over the *(3) Description of Incident* seems to suggest that the design is targeted for reporting cyber scams as shown in Figure 15 and Figure 16. Figure 19 further shows that there are many different types of currency for selection, and it will be suitable to report incidents involving ransom such as ransomware.



Financial Transaction(s)

Please complete one section for each financial transaction or attempted transaction related to this complaint. If there are no financial details, please proceed to the next section.

Transaction Type: ✓ Please select one...

If other, please specify:

Transaction Amount:

Transaction Date:

Was the money sent?

(If funds were recovere escription of Incident.)

Victim Bank Name:

Victim Bank Address:

Victim Bank Address (continued):

Victim Bank Suite/Mail Stop:

Victim Bank City:

Victim Bank Country: [None]

Victim Bank State: [None]

Victim Bank Zip Code/Route:

Victim Name on Account:

Victim Account Number:

Figure 19: Options for selecting Transaction Type

As this is a web form, the inputs can be easily consolidated for further analysis as they can be tagged into a data structure. Other than this, technical details about the incident are self-initiated by the reporter for filling in as there were no guidance on the level of details required. Some suggestions for the format as follows:

1. Allow some options on type of Incidents for ease of processing
2. Allow options to indicate if incident is an attempt or have occurred as the option on "Was the money sent" (Figure 15) is not clear in this indication
3. Allow the option for amount of ransom demanded to compare with the actual amount of ransom paid if applicable

4. Allow attachment of files like screenshots to be submitted to support the case

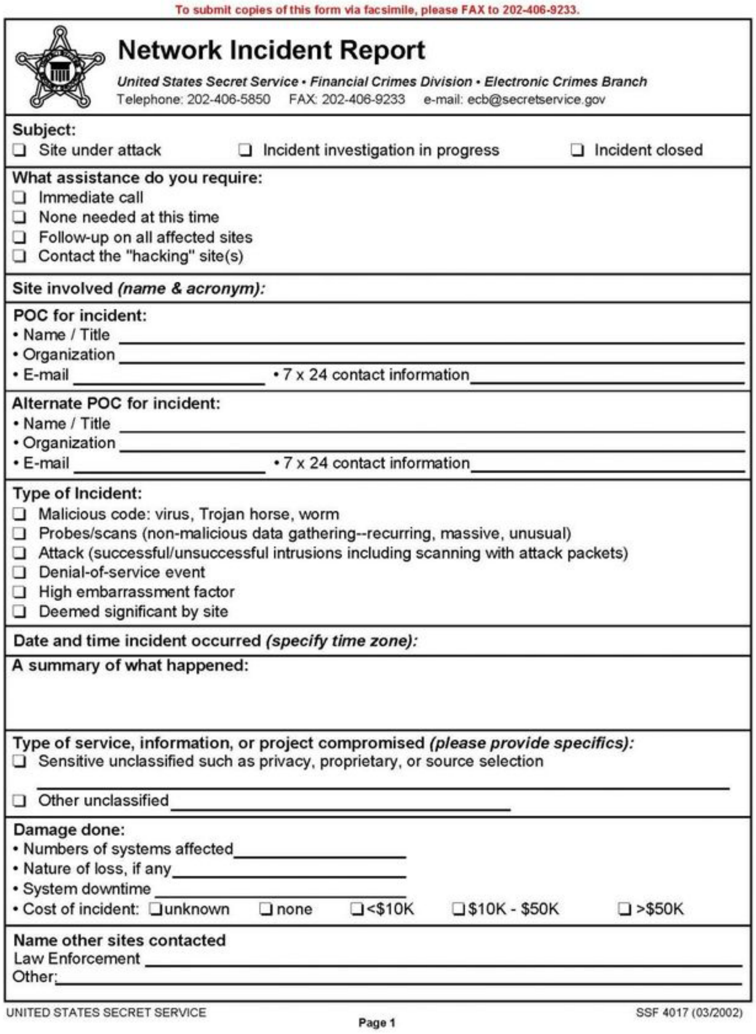
Comparing to the baseline Cyber Incident Report format, the score for FBI Cyber Incident Report Format is 3.0/18.0 as shown in Table 8.

No	Criteria	FBI Score	Comments
1.	Incident description that includes the TTPs and timeline	0.5	No mention of TTP
2.	Impact description and timeline	0.5	More suited for individual Cyber Incidents than organization
3.	Time from attack to detection	0	
4.	Time from detection to isolation	0	
5.	Time from isolation to recovery	0	
6.	Details on stakeholder reporting	0	
7.	Investigation description and timeline	0	No mention for investigation details.
8.	Recovery description that includes containment and timeline	0.5	
9.	Reflection on redundant recovery plans	0	
10.	Details on each stage of incident response	0	
11.	Platform for sharing cyber threat	0	
12.	Structure data inputs for analytics	0.5	Web form that is structured
13.	Control failure for incident	0	
14.	Add new or modify existing control to prevent incident	0	
15.	Indicators of Compromise (IOC)	0.5	Generic mention of indicator like spoofed email, email intrusion, etc
16.	Indicators of Attacks (IOA)	0.5	
17.	Indicators of Interest (IOI)	0.5	
18.	Gap in capabilities to manage cyber risk	0	
	Total Score	3.0/18	Not suitable to be adopted

Table 8: Score for Cyber Incident Report - FBI

3.3.3 United States Secret Service Cyber Incident Report Format

A format of the United States Secret Service Cyber Incident Report is shown in Figure 20. The form consists of many short questions that seems to suggest it is design for a quick report and will likely require follow up for further investigation (e.g. Forensic Investigation Report). The type of Incident is clearly indicated and it was noted that this form indicated “non-malicious” scans as a type of incident to be reported. In practice, there could be hundreds or thousands of such scans which could be tedious for the incident response team to manage.



To submit copies of this form via facsimile, please FAX to 202-406-9233.

Network Incident Report

United States Secret Service • Financial Crimes Division • Electronic Crimes Branch
Telephone: 202-406-5850 FAX: 202-406-9233 e-mail: ecb@secretservice.gov

Subject:
❑ Site under attack ❑ Incident investigation in progress ❑ Incident closed

What assistance do you require:
❑ Immediate call
❑ None needed at this time
❑ Follow-up on all affected sites
❑ Contact the "hacking" site(s)

Site involved *(name & acronym):*

POC for incident:
• Name / Title ______
• Organization ______
• E-mail ______ • 7 x 24 contact information______

Alternate POC for incident:
• Name / Title ______
• Organization ______
• E-mail ______ • 7 x 24 contact information______

Type of Incident:
❑ Malicious code: virus, Trojan horse, worm
❑ Probes/scans (non-malicious data gathering--recurring, massive, unusual)
❑ Attack (successful/unsuccessful intrusions including scanning with attack packets)
❑ Denial-of-service event
❑ High embarrassment factor
❑ Deemed significant by site

Date and time incident occurred *(specify time zone):*

A summary of what happened:

Type of service, information, or project compromised *(please provide specifics):*
❑ Sensitive unclassified such as privacy, proprietary, or source selection
______
❑ Other unclassified______

Damage done:
• Numbers of systems affected______
• Nature of loss, if any______
• System downtime ______
• Cost of incident: ❑unknown ❑ none ❑<$10K ❑$10K - $50K ❑ >$50K

Name other sites contacted
Law Enforcement ______
Other:______

UNITED STATES SECRET SERVICE Page 1 SSF 4017 (03/2002)

Figure 20: US Secret Service Cyber Incident Report Format

Some suggestions for the format:

1. Allow free text option to indicate type of incident for ease of process if reported incident is not one of the available choice

2. Collect the date and time of detection as the actual timeline of incident investigation may still be in progress
3. Collect the failure of control measures to learn the reason of incident
4. Collect the detail on recovery measures if the Cyber Incident is closed

Comparing with the baseline Cyber Incident Report, the score for US Secret Service Cyber Incident Report Format is 3.0/18.0 shown in Table 7.

No	Criteria	APPA Score	Comments
1.	Incident description that includes the TTPs and timeline	0.5	No mention of TTP
2.	Impact description and timeline	0.5	No mention of timeline
3.	Time from attack to detection	0.5	Generic mention of incident
4.	Time from detection to isolation	0	
5.	Time from isolation to recovery	0	
6.	Details on stakeholder reporting	0	
7.	Investigation description and timeline	0	
8.	Recovery description that includes containment and timeline	0	
9.	Reflection on redundant recovery plans	0	
10.	Details on each stage of incident response	0	
11.	Platform for sharing cyber threat	0	
12.	Structure data inputs for analytics	0	
13.	Control failure for incident	0	
14.	Add new or modify existing control to prevent incident	0	
15.	Indicators of Compromise (IOC)	0.5	Generic mention of attack vectors
16.	Indicators of Attacks (IOA)	0.5	
17.	Indicators of Interest (IOI)	0.5	
18.	Gap in capabilities to manage cyber risk	0	
	Total Score	3.0/18	Not suitable to be adopted

Table 9: Score for Cyber Incident Report - US Secret Service

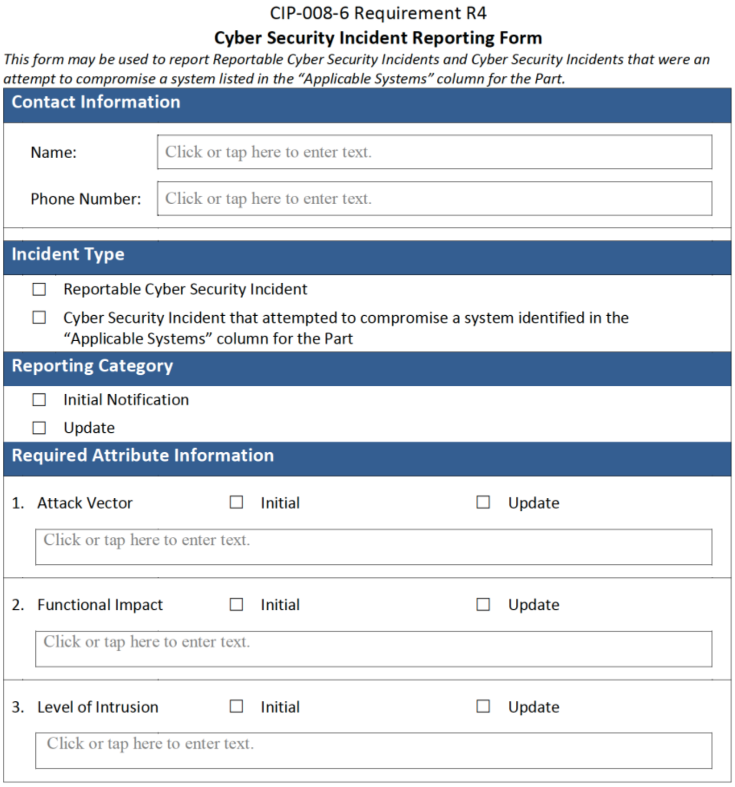
3.3.4 North American Electric Reliability Corporation (NERC) Cyber Incident Report Format

The NERC Cyber Incident Report Format is as shown in Figure 21. It shows a rather simple form that asks very broad questions with information categories: *(1) contact information, (2) Incident Type, (3) Reporting Category* and *(4) Required Attribute Information*. This format comes with specific instructions, for example, of a reporting form as shown in Figure 22. In the category *(2) Incident type*, this format differentiates attempts from actual incidents as an option to be reported. This seems to suggest that the other option for category *(2) Incident type* would require a breach to qualify.

Some suggestions for the format:

1. Allow some options on types of incidents to ease processing
2. Need to define difference between attempts of incidents and incidents that have occurred
3. Add some options to each attribute information to help ease processing
4. Indicate contact details of authority to report the Cyber Incident
5. Collect information on failure of control measures to learn from the Cyber Incident

Comparing to the baseline Cyber Incident Report, the score for NERC Cyber Incident Report Format 3.5/18.0 as shown in Table 8.



CIP-008-6 Requirement R4

Cyber Security Incident Reporting Form

This form may be used to report Reportable Cyber Security Incidents and Cyber Security Incidents that were an attempt to compromise a system listed in the "Applicable Systems" column for the Part.

Contact Information

Name: Click or tap here to enter text.

Phone Number: Click or tap here to enter text.

Incident Type

☐ Reportable Cyber Security Incident

☐ Cyber Security Incident that attempted to compromise a system identified in the "Applicable Systems" column for the Part

Reporting Category

☐ Initial Notification

☐ Update

Required Attribute Information

1. Attack Vector ☐ Initial ☐ Update

Click or tap here to enter text.

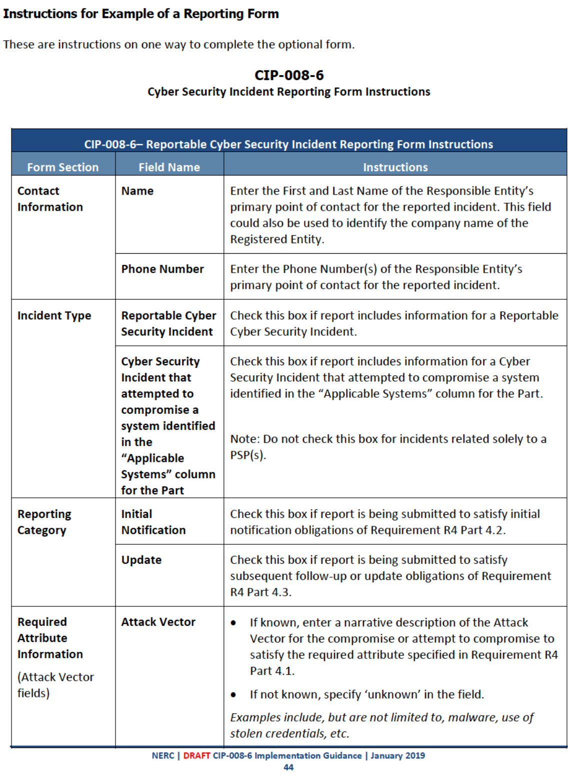
2. Functional Impact ☐ Initial ☐ Update

Click or tap here to enter text.

3. Level of Intrusion ☐ Initial ☐ Update

Click or tap here to enter text.

Figure 21: NERC Cyber Incident Report Format



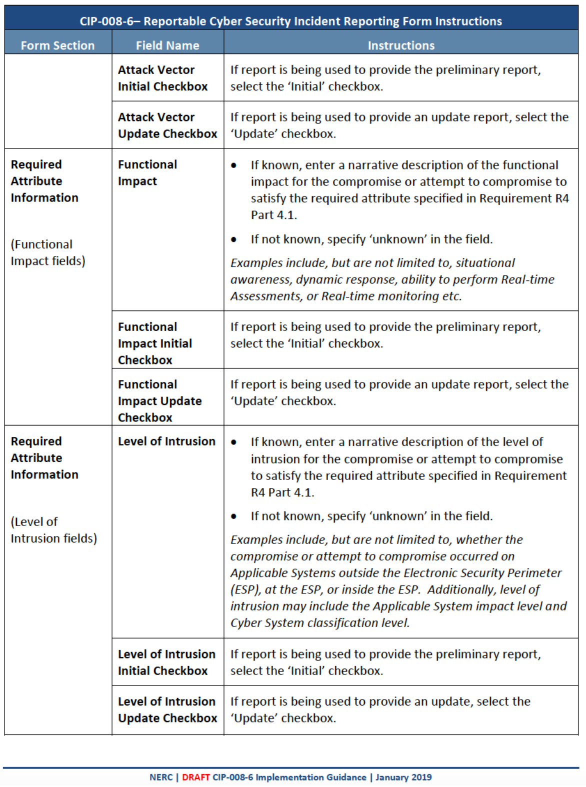
Instructions for Example of a Reporting Form

These are instructions on one way to complete the optional form.

CIP-008-6
Cyber Security Incident Reporting Form Instructions

CIP-008-6– Reportable Cyber Security Incident Reporting Form Instructions		
Form Section	**Field Name**	**Instructions**
Contact Information	**Name**	Enter the First and Last Name of the Responsible Entity's primary point of contact for the reported incident. This field could also be used to identify the company name of the Registered Entity.
	Phone Number	Enter the Phone Number(s) of the Responsible Entity's primary point of contact for the reported incident.
Incident Type	**Reportable Cyber Security Incident**	Check this box if report includes information for a Reportable Cyber Security Incident.
	Cyber Security Incident that attempted to compromise a system identified in the "Applicable Systems" column for the Part	Check this box if report includes information for a Cyber Security Incident that attempted to compromise a system identified in the "Applicable Systems" column for the Part. Note: Do not check this box for incidents related solely to a PSP(s).
Reporting Category	**Initial Notification**	Check this box if report is being submitted to satisfy initial notification obligations of Requirement R4 Part 4.2.
	Update	Check this box if report is being submitted to satisfy subsequent follow-up or update obligations of Requirement R4 Part 4.3.
Required Attribute Information (Attack Vector fields)	**Attack Vector**	• If known, enter a narrative description of the Attack Vector for the compromise or attempt to compromise to satisfy the required attribute specified in Requirement R4 Part 4.1. • If not known, specify 'unknown' in the field. *Examples include, but are not limited to, malware, use of stolen credentials, etc.*

NERC | DRAFT CIP-008-6 Implementation Guidance | January 2019
44



CIP-008-6– Reportable Cyber Security Incident Reporting Form Instructions		
Form Section	**Field Name**	**Instructions**
	Attack Vector Initial Checkbox	If report is being used to provide the preliminary report, select the 'Initial' checkbox.
	Attack Vector Update Checkbox	If report is being used to provide an update report, select the 'Update' checkbox.
Required Attribute Information (Functional Impact fields)	**Functional Impact**	• If known, enter a narrative description of the functional impact for the compromise or attempt to compromise to satisfy the required attribute specified in Requirement R4 Part 4.1. • If not known, specify 'unknown' in the field. *Examples include, but are not limited to, situational awareness, dynamic response, ability to perform Real-time Assessments, or Real-time monitoring etc.*
	Functional Impact Initial Checkbox	If report is being used to provide the preliminary report, select the 'Initial' checkbox.
	Functional Impact Update Checkbox	If report is being used to provide an update report, select the 'Update' checkbox.
Required Attribute Information (Level of Intrusion fields)	**Level of Intrusion**	• If known, enter a narrative description of the level of intrusion for the compromise or attempt to compromise to satisfy the required attribute specified in Requirement R4 Part 4.1. • If not known, specify 'unknown' in the field. *Examples include, but are not limited to, whether the compromise or attempt to compromise occurred on Applicable Systems outside the Electronic Security Perimeter (ESP), at the ESP, or inside the ESP. Additionally, level of intrusion may include the Applicable System impact level and Cyber System classification level.*
	Level of Intrusion Initial Checkbox	If report is being used to provide the preliminary report, select the 'Initial' checkbox.
	Level of Intrusion Update Checkbox	If report is being used to provide an update, select the 'Update' checkbox.

NERC | DRAFT CIP-008-6 Implementation Guidance | January 2019

Figure 22: Instructions for Example of a Reporting Form

No	Criteria	NERC Score	Comments
1.	Incident description that includes the TTPs and timeline	0.5	No mention of TTP
2.	Impact description and timeline	0.5	No mention of timeline
3.	Time from attack to detection	0	
4.	Time from detection to isolation	0	
5.	Time from isolation to recovery	0	
6.	Details on stakeholder reporting	0	
7.	Investigation description and timeline	0.5	Generic question of attack vector
8.	Recovery description that includes containment and timeline	0	
9.	Reflection on redundant recovery plans	0	
10.	Details on each stage of incident response	0	
11.	Platform for sharing cyber threat	0	
12.	Structure data inputs for analytics	0.5	Web form that is structured
13.	Control failure for incident	0	

14.	Add new or modify existing control to prevent incident	0	
15.	Indicators of Compromise (IOC)	0.5	Generic mention of attack vectors
16.	Indicators of Attacks (IOA)	0.5	
17.	Indicators of Interest (IOI)	0.5	
18.	Gap in capabilities to manage cyber risk	0	
	Total Score	3.5/18	Not suitable to be adopted

Table 10: Score for Cyber Incident Report – NERC

3.4 Summary

In this chapter, a baseline of Cyber Incident Report was derived from the NIST guiding principles on Computer Security Incident Handling. This baseline was used to compare with four other *Cyber Incident* Report formats that were available to the public. The evaluated resulted in some suggestions in improving the four formats and also showed that all four formats do not have all 18 Information Elements as compared to the baseline Cyber Incident Report format. This conclusion further emphasize that Information required depended on the purpose of the Cyber Incident Report (as discussed in Section 1.4).

These formats do not seem to be structured to facilitate learning and preventing similar incidents as there were no required information on failure of control measures. It is also observed that there is a need for a structure to categorize the *Cyber Incident* description to facilitate the sharing of information with others easily for threat intelligence that will benefit the overall ICS community. For Chapter 4, the MITRE ATT&CK Framework for ICS will be introduced so that it can be used for Cyber Incident Report in Chapter 5.

4. MITRE ATT&CK Framework for ICS

This chapter provides the overview on MITRE ATT&CK Framework that covers its background, possible use cases, overview of the entire MITRE ATT&CK Framework structure and the types of information it can facilitate in sharing. By understanding these attributions of the MITRE ATT&CK Framework, this research can proceed to evaluate using it in a Cyber Incident Report.

4.1 Introduction to MITRE ATT&CK

MITRE ATT&CK (Adversary Tactics, Techniques & Common Knowledge) is a globally-accessible knowledge base of adversary tactics and techniques based on real-world observations. The ATT&CK knowledge base is used as a foundation for the development of specific threat models and methodologies in the private sector, in government, and in the cybersecurity product and service community. ATT&CK provides a common taxonomy for both offense and defence, and has become a useful conceptual tool across many cyber security disciplines to convey threat intelligence, perform testing through red teaming or adversary emulation, and improve network and system defences against intrusions (Storm et Al. 2018 [24]).

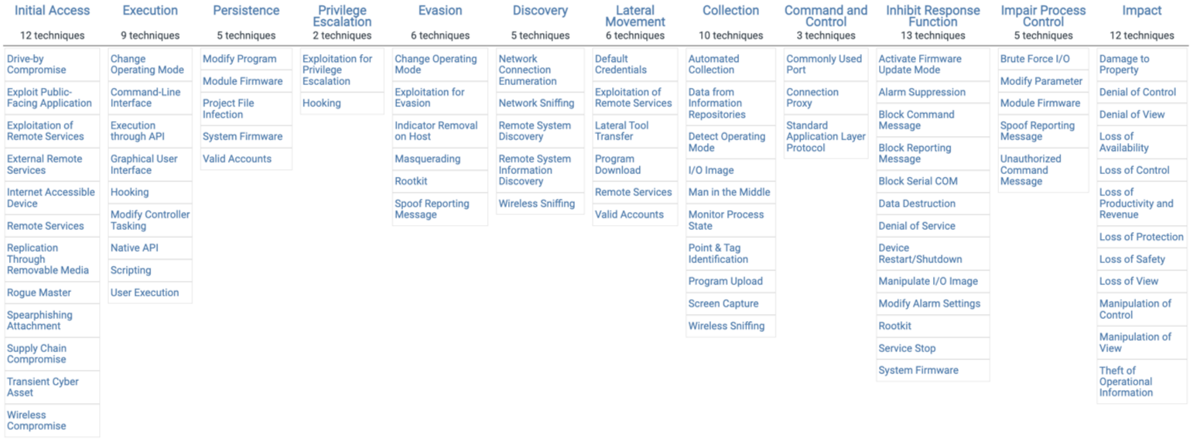
MITRE ATT&CK is a curated knowledge base and model for cyber adversary behaviour, reflecting the various phases of an adversary's attack lifecycle and the platforms they are known to target. ATT&CK focuses on how external adversaries compromise and operate within computer information networks. It originated out of a project to document and categorize post compromise adversary tactics, techniques and procedures (TTPs) against Microsoft Windows systems to improve detection of malicious behaviour. It has since grown to include Linux and macOS, and has expanded to cover behaviour leading up to the compromise of an environment, as well as technology-focused domains like mobile devices, cloud-based systems, and ICSs (Storm et Al. 2018 [24]).

4.2 MITRE ATTACK Framework Use Cases

One specific MITRE ATTA&CK Framework use case will be in Cyber Threat Intelligence Enrichment. Cyber threat intelligence covers knowledge of cyber threats and threat actor groups that impact cybersecurity. It includes information about malware, tools, TTPs, tradecraft, behavior, mitigation methods and other indicators that are associated with threats. ATT&CK is useful for understanding and documenting adversary group profiles from a behavioral perspective that is agnostic of the tools the group may use. Analysts and defenders can better understand common behaviors across many groups and more effectively map defenses to them and use common mitigation methods to detect and deter similar techniques even though the specific procedures are different.

Understanding how multiple groups use the same technique behavior allows analysts to focus on impactful defenses that span many types of threats. The structured format of ATT&CK can add value to threat reporting by categorizing behavior beyond standard indicators.

4.3 Overview of MITRE ATT&CK ICS Matrix



Initial Access	Execution	Persistence	Privilege Escalation	Evasion	Discovery	Lateral Movement	Collection	Command and Control	Inhibit Response Function	Impair Process Control	Impact
12 techniques	9 techniques	5 techniques	2 techniques	6 techniques	5 techniques	6 techniques	10 techniques	3 techniques	13 techniques	5 techniques	12 techniques
Drive-by Compromise	Change Operating Mode	Modify Program	Exploitation for Privilege Escalation	Change Operating Mode	Network Connection Enumeration	Default Credentials	Automated Collection	Commonly Used Port	Activate Firmware Update Mode	Brute Force I/O	Damage to Property
Exploit Public-Facing Application	Command-Line Interface	Module Firmware	Hooking	Exploitation for Evasion	Network Sniffing	Exploitation of Remote Services	Data from Information Repositories	Connection Proxy	Alarm Suppression	Modify Parameter	Denial of Control
Exploitation of Remote Services	Execution through API	Project File Infection		Indicator Removal on Host	Remote System Discovery	Lateral Tool Transfer	Detect Operating Mode	Standard Application Layer Protocol	Block Command Message	Module Firmware	Denial of View
External Remote Services	Graphical User Interface	System Firmware		Masquerading	Remote System Information Discovery	Program Download	I/O Image		Block Reporting Message	Spoof Reporting Message	Loss of Availability
Internet Accessible Device	Hooking	Valid Accounts		Rootkit	Wireless Sniffing	Remote Services	Man in the Middle		Block Serial COM	Unauthorized Command Message	Loss of Control
Remote Services	Modify Controller Tasking			Spoof Reporting Message		Valid Accounts	Monitor Process State		Data Destruction		Loss of Productivity and Revenue
Replication Through Removable Media	Native API						Point & Tag Identification		Denial of Service		Loss of Protection
Rogue Master	Scripting						Program Upload		Device Restart/Shutdown		Loss of Safety
Spearphishing Attachment	User Execution						Screen Capture		Manipulate I/O Image		Loss of View
Supply Chain Compromise							Wireless Sniffing		Modify Alarm Settings		Manipulation of Control
Transient Cyber Asset									Rootkit		Manipulation of View
Wireless Compromise									Service Stop		Theft of Operational Information
									System Firmware		

Figure 23: The MITRE ATTA&CK ICS Matrix

The overview of the MITRE ATT&CK for ICS matrix is shown in Figure 23 There are 12 categories of tactics and 78 techniques as at the time of writing. The MITRE ATT&CK for ICS is a collection of publicly observed and ICS-focused TTPs. These categories cover all the TTPs known to be used on ICS and it helps security operations teams easily deduce an adversary's intention for individual actions and understand how those actions relate to specific classes of defenses.

ICS Tactics represent the "what" of an ATT&CK technique or sub-technique. It is the adversary's tactical goal and the reason for performing an action. For example, an adversary may want to gain (TA0108) Initial Access to targeted victims through (T0817) Drive-by Compromise Technique by setting up compromised websites to conduct waterhole attack on the victims such as Procedure (G1000) codename ALLANITE. The specific details for each ICS Tactics are shown in Table 9 including the MITRE ATT&CK Framework unique ID, tactic name and description.

ID	Name	Description of intention
TA0108	Initial Access	The adversary is trying to get into your ICS environment.
TA0104	Execution	The adversary is trying to run code or manipulate system functions, parameters, and data in an unauthorized way.
TA0110	Persistence	The adversary is trying to maintain their foothold in your ICS environment.

TA0111	Privilege Escalation	The adversary is trying to gain higher-level permissions.
		Privilege Escalation consists of techniques that adversaries use to gain higher-level permissions on a system or network. Adversaries can often enter and explore a network with unprivileged access but require elevated permissions to follow through on their objectives. Common approaches are to take advantage of system weaknesses, misconfigurations, and vulnerabilities.
TA0103	Evasion	The adversary is trying to avoid security defenses.
TA0102	Discovery	The adversary is locating information to assess and identify their targets in your environment.
TA0109	Lateral Movement	The adversary is trying to move through your ICS environment.
TA0100	Collection	The adversary is trying to gather data of interest and domain knowledge on your ICS environment to inform their goal.
TA0101	Command and Control	The adversary is trying to communicate with and control compromised systems, controllers, and platforms with access to your ICS environment.
TA0107	Inhibit Response Function	The adversary is trying to prevent your safety, protection, quality assurance, and operator intervention functions from responding to a failure, hazard, or unsafe state.
TA0106	Impair Process Control	The adversary is trying to manipulate, disable, or damage physical control processes.
TA0105	Impact	The adversary is trying to manipulate, interrupt, or destroy your ICS systems, data, and their surrounding environment.

Table 11: MITRE ATT&CK ICS Tactics (Source: MITRE ATT&CK Framework - https://attack.mitre.org/tactics/ics/)

4.4 Types of Information Sharing

MITRE ATT&CK team encourages information sharing to enrich their database of TTPs sighted in the entire cybersecurity community. This information sharing is essential as data are actually operational in real environment and not hypothetical like proof of concepts (Storm et Al. 2018 [24]). This is useful for Cyber Incident reporting as it acts as platform for sharing cyber intelligence. There are 3 main types of information sharing with ATT&CK team as follows:

1. **Direct sighting of a technique**

   This type of information shows actual sightings of techniques being executed in the course of an attack. In other words, during an event investigation, data is collected which shows that one or more ATT&CK techniques were actually used by the adversary on (or targeted at) the victim infrastructure. Direct sightings of techniques are the most valuable type of sighting because they tell you, at a ground-truth level, that the adversary relied on a specific technique to carry out an attack.

2. **Direct sighting of malicious software**

In some cases, a technique might not be directly observed (or even be observable given sensing capability) but the presence of a piece of malicious software on the machine can give a strong hint that it was used. In other cases, software to carry out a technique might be blocked at the perimeter – in those cases, it indicates that the adversary might have wanted to use a certain technique but wasn't able to. Note that direct software sightings are most useful for software already contained in ATT&CK that directly enables one or more ATT&CK techniques.

3. **Indirect sightings of malicious software**

In other cases, threat intelligence platforms or ISACs might have data feeds that indirectly demonstrate the fact that a piece of software is being used, without directly observing it. Note that, as above, indirect software sightings are most useful for software already contained in ATT&CK that directly enables one or more ATT&CK techniques. *For example:* A file hash for mimikatz.exe shared to an ISAC or threat intel platform would be an indirect sighting of mimikatz.exe. As with a direct sighting of malware, this does provide some indication (though weaker) that an adversary was interested in performing credential access. (Source: MITRE ATT&CK - https://attack.mitre.org/resources/sightings/)

4.5 SUMMARY

In this chapter, the MITRE ATT&CK Framework was introduced with its background, possible use cases, overview on the relevant ICS Matrix and the types of information sharing. With its rich database of TTPs, MITRE ATT&CK Framework seems to be suitable as a structure for reporting Cyber Incident in terms the description of incident. It can also be used for cyber defenders in detecting and mitigating similar TTPs. It is also noted that there are some efforts in learning required to be able to use MITRE ATT&CK Framework to structure Cyber Incident Reports. For the next chapter, we will explore using case studies to evaluate the effectiveness of using MITRE ATT&CK Framework structure in a Cyber Incident Report format.

5. Evaluation of Proposed Cyber Incident Report Format

This chapter provides an evaluation on the effectiveness of using MITRE ATT&CK Framework for ICSs in a Cyber Incident Report. The evaluation is conducted through comparing three different Cyber Incident cases in the ICS industry that occurred at three different periods.

5.1 Case 1: Iran Nuclear Facilities Attack 2010

From [25] to [27], the most famous incident in power grid sectors is the Stuxnet worm, which targeted Iranian nuclear facilities in 2010. This case has been widely discussed since its discovery and will be used as a case to validate if the data type proposed can be useful in learning and preventing similar incidents in later cases.

In the Stuxnet worm, the ICS is considered secure by implementing "air-gap," that isolates itself from other systems in the network. However, the Stuxnet worm has the capability to infect via a USB drive which was connected to a workstation in the SCADA infrastructure. Stuxnet targeted PLCs in the system and maliciously re-configured PLCs to manipulate the rotation speed of the centrifuge units of the nuclear facilities. In addition, this sophisticated malware was able to masked its actions by sending normal data to the SCADA HMI (human-machine interface) system.

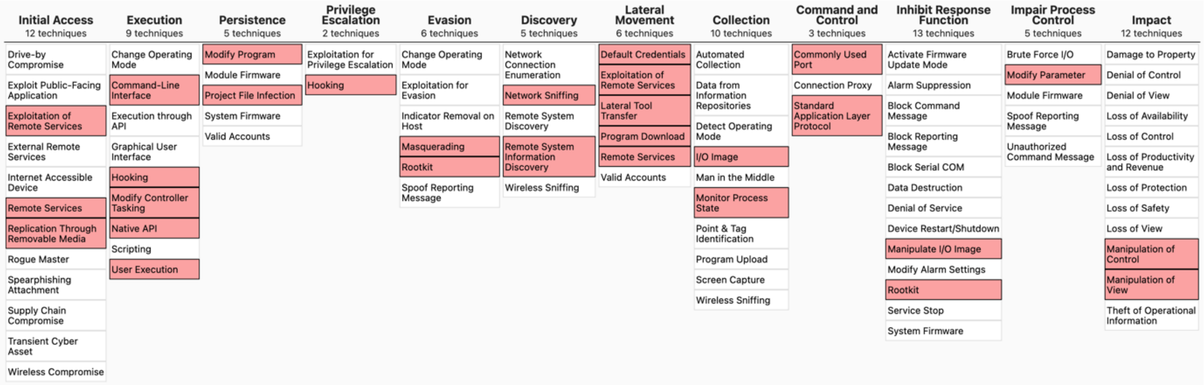
Using data directly from the [15]MITRE ATT&CK Framework for ICS, the identified TTPs used in the Stuxnet worm are as listed in Table 11 and also highlighted in the MITRE ATT&CK Matrix (Figure 24).

No.	Technique ID	Technique Name
1	T0807	Command-Line Interface
2	T0885	Commonly Used Port
3	T0812	Default Credentials
4	T0866	Exploitation of Remote Services
5	T0874	Hooking
6	T0877	I/O Image
7	T0867	Lateral Tool Transfer
8	T0835	Manipulate I/O Image
9	T0831	Manipulation of Control
10	T0832	Manipulation of View
11	T0849	Masquerading
12	T0821	Modify Controller Tasking

[15] MITRE ATT&CK Database - https://attack.mitre.org/software/S0603

13	T0836	Modify Parameter
14	T0889	Modify Program
15	T0801	Monitor Process State
16	T0834	Native API
17	T0842	Network Sniffing
18	T0843	Program Download
19	T0873	Project File Infection
20	T0886	Remote Services
21	T0888	Remote System Information Discovery
22	T0847	Replication Through Removable Media
23	T0851	Rootkit
24	T0869	Standard Application Layer Protocol
25	T0863	User Execution

Table 12: TTPs for Stuxnet Malware (Source: MITRE ATT&CK Database (https://attack.mitre.org/software/S0603/)



Initial Access 12 techniques	Execution 9 techniques	Persistence 5 techniques	Privilege Escalation 2 techniques	Evasion 6 techniques	Discovery 5 techniques	Lateral Movement 6 techniques	Collection 10 techniques	Command and Control 3 techniques	Inhibit Response Function 13 techniques	Impair Process Control 5 techniques	Impact 12 techniques
Drive-by Compromise	Change Operating Mode	**Modify Program**	Exploitation for Privilege Escalation	Change Operating Mode	Network Connection Enumeration	**Default Credentials**	Automated Collection	**Commonly Used Port**	Activate Firmware Update Mode	Brute Force I/O	Damage to Property
Exploit Public-Facing Application	**Command-Line Interface**	Module Firmware	**Hooking**	Exploitation for Evasion	**Network Sniffing**	**Exploitation of Remote Services**	Data from Information Repositories	Connection Proxy	Alarm Suppression	**Modify Parameter**	Denial of Control
Exploitation of Remote Services	Execution through API	**Project File Infection**		Indicator Removal on Host	Remote System Discovery	**Lateral Tool Transfer**	Detect Operating Mode	**Standard Application Layer Protocol**	Block Command Message	Module Firmware	Denial of View
External Remote Services	Graphical User Interface	System Firmware		**Masquerading**	**Remote System Information Discovery**	**Program Download**	**I/O Image**		Block Reporting Message	Spoof Reporting Message	Loss of Availability
Internet Accessible Device	**Hooking**	Valid Accounts		**Rootkit**	Wireless Sniffing	**Remote Services**	Man in the Middle		Block Serial COM	Unauthorized Command Message	Loss of Control
Remote Services	**Modify Controller Tasking**			Spoof Reporting Message		Valid Accounts	**Monitor Process State**		Data Destruction		Loss of Productivity and Revenue
Replication Through Removable Media	**Native API**						Point & Tag Identification		Denial of Service		Loss of Protection
Rogue Master	Scripting						Program Upload		Device Restart/Shutdown		Loss of Safety
Spearphishing Attachment	**User Execution**						Screen Capture		**Manipulate I/O Image**		Loss of View
Supply Chain Compromise							Wireless Sniffing		Modify Alarm Settings		**Manipulation of Control**
Transient Cyber Asset									**Rootkit**		**Manipulation of View**
Wireless Compromise									Service Stop		Theft of Operational Information
									System Firmware		

Figure 24: MITRE ATT&CK ICS Matrix for Stuxnet Malware (Source: MITRE ATT&CK Database - https://attack.mitre.org/software/S0603/)

5.1.1 Cyber Incident Report on Iranian Nuclear Facilities 2010

Table 12 demonstrates how the Cyber Incident Report would be using the MITRE ATT&CK Framework in the baseline Cyber Incident Report format.

No	Required Data	Cyber Incident Report
1.	Incident description that includes the TTPs and timeline	Using Details in Table 11 and Figure 24, it can describe the entire chain of event from initial access to impact and the specific TTPs that the adversary uses. As there were no publicly available information on the exact timing of these events, we will assume that the incident respondent will indicate accordingly during the documentation.
2.	Impact description and timeline	
3.	Time from attack to detection	

<table>
<tr><td>4.</td><td>Time from detection to isolation</td><td rowspan="7"></td></tr>
<tr><td>5.</td><td>Time from isolation to recovery</td></tr>
<tr><td>6.</td><td>Details on stakeholder reporting</td></tr>
<tr><td>7.</td><td>Investigation description and timeline</td></tr>
<tr><td>8.</td><td>Recovery description that includes containment and timeline</td></tr>
<tr><td>9.</td><td>Reflection on redundant recovery plans</td></tr>
<tr><td>10.</td><td>Details on each stage of incident response</td></tr>
<tr><td>11.</td><td>Platform for sharing cyber threat</td><td>Using MITRE ATT&CK Framework structure in terms of TTP, it facilitates further sharing to other ICS organizations.</td></tr>
<tr><td>12.</td><td>Structure data inputs for analytics</td><td>Using platform like web forms, each field can be tag as a data type for analytic purposes</td></tr>
<tr><td>13.</td><td>Control failure for incident</td><td>Nourian and Madnick [28] identified 35 threats based on the analyzed control structure. These threats can be categorized into the following broad categories:
1. lack of control in verifying inputs and outputs for each individual components in the control loops,
2. lack of control in verifying the source command issuer and destination command received,
3. lack of control in predicting emerging effects created by the lower-level or upper-level control loops,
4. lack of control in verifying the authenticity of the software pieces used in system components such as SCADAs, PLCs, and devices' firmwares, and
5. lack of control in creating secure tunnel for communication between the components in the network</td></tr>
<tr><td>14.</td><td>Add new or modify existing control to prevent incident</td><td>One example is to disable non-authorized removable media</td></tr>
<tr><td>15.</td><td>Indicators of Compromise (IOC)</td><td><table><tr><td>Filename and Path</td><td>Hash</td></tr></table></td></tr>
</table>

<table>
<tr><td></td><td></td><td><table><tr><td>WINDOWS\inf\mdmeric3.PNF</td><td>b834ebeb777ea07fb6aab6bf35cdf07f</td></tr><tr><td>WINDOWS\inf\oem6C.PNF</td><td>Hash may vary</td></tr><tr><td>WINDOWS\inf\oem7A.PNF</td><td>ad19fbaa55e8ad585a97bbcddcde59d4</td></tr><tr><td>WINDOWS\inf\mdmcpq3.PNF</td><td>Hash may vary</td></tr></table>Source: US CERT - https://www.cisa.gov/uscert/ics/advisories/ICSA-10-272-01</td></tr>
<tr><td>16.</td><td>Indicators of Attacks (IOA)</td><td>Unintended and uncontrollable speed adjustment of ICS components that should be detected by monitoring systems</td></tr>
<tr><td>17.</td><td>Indicators of Interest (IOI)</td><td>No data for example</td></tr>
<tr><td>18.</td><td>Gap in capabilities to manage cyber risk</td><td>Encryption for secure communications between components</td></tr>
</table>

Table 13: Cyber Incident Report for Iran Nuclear Plant Incident 2010

5.2 Case 2: Ukraine Power Grid Attack 2015

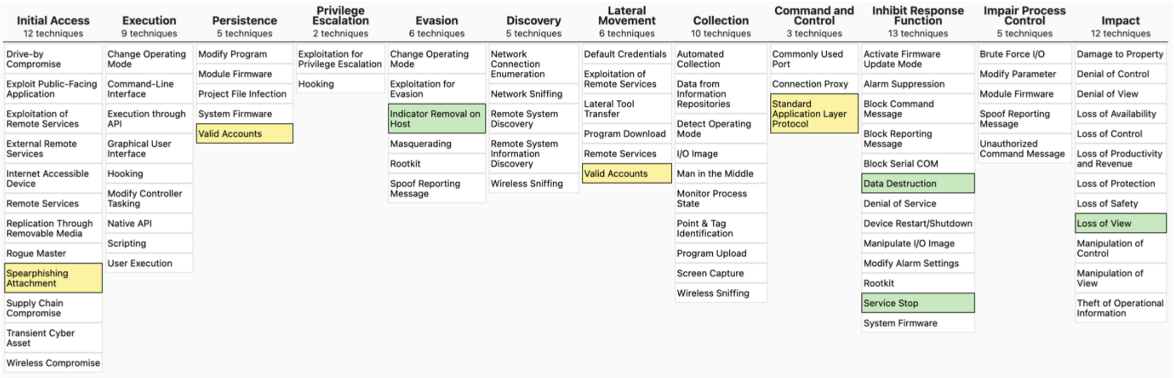
In 2015, power plants in Ukraine were attacked by hackers. This was a very well-prepared attack, and it is said that the attack started six months before the incident. The attacker started with a traditional cyber-attack strategy by Phishing emails and successfully infected targeted victims' computers with a malware called BlackEnergy. The BlackEnergy malware was used to collect useful information, including VPN credentials used for remotely accessing SCADA control system that were virtually separated by a firewall appliance from the other systems in the network. Hence, they managed to compromise the SCADA control system and inject malicious control commands to open a large number of circuit breakers. In addition, the attacker also deployed measures in the form of a malware called KillDisk to delay the recovery actions. The incident, as a result, caused a massive power outage that lasted for hours ([29] to [34]).

This particular malware has been identified to have 7 TTPs corresponding to [16]MITRE ATT&CK Framework ICS Matrix as shown in Table 13 and also highlighted in the MITRE ATT&CK Matrix in Figure 25 where the colours in Yellow indicates TTPs for BlackEnergy and Green indicates TTPs for KillDisk.

[16] MITRE ATT&CK - https://attack.mitre.org/software/S0089

No.	Technique ID	Technique Name
1	T0865	Spearphishing Attachment
2	T0869	Standard Application Layer Protocol
3	T0859	Valid Accounts
4	T0809	Data Destruction
5	T0872	Indicator Removal on Host
6	T0829	Loss of View
7	T0881	Service Stop

Table 14: ATT&CK TTP identified in BlackEnergy and KillDisk (Source: MITRE ATT&CK - https://attack.mitre.org/software/S0089/)



Initial Access 12 techniques	Execution 9 techniques	Persistence 5 techniques	Privilege Escalation 2 techniques	Evasion 6 techniques	Discovery 5 techniques	Lateral Movement 6 techniques	Collection 10 techniques	Command and Control 3 techniques	Inhibit Response Function 13 techniques	Impair Process Control 5 techniques	Impact 12 techniques
Drive-by Compromise	Change Operating Mode	Modify Program	Exploitation for Privilege Escalation	Change Operating Mode	Network Connection Enumeration	Default Credentials	Automated Collection	Commonly Used Port	Activate Firmware Update Mode	Brute Force I/O	Damage to Property
Exploit Public-Facing Application	Command-Line Interface	Module Firmware	Hooking	Exploitation for Evasion	Network Sniffing	Exploitation of Remote Services	Data from Information Repositories	Connection Proxy	Alarm Suppression	Modify Parameter	Denial of Control
Exploitation of Remote Services	Execution through API	Project File Infection		Indicator Removal on Host	Remote System Discovery	Lateral Tool Transfer	Detect Operating Mode	Standard Application Layer Protocol	Block Command Message	Module Firmware	Denial of View
External Remote Services	Graphical User Interface	System Firmware		Masquerading	Remote System Information Discovery	Program Download	I/O Image		Block Reporting Message	Spoof Reporting Message	Loss of Availability
Internet Accessible Device	Hooking	Valid Accounts		Rootkit	Wireless Sniffing	Remote Services	Man in the Middle		Block Serial COM	Unauthorized Command Message	Loss of Control
Remote Services	Modify Controller Tasking			Spoof Reporting Message		Valid Accounts	Monitor Process State		Data Destruction		Loss of Productivity and Revenue
Replication Through Removable Media	Native API						Point & Tag Identification		Denial of Service		Loss of Protection
Rogue Master	Scripting						Program Upload		Device Restart/Shutdown		Loss of Safety
Spearphishing Attachment	User Execution						Screen Capture		Manipulate I/O Image		Loss of View
Supply Chain Compromise							Wireless Sniffing		Modify Alarm Settings		Manipulation of Control
Transient Cyber Asset									Rootkit		Manipulation of View
Wireless Compromise									Service Stop		Theft of Operational Information
									System Firmware		

Figure 25: MITRE ATT&CK ICS MATRIX for Ukraine Power Grid Attack 2015 (Source: MITRE ATT&CK - https://attack.mitre.org/software/S0089/)

5.2.1 Cyber Incident Report on Ukraine Power Grid Attack 2015

Table 14 demonstrates how the Cyber Incident Report would be using the MITRE ATT&CK Framework in the baseline Cyber Incident Report format.

No	Required Data	Cyber Incident Report
1.	Incident description that includes the TTPs and timeline	Using Details in Table 10 and Figure 26, it can describe the entire chain of event from initial access to impact and the specific TTPs that the adversary uses. As there were no publicly available information on the exact timing of these events, we will assume that the incident respondent will indicate accordingly during the documentation.
2.	Impact description and timeline	
3.	Time from attack to detection	
4.	Time from detection to isolation	

<table>
<tr><td>5.</td><td>Time from isolation to recovery</td><td rowspan="6"></td></tr>
<tr><td>6.</td><td>Details on stakeholder reporting</td></tr>
<tr><td>7.</td><td>Investigation description and timeline</td></tr>
<tr><td>8.</td><td>Recovery description that includes containment and timeline</td></tr>
<tr><td>9.</td><td>Reflection on redundant recovery plans</td></tr>
<tr><td>10.</td><td>Details on each stage of incident response</td></tr>
<tr><td>11.</td><td>Platform for sharing cyber threat</td><td>Using MITRE ATT&CK Framework structure in terms of TTP, it facilitates further sharing to other ICS organizations.</td></tr>
<tr><td>12.</td><td>Structure data inputs for analytics</td><td>Using platform like web forms, each field can be tag as a data type for analytic purposes</td></tr>
<tr><td>13.</td><td>Control failure for incident</td><td>An example could be Lack of control in communication to non-reputable websites that allowed HTTP POST request for malware to callback its command-and-control servers.</td></tr>
<tr><td>14.</td><td>Add new or modify existing control to prevent incident</td><td>An example could be Enable verification of non-reputable websites communication and downloads</td></tr>
<tr><td>15.</td><td>Indicators of Compromise (IOC)</td><td>
<table>
<tr><td><i>Word document with macros (Trojan-Downloader.Script.Generic)</i></td><td>e15b36c2e394d599a8ab352159089dd2</td></tr>
<tr><td><i>Dropper from Word document (Backdoor.Win32.Fonten.y)</i></td><td>ac2d7f21c826ce0c449481f79138aebd</td></tr>
<tr><td><i>Final payload from Word document (Backdoor.Win32.Fonten.o)</i></td><td>3fa9130c9ec44e36e52142f3688313ff</td></tr>
<tr><td><i>BlackEnergy C&C Server</i></td><td>IP address: 5.149.254[.]114</td></tr>
</table>
Source: BlackEnergy APT Attacks in Ukraine employ spearphishing with Word documents (https://securelist.com/blackenergy-apt-attacks-in-ukraine-employ-spearphishing-with-word-documents/73440/)</td></tr>
<tr><td>16.</td><td>Indicators of Attacks (IOA)</td><td>Unintended and uncontrollable adjustment of ICS component</td></tr>
</table>

17.	Indicators of Interest (IOI)	No data for example
18.	Gap in capabilities to manage cyber risk	Encryption for secure communications between components

Table 15:Cyber Incident Report for Ukraine Power Grid Incident 2015

5.3 Case 3: Ukraine Power Grid Attack 2016

With reference to [35] to [41], Ukrainian power plants were attacked again in 2016. In this incident, a malware called Industroyer or CrashOverride was utilized. One notable capability of the malware is that it alone can send messages compliant with standards used in the modernized power grid systems, such as IEC 61850 and IEC 60870, under control of a remote attacker via command and control channel. This implies that, once this malware infects any of the devices in the power grid control system, an attacker could inject malicious control commands without compromising the SCADA HMI workstation, as was the case in 2015 incident discussed earlier.

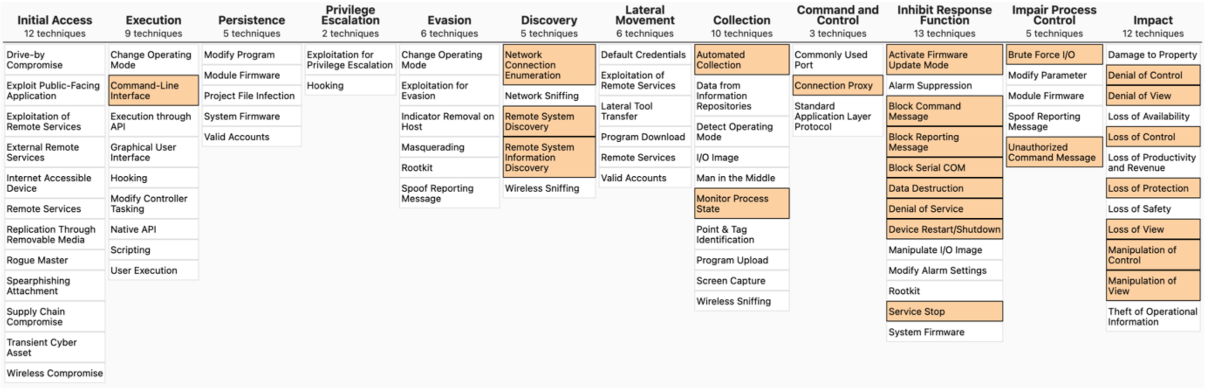
Based on [17]MITRE ATT&CK Framework ICS Matrix, this particular malware has been identified to have 24 TTPs corresponding to its ICS Matrix as shown in Table 15 and also highlighted in the MITRE ATT&CK Matri (Figure 26).

No.	Technique ID	Technique Name
1	T0800	Activate Firmware Update Mode
2	T0802	Automated Collection
3	T0803	Block Command Message
4	T0804	Block Reporting Message
5	T0805	Block Serial COM
6	T0806	Brute Force I/O
7	T0807	Command-Line Interface
8	T0884	Connection Proxy
9	T0809	Data Destruction
10	T0813	Denial of Control
11	T0814	Denial of Service
12	T0815	Denial of View
13	T0816	Device Restart/Shutdown
14	T0827	Loss of Control
15	T0837	Loss of Protection

[17] MITRE ATTA&CK Framework - https://attack.mitre.org/software/S0604

16	T0829	Loss of View
17	T0831	Manipulation of Control
18	T0832	Manipulation of View
19	T0801	Monitor Process State
20	T0840	Network Connection Enumeration
21	T0846	Remote System Discovery
22	T0888	Remote System Information Discovery
23	T0881	Service Stop
24	T0855	Unauthorized Command Message

Table 16: ATT&CK TTP identified in Industroyer (Source: MITRE ATTA&CK Framework - https://attack.mitre.org/software/S0604/)



Initial Access 12 techniques	Execution 9 techniques	Persistence 5 techniques	Privilege Escalation 2 techniques	Evasion 6 techniques	Discovery 5 techniques	Lateral Movement 6 techniques	Collection 10 techniques	Command and Control 3 techniques	Inhibit Response Function 13 techniques	Impair Process Control 5 techniques	Impact 12 techniques
Drive-by Compromise	Change Operating Mode	Modify Program	Exploitation for Privilege Escalation	Change Operating Mode	Network Connection Enumeration	Default Credentials	Automated Collection	Commonly Used Port	Activate Firmware Update Mode	Brute Force I/O	Damage to Property
Exploit Public-Facing Application	Command-Line Interface	Module Firmware	Hooking	Exploitation for Evasion	Network Sniffing	Exploitation of Remote Services	Data from Information Repositories	Connection Proxy	Alarm Suppression	Modify Parameter	Denial of Control
Exploitation of Remote Services	Execution through API	Project File Infection		Indicator Removal on Host	Remote System Discovery	Lateral Tool Transfer	Detect Operating Mode	Standard Application Layer Protocol	Block Command Message	Module Firmware	Denial of View
External Remote Services	Graphical User Interface	System Firmware		Masquerading	Remote System Information Discovery	Program Download	I/O Image		Block Reporting Message	Spoof Reporting Message	Loss of Availability
Internet Accessible Device	Hooking	Valid Accounts		Rootkit	Wireless Sniffing	Remote Services	Man in the Middle		Block Serial COM	Unauthorized Command Message	Loss of Control
Remote Services	Modify Controller Tasking			Spoof Reporting Message		Valid Accounts	Monitor Process State		Data Destruction		Loss of Productivity and Revenue
Replication Through Removable Media	Native API						Point & Tag Identification		Denial of Service		Loss of Protection
Rogue Master	Scripting						Program Upload		Device Restart/Shutdown		Loss of Safety
Spearphishing Attachment	User Execution						Screen Capture		Manipulate I/O Image		Loss of View
Supply Chain Compromise							Wireless Sniffing		Modify Alarm Settings		Manipulation of Control
Transient Cyber Asset									Rootkit		Manipulation of View
Wireless Compromise									Service Stop		Theft of Operational Information
									System Firmware		

Figure 26: MITRE ATT&CK ICS MATRIX for Ukraine Power Grid Attack 2016 (Source: MITRE ATTA&CK Framework - https://attack.mitre.org/software/S0604/)

5.3.1 Cyber Incident Report on Ukraine Power Grid Attack 2016

Table 16 demonstrates how the Cyber Incident Report would be using the MITRE ATT&CK Framework in the baseline Cyber Incident Report format.

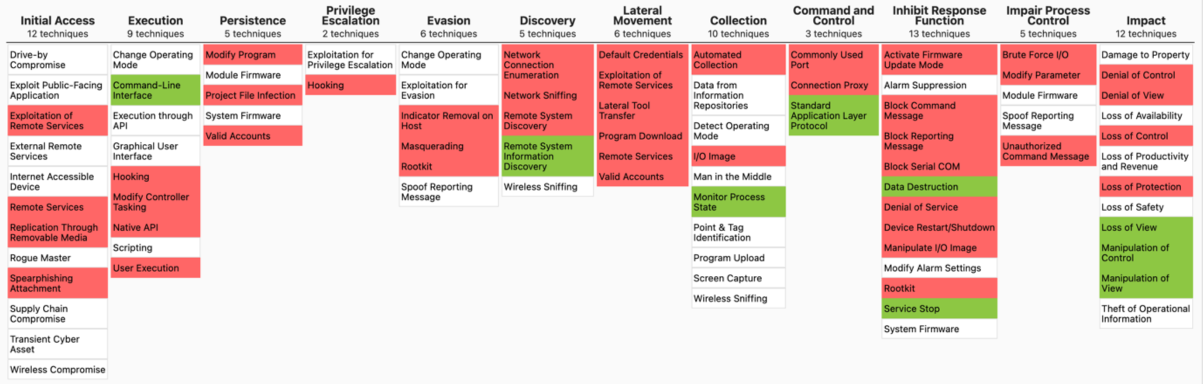
No	Required Data	Cyber Incident Report
1.	Incident description that includes the TTPs and timeline	Using Details in Table 12 and Figure 27, it can describe the entire chain of event from initial access to impact and the specific TTPs that the adversary uses. As there were no publicly available information on the exact timing of these events, we will assume that the incident respondent will indicate accordingly during the documentation.
2.	Impact description and timeline	
3.	Time from attack to detection	
4.	Time from detection to isolation	

5.	Time from isolation to recovery	
6.	Details on stakeholder reporting	
7.	Investigation description and timeline	
8.	Recovery description that includes containment and timeline	
9.	Reflection on redundant recovery plans	
10.	Details on each stage of incident response	
11.	Platform for sharing cyber threat	Using MITRE ATT&CK Framework structure in terms of TTP, it facilitates further sharing to other ICS organizations.
12.	Structure data inputs for analytics	Using platform like web forms, each field can be tag as a data type for analytic purposes
13.	Control failure for incident	An example could be Lack of control in COM port communication
14.	Add new or modify existing control to prevent incident	An example could be controlling the communication in COM ports
15.	Indicators of Compromise (IOC)	SHA-1 hashes: 1. F6C21F8189CED6AE150F9EF2E82A3A57843B587D 2. CCCCE62996D578B984984426A024D9B250237533 3. 8E39ECA1E48240C01EE570631AE8F0C9A9637187 4. 2CB8230281B86FA944D3043AE906016C8B5984D9 5. 79CA89711CDAEDB16B0CCCCFDCFBD6AA7E57120A 6. 94488F214B165512D2FC0438A581F5C9E3BD4D4C 7. 5A5FAFBC3FEC8D36FD57B075EBF34119BA3BFF04 8. B92149F046F00BB69DE329B8457D32C24726EE00 9. B335163E6EB854DF5E08E85026B2C3518891EDA8 IP Addresses of C&C servers: 1. 195.16.88[.]6 2. 46.28.200[.]132 3. 188.42.253[.]43 4. 5.39.218[.]152 5. 93.115.27[.]57 Source: WIN32/Industroyer by ESET - https://www.welivesecurity.com/wp-content/uploads/2017/06/Win32_Industroyer.pdf
16.	Indicators of Attacks (IOA)	Unintended and uncontrollable adjustment of ICS component
17.	Indicators of Interest (IOI)	No data for example
18.	Gap in capabilities to manage cyber risk	Encryption for secure communications between components

Table 17: Cyber Incident Report for Ukraine Power Grid Incident 2016

5.4 Comparison of 3 Cases

With the usage of MITRE ATT&CK Framework for ICS, we can compare across the 3 cases to identify any similar TTP being used for the respective cases. Figure 27 shows the MITRE ATT&CK ICS Matrix with the repeated TTPs for more than 1 case highlighted in GREEN. Table 17 compiles the respective TTPs across the 3 cases and there were indeed techniques used between Case 1 and 2, Case 2 and 3 and also Case 1 and 3.



Initial Access 12 techniques	Execution 9 techniques	Persistence 5 techniques	Privilege Escalation 2 techniques	Evasion 6 techniques	Discovery 5 techniques	Lateral Movement 6 techniques	Collection 10 techniques	Command and Control 3 techniques	Inhibit Response Function 13 techniques	Impair Process Control 5 techniques	Impact 12 techniques
Drive-by Compromise	Change Operating Mode	Modify Program	Exploitation for Privilege Escalation	Change Operating Mode	Network Connection Enumeration	Default Credentials	Automated Collection	Commonly Used Port	Activate Firmware Update Mode	Brute Force I/O	Damage to Property
Exploit Public-Facing Application	Command-Line Interface	Module Firmware	Hooking	Exploitation for Evasion	Network Sniffing	Exploitation of Remote Services	Data from Information Repositories	Connection Proxy	Alarm Suppression	Modify Parameter	Denial of Control
Exploitation of Remote Services	Execution through API	Project File Infection		Indicator Removal on Host	Remote System Discovery	Lateral Tool Transfer	Detect Operating Mode	Standard Application Layer Protocol	Block Command Message	Module Firmware	Denial of View
External Remote Services	Graphical User Interface	System Firmware		Masquerading	Remote System Information Discovery	Program Download	I/O Image		Block Reporting Message	Spoof Reporting Message	Loss of Availability
Internet Accessible Device	Hooking	Valid Accounts		Rootkit	Wireless Sniffing	Remote Services	Man in the Middle		Block Serial COM	Unauthorized Command Message	Loss of Control
Remote Services	Modify Controller Tasking			Spoof Reporting Message		Valid Accounts	Monitor Process State		Data Destruction		Loss of Productivity and Revenue
Replication Through Removable Media	Native API						Point & Tag Identification		Denial of Service		Loss of Protection
Rogue Master	Scripting						Program Upload		Device Restart/Shutdown		Loss of Safety
Spearphishing Attachment	User Execution						Screen Capture		Manipulate I/O Image		Loss of View
Supply Chain Compromise							Wireless Sniffing		Modify Alarm Settings		Manipulation of Control
Transient Cyber Asset									Rootkit		Manipulation of View
Wireless Compromise									Service Stop		Theft of Operational Information
									System Firmware		

Figure 27: MITRE ATT&CK ICS Matrix showing similar TTPs occurring in multiple cases in GREEN

No.	Technique ID	Technique NAME	Case 1 (Iran Nuclear)	Case 2 (Ukraine 2015)	Case 3 (Ukraine 2016)
1	T0807	Command-Line Interface	Yes	No	Yes
2	T0888	Remote System Information Discovery	Yes	No	Yes
3	T0801	Monitor Process State	Yes	No	Yes
4	T0831	Manipulation of Control	Yes	No	Yes
5	T0832	Manipulation of View	Yes	No	Yes
6	T0869	Standard Application Layer Protocol	Yes	Yes	No
7	T0829	Loss of View	No	Yes	Yes
8	T0809	Data Destruction	No	Yes	Yes
9	T0881	Service Stop	No	Yes	Yes

Table 18: MITRE ATT&CK ICS TTP compared across 3 cases

By using MITRE ATT&CK Framework for ICS, similar techniques across different Cyber Incidents cases can be identified such that there are existing controls that could help detect or mitigate vulnerabilities in ICS. Even though the specific procedures in each technique can be very different, the mitigation methods are the same across the same technique. Table 18 illustrates the suggested mitigation methods for the 9 techniques identified.

For Case 1 and 2 example, the procedures and mitigations for Technique (T0869) Standard Application Layer Protocol are shown in Table 18.

ID	Name	Description
Procedures		
S0089	BlackEnergy	Sandworm Team uses HTTP POST request to contact external command and control servers. [1]
S0603	Stuxnet	Stuxnet uses a thread to monitor a data block DB890 of sequence A or B. This thread is constantly running and probing this block (every 5 minutes). On an infected PLC, if block DB890 is found and contains a special magic value (used by Stuxnet to identify his own block DB890), this blocks data can be read and written. This thread is likely used to optimize the way sequences A and B work, and modify their behavior when the Step7 editor is opened.
Mitigations		
M0807	Network Allowlists	Network allowlists can be implemented through either host-based files or system host files to specify what external connections (e.g., IP address, MAC address, port, protocol) can be made from a device. Allowlist techniques that operate at the application layer (e.g., DNP3, Modbus, HTTP) are addressed in the Filter Network Traffic mitigation.
M0931	Network Intrusion Prevention	Network intrusion detection and prevention systems that use network signatures to identify traffic for specific adversary malware can be used to mitigate activity at the network level.
M0930	Network Segmentation	Ensure proper network segmentation between higher level corporate resources and the control process environment.

Table 19: Procedures and Mitigations for Case 1 and 2 (Source: https://attack.mitre.org/techniques/T0869/)

For Case 1 and 3 example, the procedures and mitigations for Technique (T0807) Command-Line Interface are shown in Table 19.

ID	Name	Description
Procedures		
S0604	Industroyer	The name of the Industroyer payload DLL is supplied by the attackers via a command line parameter supplied in

		one of the main backdoors execute a shell command commands. [2]
S0603	Stuxnet	Stuxnet will store and execute SQL code that will extract and execute Stuxnet from the saved CAB file using xp_cmdshell with the following command: set @s = master..xp _ cmdshell extrac32 /y +@t+ +@t+x; exec(@s); [4]
Mitigations		
M0942	Disable or Remove Feature or Program	Consider removing or restricting features that are unnecessary to an asset's intended function within the control environment.
M0938	Execution Prevention	Execution prevention may block malicious software from accessing protected resources through the command line interface.

Table 20: Procedures and Mitigations for Case 1 and 3 (Source: https://attack.mitre.org/techniques/T0807/)

For Case 2 and 3 example, the procedures and mitigations for Technique (T0829) Loss of View are shown in Table 19.

ID	Name	Description
Procedures		
S0607	KillDisk	KillDisk erases the master boot record (MBR) and system logs, leaving the system unusable.
S0604	Industroyer	Industroyer's data wiper component removes the registry \image path\ throughout the system and overwrites all files, rendering the system unusable.
Mitigations		
M0953	Data Backup	Take and store data backups from end user systems and critical servers. Ensure backup and storage systems are hardened and kept separate from the corporate network to prevent compromise. Maintain and exercise incident response plans [8], including the management of \gold-copy\ back-up images and configurations for key systems to enable quick recovery and response from adversarial activities that impact control, view, or availability.

M0810	Out-of-Band Communications Channel	Provide operators with redundant, out-of-band communication to support monitoring and control of the operational processes, especially when recovering from a network outage [9]. Out-of-band communication should utilize diverse systems and technologies to minimize common failure modes and vulnerabilities within the communications infrastructure. For example, wireless networks (e.g., 3G, 4G) can be used to provide diverse and redundant delivery of data.
M0811	Redundancy of Service	Hot-standbys in diverse locations can ensure continued operations if the primarily system are compromised or unavailable. At the network layer, protocols such as the Parallel Redundancy Protocol can be used to simultaneously use redundant and diverse communication over a local network. [10]

Table 21: Procedures and Mitigations for Case 2 and 3 (Source: https://attack.mitre.org/techniques/T0829/)

5.5 SUMMARY

This chapter evaluated using MITRE ATT&CK Framework in *Cyber Incident* Reports by comparing three *Cyber Incident* from three different periods. The comparison showed that there were similar TTPs across either 2 of the 3 cases. According to MITRE ATT&CK Framework, the mitigations methods are the same for each technique category hence the vulnerability can be mitigated when it is implemented correctly. As some of the ATT&CK categorizes are board, it is uncertain that the same mitigation will work for every variation. However, this work did not find any information on whether the incident responders in cases 2 and 3 were able to learn and implement the mitigations of the earlier cases. Hence, it is useful to use MITRE ATT&CK Framework to describe a Cyber Incident, but it requires more data of Cyber Incidents to validate the effectiveness.

6. CONCLUSION

This chapter will describe the lessons learned from the work done in this study. The limitation for this study will also be noted and possible future research will be proposed.

6.1 LESSONS LEARNED

Can organizations that rely on ICSs improve their cybersecurity posture through Cyber Incident Reports?

Yes, Cyber Incident Reports contribute to the database of threats and their TTPs. With the increased emphasis on regulating organizations in reporting *Cyber Incidents* promptly such as the CIRCIA 2022, the database will be enriched further. Organizations must share *Cyber Incident* information with other similar organizations to improve their security posture. Threat actors thrive on victims' tardiness and reluctance to share Cyber Incidents so that they can continue to use their unique tradecraft on similar setups in other organizations. The opportunity to exploit will be limited once the information is shared, and mitigation can be implemented as soon as possible to deter further Cyber Incidents.

What are the necessary ingredients for Cyber Incident Reports to be effective?

The effectiveness of Cyber Incident Reports depends on many factors such as the following:

1. "What" - What type(s) of information is required needs to be spelled out clearly so that organizations report the relevant information from the start to reduce time on checking and corresponding.
2. "How" – The format of reports needs to be standardized to reduce ambiguous reporting that includes the structure of describing the respective information element. This work experimented using MITRE ATT&CK Framework to describe the incident and further work is needed to show its effectiveness.
3. "Why" – The reason(s) for failed or absence of control measures that exist should be clearly reported as many existing incidents were caused by non-technical issues such as improper implementation of security controls.
4. "Who" – The role in the organization that is accountable for Cyber Incident Reporting is unclear in the current regulations as not all organization has a CIO/CISO. Hence, the regulation should indicate the person accountable for compliance and its punishment for non-compliance.
5. "Where" - A common reporting website where the Office manages, and all other federal agencies should direct the reporting to this centralized site.
6. "When" – The timeline established for Cyber Incident Reporting differs between different governing bodies such as 72 hours for CIRCIA and 96 hours for SEC. This may confuse ICS organizations who need to comply with both regulations. On top of

that, many organizations only realize that there is a Cyber Incident happening long after it started so the information may not be as recent and useful.

From the evaluation of the information required in the existing Cyber Incident Report format in Chapter 3, it is not obvious how it could make a significant difference to other organizations. Information such as “why” as mentioned above were not compulsory in submitting the report. Hence, even as organizations report their incidents within the regulated time frame, it is of little use if such information is not shared in mitigating similar incidents. Without a common structure of reporting, a lot of time will be spent processing the data before it can be shared effectively.

Other thoughts

Cybersecurity incidents are serious risks that could impact a business significantly. However, it is currently not prioritized in terms of professional bodies. Professional functions such as the American Institute of Certified Public Accountants (AICIA) require accountants to be certified and are regulated by certain laws. Another example is the need for engineers to be certified Professional Engineers by licensing boards in order to be accountable for the structural and electrical design of a building. Hence, if *Cyber Incident*s in critical infrastructure can be comparable to the safety considerations of electrical designs, a professional body regulated by law could be set up to ensure systems design can meet a certain level of standards.

Many security agencies and vendors publish guides on principles and best practices in designing an incident response team which includes documentation requirements. These guides usually provide strategies, and it will take a professional cybersecurity practitioner to implement them into an actual operational process that is suitable for their organization. During the study of various Cyber Incident Report formats, the form is found to be insufficient in collecting critical data. Many organizations use this simple form for victims to submit their cases as though it is like getting a queue number for prioritization to attend to a doctor.

There is the initial report format that the "victim" uses to report to the authorities, and there is another follow-up report that the authorities use for documenting their investigation. The follow-up report covers more details in forensic investigation that includes the specific work done and the discovery of various sources of logs and components of the entire system and organization. It was challenging to obtain the follow-up version from the respective authorities as they cited a confidential process for investigation. This approach does not help victims check through their findings and will require the investigator to follow up, which further delays the eventual sharing of the incident.

6.2 LIMITATION

This study depended on the interpretation of cybersecurity principles and industry best practices through guides and recommendation. It is used as an academic study on how the Cyber Incident report format can look like and how it can benefit the sharing of incident information with the specific categories required. It should be further improved with more used cases and made further adoption easier.

6.3 FUTURE RESEARCH

The research presented in this thesis should serve to encourage further exploration of the Cyber Incident Report to increase its effectiveness that can improve the ICS community security posture.

A further recommendation is the study of the effects of setting up a professional body for a cyber security practitioner to be certified and the requirement of having such certified personnel in the ICS organization to ensure accountability in the ICS cybersecurity design and compliance requirement. Like the National Initiative for Cybersecurity Careers and Studies in NIST Cybersecurity Professional Practitioner Certification Training, it could be made compulsory by law to have such qualified personnel in every organization for accountability. With the CIRCIA 2022 leading the way, more regulations seem to be essential in ensuring the emphasis on managing cyber risk in organizations. A study on the implementation plans and the impact on organizations, in general, can help the community understand the effectiveness and impact of such a setup.

Another recommendation is the study on the usefulness of the 18 Information Elements derived in this work using data from actual incident reports. Each of the Information Elements can be evaluated on its usefulness for specific purposes of reporting. For example, what are the Information Element that are important specifically for ransomware or Cyber Incidents that do not have any breach.

7. Bibliography

[1] Johnson et al., Guide to Cyber Threat Information Sharing, SP 800-150, NIST, https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-150.pdf, (Accessed July 31, 2022)

[2] G. Loukas, Cyber-physical attacks : a growing invisible threat, n.d.

[3] Stouffer et al., Guide to Industrial Control Systems (ICS) Security, SP 800-82 v2, NIST, https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-82r2.pdf, (Accessed July 31, 2022)

[4] Cichonski et al., 2012, Computer Security Incident Handling Guide, NIST SP 800-61 R2, https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-61r2.pdf, (Accessed July 31, 2022)

[5] Ross et al., Developing Cyber-Resilient Systems: A Systems Security Engineering Approach, 2020, https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-160v2r1.pdf , (Accessed July 31, 2022)

[6] Boer and Idler, June 2021, Effective Cyber Incident Reporting: a call for greater consistency, improved information-sharing and closer cross-broader cooperation, Institute of International Finance, https://www.iif.com/Publications/ID/4455/IIF-Paper-on-the-Importance-of-More-Effective-Cyber-Incident-Reporting, (Accessed July 31, 2022)

[7] Use of Cryptocurrency in Ransomware Attacks, Available Data, and National Security Concerns, 2021, Homeland Security & Governmental Affairs, https://www.hsgac.senate.gov/imo/media/doc/HSGAC%20Majority%20Cryptocurrency%20Ransomware%20Report.pdf ((Accessed July 31, 2022)

[8] Hennin et al., 2008, Control System Cyber Incident Reporting Protocol, Raytheon, https://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=4534497, (accessed June 30, 2022)

[9] Varga et. Al., 2020, Evaluation of Information Elements in a Cyber Incident Report, KTH Royal Institue of Technology https://conferences.computer.org/eurosp/pdfs/EuroSPW2020-7k9FlVRX4z43j4uE2SeXU0/859700a017/859700a017.pdf, (accessed August 15, 2022)

[10] Cyber Incident Reporting for Critical Infrastructure Act of 2022, CISA, https://www.cisa.gov/sites/default/files/publications/Cyber-Incident-Reporting-ForCriticalInfrastructure-Act-o-f2022_508.pdf, (accessed June 30, 2022)

[11] Neto et al., January 2020, A Case Study of the Capital One Data Breach, MIT, https://web.mit.edu/smadnick/www/wp/2020-07.pdf, (accessed June 30, 2022)

[12] Operational technology research report 2021, Skybox Security, 2021, https://www.skyboxsecurity.com/resources/report/cybersecurity-risk-underestimated-operational-technology-organizations/?modal=true, (Accessed July 31, 2022)

[13] Internet Crime Report 2021, Internet Crime Compliant Center, FBI,

https://www.ic3.gov/Media/PDF/AnnualReport/2021_IC3Report.pdf (accessed June 30, 2022)

[14] Report Cyber Incident, Cybersecurity & Infrastructure Security Agency, https://www.cisa.gov/reporting-cyber-incidents, (accessed August 15, 2022)

[15] Framework for Improving Critical Infrastructure Cybersecurity, NIST, 2018 https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.04162018.pdf (accessed June 30, 2022)

[16] Security and Privacy Controls for Federal Information Systems and Organizations, NIST SP 800-53 Rev. 5, September 2020, NIST, https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r5.pdf, (accessed August 15, 2022)

[17] CIS Control 19. Incidnet Response and Management, Pg 21, Implementation Guide for Industrial Control Systems v7, CIS Controls, Center for Internet Security, https://learn.cisecurity.org/cis-controls-download, , (accessed August 15, 2022)

[18] Homeland Security (2009) Recommended Practice: Developing an Industrial Control Systems Cybersecurity Incident Response Capability, https://www.cisa.gov/uscert/sites/default/files/recommended_practices/final-RP_ics_cybersecurity_incident_response_100609.pdf, (accessed August 15, 2022)

[19] Pauna, A. et al. (2013). Can We Learn from SCADA Security Incidents. White Paper, European Union Agency for Network and Information Security, Heraklion, Crete, Greece, https://www.enisa.europa.eu/publications/can-we-learn-from-scada-security-incidents/@@download/fullReport, (accessed August 15, 2022)

[20] Incident Response using MITRE ATTACK, Sep 16, 2020, Security Controls and Resilience, Huntsman: https://www.huntsmansecurity.com/blog/incident-response-using-mitre-attack/, (accessed August 15, 2022)

[21] Optimize Your Incident Response Planning with the MITRE Framework, Aug 10, 2021, Trend Micro: https://www.trendmicro.com/en_us/ciso/21/h/optimize-your-incident-response-planning-with-the-mitre-framework.html, (accessed August 15, 2022)

[22] Iranian Government-Sponsored Actors Conduct Cyber Operations Against Global Governement and Commercial Networks, Feb 24, 2022, CISA: https://www.cisa.gov/uscert/ncas/alerts/aa22-055a, (accessed August 15, 2022)

[23] Multiple Vulnerabilities in Google Chrome Could Allow for Arbitary Code Execution, Jun 12, 2022, CIS: https://www.cisecurity.org/advisory/multiple-vulnerabilities-in-google-chrome-could-allow-for-arbitrary-code-execution_2022-084, (accessed August 15, 2022)

[24] B. Storm, A.Applebaum, D.Miller, K. Nickels, A.Pennington, C.Thomas, MITRE ATT&CK: Design and Philosophy, July 2018N.G. Leveson, J.P. Thomas, STPA Handbook, 2018. http://psas.scripts.mit.edu/home/ (accessed April 28, 2019).

[25] Nicolas Falliere, Liam O. Murchu, Eric Chien. (2011, February). W32.Stuxnet Dossier, https://www.wired.com/images_blogs/threatlevel/2010/11/w32_stuxnet_dossier.pdf, (accessed August 15, 2022)

[26] Matrosov, A., Rodionov, E., Harley, D., Malcho, J.. (n.d.). Stuxnet Under the Microscope. https://esetnod32.ru/company/viruslab/analytics/doc/Stuxnet_Under_the_Microscope.pdf , (accessed August 15, 2022)

[27] Ralph Langner. (2013, November). Ralph Langner. (2013, November). To Kill a Centrifuge: A Technical Analysis of What Stuxnet's Creators Tried to Achieve. https://www.langner.com/wp-content/uploads/2017/03/to-kill-a-centrifuge.pdf , (accessed August 15, 2022)

[28] A. Nourian, S. Madnick, A Systems Theoretic Approach to the Security Threats in Cyber Physical Systems Applied to Stuxnet, MIT, https://mitsloan.mit.edu/shared/ods/documents?PublicationDocumentID=4565, (accessed August 15, 2022)

[29] F-Secure Labs. (2014). BlackEnergy & Quedagh: The convergence of crimeware and APT attacks. https://blog-assets.f-secure.com/wp-content/uploads/2019/10/15163408/BlackEnergy_Quedagh.pdf, (accessed August 15, 2022)

[30] Baumgartner, K. and Garnaeva, M.. (2014, November 3). BE2 custom plugins, router abuse, and target profiles. https://papers.vx-underground.org/papers/Malware%20Defense/Malware%20Analysis/2014-11-03%20-%20BE2%20custom%20plugins,%20router%20abuse,%20and%20target%20profiles.pdf, (accessed August 15, 2022)

[31] Baumgartner, K. and Garnaeva, M.. (2015, February 17). BE2 extraordinary plugins, Siemens targeting, dev fails, https://papers.vx-underground.org/papers/Malware%20Defense/Malware%20Analysis/2015-02-17%20-%20BE2%20extraordinary%20plugins,%20Siemens%20targeting,%20dev%20fails.pdf , (accessed August 15, 2022)

[32] Cherepanov, A.. (2016, January 3). BlackEnergy by the SSHBearDoor: attacks against Ukrainian news media and electri, https://samples.vx-underground.org/APTs/2016/2016.01.03/Paper/Reference/blackenergy-sshbeardoor-details-2015-attacks-ukrainian-news-media-electric-industry.pdf, (accessed August 15, 2022)

[33] Booz, Allen and Hamilton, 2016, When The Lights Went Out. https://www.boozallen.com/content/dam/boozallen/documents/2016/09/ukraine-report-when-the-lights-went-out.pdf, (accessed August 15, 2022)

[34] Hultquist, J.. (2016, January 7). Sandworm Team and the Ukrainian Power Authority Attacks. https://ia601007.us.archive.org/31/items/Russia-Ukraine-Power-Cyber-War/SandwormTeamAndTheUkrainianPowerAuthority.pdf, (accessed August 15, 2022)

UK NCSC. (2020, October 19). UK exposes series of Russian cyber attacks against Olympic and Paralympic Games . https://www.gov.uk/government/news/uk-exposes-series-of-russian-cyber-attacks-against-olympic-and-paralympic-games, (accessed August 15, 2022)

[35] Secureworks. (2020, May 1). IRON VIKING Threat Profile. https://www.secureworks.com/research/threat-profiles/iron-viking,

[36] Anton Cherepanov. (2017, June 12). Win32/Industroyer: A new threat for industrial controls systems. (accessed August 15, 2022)

[37] Dragos Inc.. (2017, June 13). CRASHOVERRIDE Analysis of the Threat to Electric Grid Operations. https://www.welivesecurity.com/wp-content/uploads/2017/06/Win32_Industroyer.pdf, (accessed August 15, 2022)

[38] Joe Slowik. (2018, October 12). Anatomy of an Attack: Detecting and Defeating CRASHOVERRIDE., https://www.dragos.com/wp-content/uploads/CRASHOVERRIDE2018.pdf, (accessed August 15, 2022)

[39] Joe Slowik 2019, August 15 CRASHOVERRIDE: Reassessing the 2016 Ukraine Electric Power Event as a Protection-Focused Attack , https://dragos.com/wp-content/uploads/CRASHOVERRIDE.pdf, (accessed August 15, 2022)

[40] Dragos Inc. 2017, June 13 Industroyer - Dragos - 201706: Analysis of the Threat to Electic Grid Operations , https://www.dragos.com/wp-content/uploads/CrashOverride-01.pdf, (accessed August 15, 2022)

[41] Dragos 2018, October 12 Anatomy of an Attack: Detecting and Defeating CRASHOVERRIDE , https://www.dragos.com/resource/anatomy-of-an-attack-detecting-and-defeating-crashoverride/, (accessed August 15, 2022)