Cybersecurity Incident Report (CIR)
Conceptual Database Design Document

Gnanitha Garikipati & Shahriar Rahman Dipon

March 2024

This document outlines a conceptual database design for Cybersecurity Incident Reports (CIRs) that could be used by the Cybersecurity and Infrastructure Security Agency (CISA) to fulfil the requirements of the Cyber Incident Reporting for Critical Infrastructure Act of 2022 (CIRCIA).

1 Cybersecurity Incident Reports

All organizations covered by CIRCIA must report cybersecurity incidents to CISA. These reports will contain detailed information about each incident, and the information will be stored in the CIR database.

When a cybersecurity incident occurs, if it is detected, an individual from an affected organization will fill out a CIR and submit it to CISA. That person will then be listed as the point of contact (POC) for that incident, unless they specify another POC. So at most two people can be associated with any given report. If multiple reports are made about a single incident, there may be multiple POCs for the incident. When any report is made, if it is concerning an unrecorded incident, then a new incident record will be created. Otherwise, an existing incident record will be updated accordingly (some attributes may be automatically updated, but others will be updated by someone who manually reviews reports).

Organizations are either part of the critical infrastructure/private sector, the US Federal Government, a foreign government, a US State, Local, Tribal, or Territorial Government, an Information Sharing and Analysis Center, or they are individuals who, while they aren’t

technically organizations, can be affected by incidents similarly. An incident may also involve other organizations that are indirectly negatively impacted, or needed for support. The database will keep track of which involved organizations have been notified about the incident.

Information about the narrative and categorization of the incident will be recorded. This will include any specific techniques used by attackers, such as known malware (malicious code) or exploits to common software vulnerabilities. When malicious code is involved, information about antivirus software installed on the affected machines and the network activity of the virus may also be recorded. The database will also hold information about the impact of the incident, including known relevant details about hosts involved and/or data breached. Some details about the incident, such as specific IOCs (indicators of compromise), are not required in the records, but may be included in the incident narrative, if relevant.

This document presents the conceptual schema for the CIR database. It is organized into four sections. This section, section 1, is the introduction to the scope of the mini-world covered by the database. Section 2 contains the notation and definitions for the conceptual schema as found in the template document. Section 3 describes in detail the conceptual schema following the guidelines found in section 2. Section 4 lists the most important queries that may be posed to this specific database, as well as some additional example queries.

2 Notation and Definitions (taken from Dr. Soraya Abad Mota's template)

The notation used: all upper case for the entity names, lower case for the relationship names, and the first letter capitalized for attribute names.

The description of the entities starts with a sentence which explains their meaning. Then the attributes to describe the instances are included. The relationships are also described by a sentence and a list of attributes if they have them.

Each attribute has a four-letter code which describes the type of attribute according to the four classification criteria for attributes. The format for this code is: (xyzw), where

- x tells that the attribute is simple (S) or composite (C),
- y tells that the attribute has a single value (S) or is multivalued (M),
- z tells that the attribute is primitive (stored) (P) or derived (D), in case it is derived, an explanation of how to deduce it from other attributes or a formula/procedure must be specified, and
- w tells that the attribute is fixed (F) (i. e. it must have a value that is not null) or optional (O), i.e. the domain of the attribute allows the null value.

For example, an attribute that has the SSPF code is a simple attribute with a single value which is primitive and fixed. An example of this kind of attribute could be the Social Security Number (SSN). On the other hand, an attribute with the (CSPO) code is a composite attribute with a single value, primitive and optional. In this case, the date of birth could be an attribute with this code. If there is a single attribute that has the key constraint, it can be underlined. If the key constraint applies to more than one attribute or if there are several combinations of attributes with the key constraint property it is better to list them separately.

If there are attributes that are very common and are used more than once, they can be defined as general types to be used as the type of each attribute which uses the same format.

3 Conceptual Schema of the CIR Database

The order of presentation of the conceptual schema is:

1. The entities' descriptions, examples, and attributes.
2. The relationships' descriptions and, if they exist, attributes.
3. The EER diagram.

4. The semantic integrity constraints.

3.1 Entities

The entities defined for this database are:

- PERSON
- CONTACT
- INDIVIDUAL
- REPORT
- INCIDENT
- EXPLOIT
- MALWARE
- ANTIVIRUS
- NETWORK ACTIVITY
- IMPACT
- HOST
- DATA
- ORGANIZATION
- CRIT INFR/PRIV SECT
- US FED GOV
- FOREIGN GOV
- SLTT GOV
- ISAC

A detailed description of each entity follows.

PERSON: a person who is the submitter/POC for an incident or is an individual affected by an incident.

Attributes:

- Last_Name (SSPF)
- First_Name (SSPF)
- Phone (SSPF)
- Email (SSPF)

CONTACT: a subclass of Person; someone who submits a report or is the point of contact for a report.

Attributes:

- Job_Title (SSPF)
- Alt_Phone (SSPO)
- Mobile (SSPO)
- Pager (SSPO)
- Fax (SSPO)

INDIVIDUAL: a subclass of person; someone who is affected by an incident as an individual, not as part of an organization.

REPORT: A specific cybersecurity incident report submitted by a contact. Attributes

- Submission_Date/Time (CSPF)
- Estimated_Recovery_Time_Clock_Hours (SSPO)
- Estimated_Recovery_Time_Staff_Hours (SSPO)
- Estimated_Damage_Accounts ($$$ Loss) (SSPO)

INCIDENT: a specific cybersecurity incident; more than one report may be made about one incident.

Attributes:

- CISA_Incident_ID (assigned upon creation) (SSPF)

- Attack_Start_Date/Time (CSPF)
- Attack_First_Detected_Date/Time (CSPF)
- Incident_Narrative (SSPF)
- Attack_Ended (Y/N) (SSPF)
- Attack_Duration (in hours) (SSPF)
- Observed_Activity_Network_Location (SMPF)
- Attack_Vector (general cause of incident) (SSPF)
- Incident_Type (Phishing, DOS, Password Attack, etc.) (SSPF)
- Suspected_Perpetrator(s) (threat actor type) (SMPF)
- Disclosed_to_Public (Y/N) (SSPF)

EXPLOIT: a subclass of incident that exploits a known software vulnerability that has a CVE (Common Vulnerabilities and Exposures number).

Attributes:

- CVE (e.g. CVE-2019-0709) (SSPF)
- Common_Name (e.g. BlueKeep) (SSPO)

MALWARE: a subclass of incident that involves some kind of malware (malicious code).

Attributes:

- Type (Spyware, Trojan Horse, Worm, etc.) (SSPF)
- Name (DarkHotel, Emotet, Stuxnet, etc.) (SSPO)
- Signature (SSPO)
- Description (SSPF)

ANTIVIRUS: an instance of antivirus software that is encountered by malware.

Attributes:

- Antivirus_Name (SSPF)
- Detect_Malware (Y/N) (SSPF)

- Last_Updated (Date) (SSPF)

NETWORK ACTIVITY: an instance of the malware's network activity.

Attributes:

- Port_Number (SSPF)
- Protocol (TCP, UDP, etc.) (SSPF)
- Type (Source or Destination) (SSPF)

IMPACT: details about the specific impact of a specific cybersecurity incident. Attributes:

- Total_Impacted_Hosts (number) (SSPF)
- Total_Impacted_People (number) (SSPF)
- Total_Impacted_Records (number) (SSPF)
- Functional_Impact (support doc 1, page 4) (SSPF)
- Information_Impact (support doc 1, pages 4-5) (SSPF)
- Recoverability (support doc 1, page 5) (SSPF)
- Cross-Sector_Dependency (SSPF)
- Severity_Score (SSPF)
- Is_Major (Y/N) (SSPF)
- Potential_Impact (SSPF)
- Remediation_Steps_Taken (SSPO)
- Lessons_Learned (SSPO)

HOST: a specific host or group of hosts (bulk host) included in the impact of an incident.

Attributes:

- IP_Address(es) (SMPF)

- Host_Type (Attacking, Victim, or Both) (SSPF)
- Host_Name (SSPO)
- Affected_OS (SSPO)
- Affected_Applications (SSPO)
- Primary_Purpose (User Desktop, Web Server, etc.) (SSPO)

DATA: an instance of more detailed information about impacted data.

Attributes:

- Impacted_Records(number) (SSPF)
- Impact_Type (Access or Exposure) (SSPF)
- Relevant_Data_Type(s) (SSN, email, etc.) (SMPF)

ORGANIZATION: The union of all entities containing organizations that are either affected by or involved in incidents.

CRIT INFR/PRIV SECT: an organization in a Critical Infrastructure and/or Private Sector.

Attributes:

- Organization_or_Company_Name (SSPF)
- Org_Type (Hospital, University, etc.) (SSPF)
- Internal_Tracking_No (SSPO)

US FED GOV: an agency in the United States Federal Government.

Attributes:

- **Federal_Agency** (SSPF)
- **Subagency** (SSPF)
- Internal_Tracking_No (SSPO)

FOREIGN GOV: an agency in a foreign government.

Attributes:

- Country (SSPF)
- National_CSIRT (Y/N) (SSPF)
- Internal_Tracking_No (SSPO)

SLTT GOV: an agency in a US State, Local, Tribal, or Territorial Government.

Attributes:

- State (SSPF)
- SLTT_Organization_Name (SSPF)
- Organization_Name (SSPO)
- Internal_Tracking_No (SSPO)

ISAC: an organization that is an Information Sharing and Analysis Center.

Example: Financial Services ISAC

Attributes:

- **Subagency** (SSPF)
- Internal_Tracking_No (SSPO)

3.2 Relationships

There are four regular relationships (reports, updates/creates, affects, and involves), five identifying relationships (encounters, attacks_through, causes, includes, and breaches), two overlapping generalization/specializations, and one union in this schema. The regular and identifying relationships are described below.

reports: the relationship between a cybersecurity incident report and the person who submitted it/is the POC for it.

Attributes:

- Reporter_Type (Submitter, POC, or Both) (SSPF)

updates/creates: the relationship between an incident and a report that updates or creates it.

encounters: the relationship between malware and any antivirus it encounters that is installed on the affected machines.

attacks_through: the relationship between malware and the network activity it attacks through.

causes: relationship between an incident and the impact it causes. **includes:** the relationship between an incident's impact and the host(s) included in it.

breaches: the relationship between an incident's impact and a specific set of relevant data breached by it.

affects: the relationship between an incident and an organization that is affected by it.

Attributes:

- Primary_Affected_Sector (SSPO*)
- Location (address of incident location for organization) (CSPF)

involves: the relationship between an incident and an organization that is involved with it because it is indirectly impacted, a supporting organization, or both.

Attributes:

- Involvement_Type (Indirectly Impacted, Supporting, or Both) (SSPF)
- Notified (Y/N) (SSPF)

3.2 Semantic Integrity Constraints

1. The Primary Affected Sector attribute of the Affects relationship is fixed if the Organization is Crit Infr/Priv Sect, and optional otherwise.

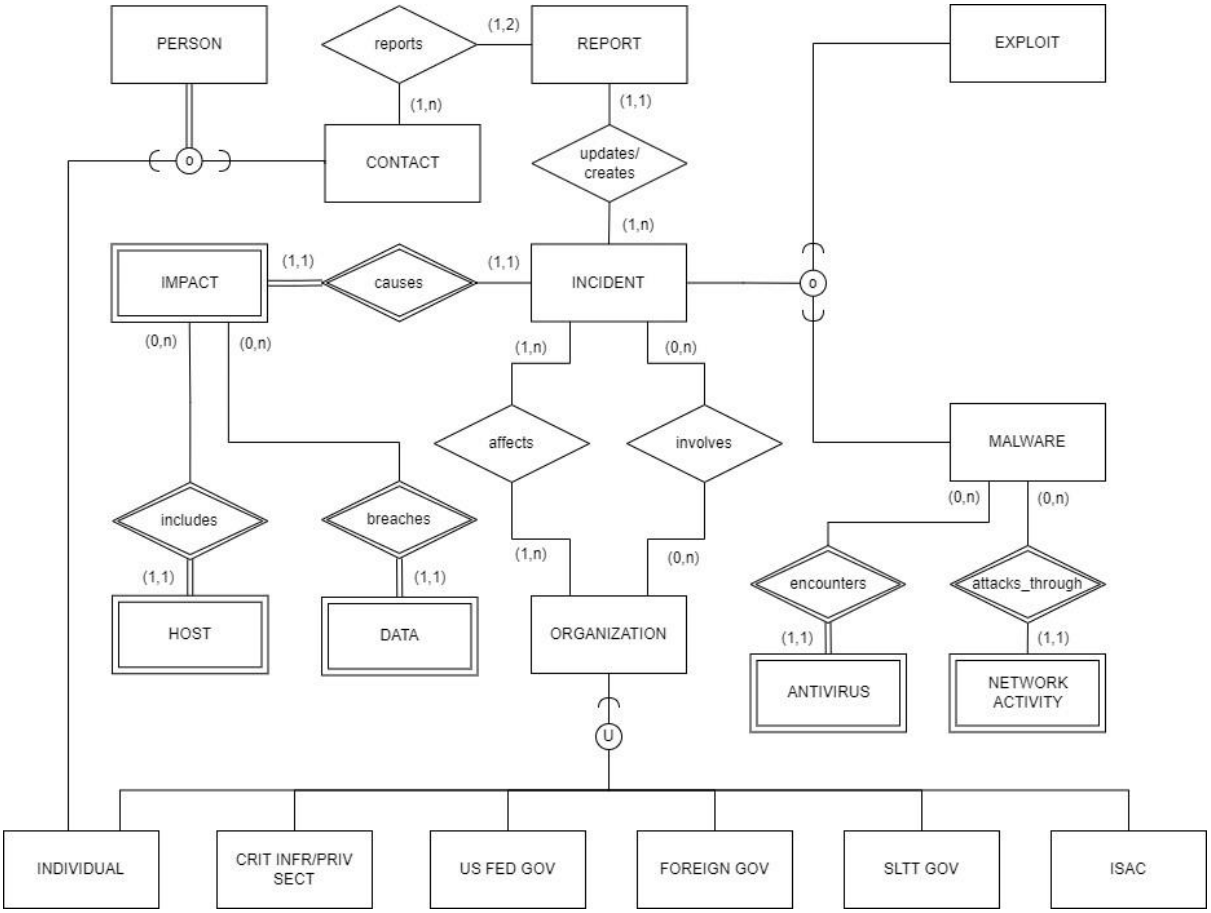

Figure 1: The EER Diagram of CIR Database

4 Example Queries

1. Kinds of CIR more prevalent at US universities in the past 2 years, 4 years, and 10 years.
2. Statistics of CIRs reported by specific organizations.
3. List the most important cybersecurity incidents that occur in the US in the past year. Most important could mean the number of people or institutions affected, or severity of the attack.
4. Which are new cybersecurity incidents which occurred in the past year.
5. Find a specific cybersecurity incident report given its type, description, and affected organization, or CISA Incident ID number.

6. Find all the cybersecurity incident reports by the malicious code with the same signature.
7. Provide statistics by different criteria of all the CIRs reported in a specific period of time.
8. Summarize all the attacks of a specific type that have occurred to a specific organization or type of organization during their lifetime or in a specific period of time.
9. List all the organizations and their classification (federal, government, tribal, etc.) that have reported cybersecurity incidents, how many and of which kind.
10. List all the cybersecurity incidents which have been reported by type and in descending order of the number of incidents.
11. List all incidents that involved the exploitation of a particular known software vulnerability (CVE).
12. List all incidents that a specific person either submitted a report for, is listed as the POC for, or was affected by as an individual.
13. List incidents where a specific type of data (SSN, for instance) was accessed without authorization, and tell how many records were impacted.
14. Show statistics for attacks utilizing a specific type of malware (Ransomware, for instance), including which antivirus software detected the malware and what kinds of protocols the malware was active in.

5 The Logical Relation Schema (LRS) for the Cybersecurity Incident Report (CIR) Database

The conceptual schema described for the Company Database is mapped into the Relational Schema presented in this section. All the attributes underlined in the same Relation belong to the primary key. By default, all the attributes that do not belong to the primary key may be null, unless explicitly specified otherwise.

ORGANIZATION (*Victim_ID*)

The *Victim_ID* is an artificial or surrogate key for ORGANIZATION and may not be null.

Domains:	Victim_ID	Unique identifier

CRIT INFR/PRIV SECT (*Organization_or_Company_Name, Org_Type, Internal_Tracking_No, Victim_ID)*

The *Victim_ID* is a foreign key references to ORGANIZATION and may not be null.

Domains:	Organization_or_Company_Name	Name of the Company or the Organization
	Org_Type	Organization type like Hospital, University, etc.
	Internal_Tracking_No	An auto generated number
Foreign Key:	Victim_ID	

US FED GOV (*Federal_Agency, FSubagency, Internal_Tracking_No, Victim_ID)*

The *Victim_ID* is a foreign key references to ORGANIZATION and may not be null.

Domains:	Federal_Agency	Name of the federal agency
	FSubagency	Name of associated sub-agency
	Internal_Tracking_No	An auto generated number
Foreign Key:	Victim_ID	

FORIEGN GOV (*Country, National_CSIRT, Internal_Tracking_No, Victim_ID)*

The *Victim_ID* is a foreign key references to ORGANIZATION and may not be null.

Domains:	Country	Name of the country
	National_CSIRT	Yes/No
	Internal_Tracking_No	An auto generated number
Foreign Key:	Victim_ID	

SLTT GOV (*Subagency, Internal_Tracking_No, Victim_ID)*

The *Victim_ID* is a foreign key references to ORGANIZATION and may not be null.

Domains:	Subagency	Name of the sub-agency associated
	Internal_Tracking_No	An auto generated number
Foreign Key:	Victim_ID	

INDIVIDUAL (*Last_Name, First_Name, SSN, Phone, Email, Victim_ID)*

INDIVIDUAL is a shared sub-class for both PERSON and ORGANIZATION. So, it has a superkey and foreign key from PERSON and the *Victim_ID* is a foreign key references ORGANIZATION.

Domains:	Last_Name	Name of the person
	First_Name	Name of the person
	SSN	9 digit number
	Phone	10 digit phone number
	Email	Email address of the person
Foreign Key:	Victim_ID	

CONTACT (*Last_Name, First_Name, Phone, Email, Job_Title, Alt_Phone, Mobile, Pager, Fax)*

Last_Name, First_Name, Phone, Email is a superkey and foreign key references to PERSON.

Domains:	Last_Name	Name of the person
	First_Name	Name of the person
	Phone	10 digit phone number
	Email	Email address of the person
	Job_Title	Tile of the job associated with the person
	Alt_Phone	Alternative 10 digit phone number
	Mobile	10 digit mobile number
	Pager	Numeric/alphanumeric code for pager
	Fax	Numeric fax number

REPORT (*Report_ID, Submission_Date, Submission_Time, Estimated_Recovery_Time,_Clock_Hours, Estimated_Recovery_Time_Staff_Hours, Estimated_Damage_Accounts, CISA_Incident_ID)*

Report_ID is an artificial key and primary key of REPORT, *CISA_Incident_ID* is the foreign key references INCIDENT and may not be null.

Domains:	Submission_Date	Date formatted MM/DD/YYYY
	Submission_Time	Time formatted HH:MM (24 hour format)
	Estimated_Recovery_Time_Clock_Hours	Number of hours (number)
	Estimated_Recovery_Time_Staff_Hours	Number of hours (number)
	Estimated_Damage_Accounts ($$$ Loss)	Money lost (number)
Foreign Key:	*CISA_Incident_ID*	

INCIDENT (*CISA_Incident_ID, Attack_Start_Date, Attack_Start_Time, Attack_First_Detected_Date, Attack_First_Detected_Time, Incident_Narrative, Attack_Ended, Attack_Duration, Attack_Vector, Incident_Type, EFlag, CVE, Common_Name, MFlag, Type, Name, Signature, Description)*

INCIDENT has two sub classes EXPLOIT and MALWARE, with overlapping relation between them, So here the single relation with multiple attributes is considered, with *EFlag* and *MFlag* as Boolean flags for EXPLOIT and MALWARE respectively.

Domains:	CISA_Incident_ID	An auto generated number
	Attack_Start_Date	Date formatted MM/DD/YYYY
	Attack_Start_Time	Time formatted HH:MM (24 hour format)
	Attack_First_Detected_Date	Date formatted MM/DD/YYYY
	Attack_First_Detected_Time	Time formatted HH:MM (24 hour format)
	Incident_Narrative	Description of the incident occurred (text)
	Attack_Ended	Yes/No
	Attack_Duration	Number of hours (number)
	Attack_Vector	Cause of the incident, like web, attrition, etc.
	Incident_Type	Type of Incident like, DDOS, phishing, Password Attack, etc.
	EFlag	Boolean value (1 or 0)
	CVE	The number associated with the CVE, unique for every exploit
	Common_Name	Name of the exploit
	MFlag	Boolean value (1 or 0)
	Type	Type of the malware like, Spyware, Trojan, Virus, etc.

	Name	Name of the malware like DarkHotel, Emotel, Stuxnet, etc.
	Signature	Pattern associated with malware like bitstream
	Description	Description of the malware

OBSERVED_ACTIVITY_NETWORK_LOCATION (*CISA_Incident_ID, Location_Area)*

OBSERVED_ACTIVITY_NETWORK_LOCATION is a multivalued attribute of the INCIDENT, *CISA_Incident_ID,* is foreign key references INCIDENT.

Domains:	CISA_Incident_ID	An auto generated number referenced from INCIDENT
	Location_Area	Part of the network name where the activity was observed
Foreign Key:	CISA_Incident_ID	

SUSPECTED_PERPETRATORS (*CISA_Incident_ID, Perpetrators)*

SUSPECTED_PERPETRATORS is a multivalued attribute of the INCIDENT, *CISA_Incident_ID,* is foreign key references INCIDENT.

Domains:	CISA_Incident_ID	An auto generated number referenced from INCIDENT
	Perpetrators	Type of the treat actor
Foreign Key:	CISA_Incident_ID	

ANTIVIRUS (*CISA_Incident_ID, Antivirus_Name, Detect_Malware, Last_Updated)*

ANTIVIRUS is weak entity of MALWARE, *CISA_Incident_ID,* is foreign key references INCIDENT relation.

Domains:	CISA_Incident_ID	An auto generated number referenced from INCIDENT

	Antivirus_Name	Name of the Antivirus like, McAfee, Avast etc.
	Detect_Malware	Boolean entry; indicate if malware detected or not
	Last_Updated	Date formatted MM/DD/YYYY
Foreign Key:	CISA_Incident_ID	

NETWORK_ACTIVITY (*CISA_Incident_ID, Port_Number, Protocol, Type)*

NETWORK_ACTIVITY is weak entity of MALWARE, *CISA_Incident_ID,* is foreign key references INCIDENT relation.

Domains:	CISA_Incident_ID	An auto generated number referenced from INCIDENT
	Port_Number	Number of the port to which the network is associated to.
	Protocol	Communication protocol used for network activity for the reported incident like, TCP, UDP
	Type	Source/ Destination
Foreign Key:	CISA_Incident_ID	

IMPACT (*CISA_Incident_ID*, *Imapct_ID*, *Total_Impacted_Hosts, Total_Impacted_People, Total_Impacted_Records, Functional_Impact, Informational_Impact, Recoverability, Cross-Sector_Dependency, Severity_Score, Is_Major)*

IMPACT is a weak entity of the INCIDENT, *CISA_Incident_ID,* is foreign key references INCIDENT relation and included an artificial key *Imapct_ID.*

Domains:	CISA_Incident_ID	An auto generated number referenced from INCIDENT

Impact_ID	A number assigned to the impact report
Total_Imoacted_Hosts	Number of hosts got affected
Total_Impacted_People	Number of people affected
Functional_Impact	The current level of impact on agency functions or services, refer apendix
Information_Impact	The type of information lost, compromised, or corrupted, refer apendix
Recoverability	Description of estimation of time and resources needed to recover from the incident, refer apendix
Cross-Sector_Dependency	Whether the incident is depended on any other incidents, its description.
Severity_Score	A number indicating the level of severity
Is_Major (Y/N)	Boolean entry; Yes/No
Potential_Impact	The estimated impact level for the nation. (text)
Remediation_Steps_Taken	If known can mention the mitigation activity steps
Lessons_Learned	Optional

Foreign Key: CISA_Incident_ID

HOST (*CISA_Incident_ID, Impact_ID, Host_Name, Host_Type, Affected_OS, Affected_Applications, Primary_Purpose)*

HOST is a weak entity of the IMPACT, *CISA_Incident_ID,* is foreign key references INCIDENT relation and *Impact_ID* is a foreign key reference to IMPACT relation.

Domains:	CISA_Incident_ID	An auto generated number referenced from INCIDENT
	Impact_ID	Number assigned to impact report and is referenced from IMPACT
	Host_Type (Attacking, Victim, or Both)	Depiction of the host being a victim or attacker
	Host_Name	Name of host
	Affected_OS	Affected operating system in use
	Affected_Applications	Applications affected
	Primary_Purpose (User Desktop, Web Server, etc.)	Purpose of the victim machine in use
Foreign Key:	CISA_Incident_ID, Impact_ID	

DATA (*CISA_Incident_ID, Impact_ID, Imapcted_Records, Impact_Type, Relevant_Data_Types)*

DATA is a weak entity of the IMPACT, *CISA_Incident_ID,* is foreign key references INCIDENT relation and *Impact_ID* is a foreign key reference to IMPACT relation.

Domains:	CISA_Incident_ID	An auto generated number referenced from INCIDENT
	Impact_ID	Number assigned to impact report and is referenced from IMPACT
	Impacted_Records	Number of records impacted
	Impact_Type	Access/Exposure
Foreign Key:	CISA_Incident_ID, Impact_ID	

IP ADDRESS (*CISA_Incident_ID, Impact_ID, Host_Name, IP_Address)*

IP ADDRESS is a multivalued attribute of the HOST, *CISA_Incident_ID,* is foreign key references INCIDENT relation, *Impact_ID* is a foreign key reference to IMPACT relation, *Host_Name* is a foreign key reference to HOST relation.

Domains:	CISA_Incident_ID	An auto generated number referenced from INCIDENT
	Impact_ID	Number assigned to impact report and is referenced from IMPACT
	Host_Name	Identifier assigned to a device connected to a network
Foreign Key:	CISA_Incident_ID, Impact_ID	

RELEVANT DATA TYPE (*CISA_Incident_ID, Impact_ID, Impacted_Type, Data_Type)*

RELEVANT DATA TYPE is a multivalued attribute of the DATA. *CISA_Incident_ID,* is foreign key references INCIDENT relation, *Impact_ID* is a foreign key reference to IMPACT relation, *Impacted_Type* is a foreign key reference to DATA relation.

Domains:	CISA_Incident_ID	An auto generated number referenced from INCIDENT
	Impact_ID	Number assigned to impact report and is referenced from IMPACT
	Impacted_Type	Access/Exposure
	Data_Type	Data type like SSN, email, etc.
Foreign Key:	CISA_Incident_ID, Impact_ID, Impacted_Type	

reports (*Last_Name, First_Name, Phone, Email, Job_Title, Alt_Phone , Reporter_Type,)*

{Last_Name, First_Name, Phone, Email, Job_Title, Alt_Phone} is foreign key from CONTACT relation.

Domains:	Last_Name	Name of the reporting person

	First_Name	Name of the reporting person
	Phone	10-digit phone number of reporting person
	Email	Email address of reporting person
	Job_Title	Job designation of the reporting person
	Alt_Phone	10 digit phone number
	Reporter_Type	Submitter/POC/Both
Foreign Key:	Last_Name, First_Name, Phone, Email, Job_Title, Alt_Phone	

affects (*CISA_Incident_ID, Victim_ID, Primary_Affcted_Sector, Location_Address, Location_Contact_Information)*

CISA_Incident_ID, Victim_ID are the foreign key that refer to INCIDENT and ORGNIZATION.

Domains:	CISA_Incident_ID	An auto generated number referenced from INCIDENT
	Victim_ID	An auto generated number referenced from ORGANIZATION
	Primary_Affected_Sector	Name of the sector
	Location_Address	Address of the affected organization
	Location_Contact_Information	Contact information of the affected organization
Foreign Key(s):	CISA_Incident_ID, Victim_ID	

involves (*CISA_Incident_ID, Victim_ID, Involvement_Type, Notified)*

CISA_Incident_ID, Victim_ID are foreign key that refer to INCIDENT and ORGNIZATION.

Domains:	CISA_Incident_ID	An auto generated number referenced from INCIDENT
	Victim_ID	An auto generated number referenced from ORGANIZATION
	Involvement_Type	Indirectly/Supporting/Both
	Notified	Yes/No
Foreign Key(s):	CISA_Incident_ID, Victim_ID	

6 Additional Integrity Constraints for Relational Schema

1. Attack_Start_Date >= Attack_First_Detected_Date
2. Attack_Start_Time>= Attack_First_Detected_Time
3. The levels of the impact(functional, informational, recoverability) should be one of those given in the appendix.
4. Host_Name is unique to every host.
5. Antivirus_Name is unique.
6. Organization ID has different values for different types.
7. The Organization_ID is different accordingly to the subclass it is part of. For individual- it is the social security number, for private business- it is the registration number, for foreign government- it is the name of the country that is recognized by the US.

7 Domain Definition and Constraints

1. The Domain date should be in the format MM/DD/YYYY for all the dates in the schema.

2. The phone number should be formatted as +(country_code) (Area_Code)-(XXX)-(XXXX)

8 Possible Extensions and Additional Comments

1. Can incorporate support for storing and retrieving multimedia data, like images, videos and audio files within database.
2. Can convert this database into a graph database for better statistical analysis of the incidents and attacks occurred over years.
3. Integrating the database with cloud extension helps in storing and backing up the data efficiently.
4. Security enhancement could be carried out by encrypting the database to prevent unauthorized access.
5. Incorporating Machine Learning techniques helps to identify the underlying patterns among various data.
6. Developing a web application helps in integrating with other services and data entry is made easier.

9 Appendix

1. Functional Impact levels depends on following categories based on US-CERT

- NO IMPACT – Event has no impact
- NO IMPACT TO SERVICES – Event has no impact to any business or Industrial Control Systems (ICS) services or delivery to entity customers.
- MINIMAL IMPACT TO NON-CRITICAL SERVICES – Some small level of impact to noncritical systems and services.
- MINIMAL IMPACT TO CRITICAL SERVICES –Minimal impact but to a critical system or service, such as email or active directory.
- SIGNIFICANT IMPACT TO NON-CRITICAL SERVICES – A non-critical service or system has a significant impact.

- DENIAL OF NON-CRITICAL SERVICES – A non-critical system is denied or destroyed.
- SIGNIFICANT IMPACT TO CRITICAL SERVICES – A critical system has a significant impact, such as local administrative account compromise.
- DENIAL OF CRITICAL SERVICES/LOSS OF CONTROL – A critical system has been rendered unavailable.

2. Informational Impact levels depends on following categories based on US-CERT

- NO IMPACT – No known data impact.
- SUSPECTED BUT NOT IDENTIFIED – A data loss or impact to availability is suspected, but no direct confirmation exists.
- PRIVACY DATA BREACH – The confidentiality of personally identifiable information (PII6) or personal health information (PHI) was compromised.
- PROPRIETARY INFORMATION BREACH –The confidentiality of unclassified proprietary information7, such as protected critical infrastructure information (PCII), intellectual property, or trade secrets was compromised.
- DESTRUCTION OF NON-CRITICAL SYSTEMS – Destructive techniques, such as master boot record (MBR) overwrite; have been used against a non-critical system.
- CRITICAL SYSTEMS DATA BREACH – Data pertaining to a critical system has been exfiltrated.
- CORE CREDENTIAL COMPROMISE – Core system credentials (such as domain or enterprise administrative credentials) or credentials for critical systems have been exfiltrated.
- DESTRUCTION OF CRITICAL SYSTEM – Destructive techniques, such as MBR overwrite; have been used against a critical system.

3. Recoverability Impact levels can be one of the 4 listed below,

- REGULAR - Time to recovery is predictable with existing resources.
- SUPPLEMENTED – Time to recovery is predictable with additional resources.
- EXTENDED – Time to recovery is unpredictable; additional resources and outside help are needed.
- NOT RECOVERABLE – Recovery from the incident is not possible (e.g., sensitive data exfiltrated and posted publicly).

References

- https://www.cisa.gov/sites/default/files/publications/Federal_Incident_Notificati o n_Guidelines.pdfLinks to an external site.
- In the news, the need for a common platform for reportingLinks to an external site.
- Sharing_Cyber_Event_Information_Fact_Sheet_FINAL_v4.pdf
- CIRCIALinks to an external site.

ACKNOWLEDGEMENT

We would like to thank Dr. Soraya Abad-Mota for her feedback. We would also like to thank Nathaniel Filer and Gabriel Urbaitis for their resources provided. The logical schema is based upon their conceptual schema. The introduction, section 1, 3, and 5 are from their report.