CYBER INCIDENT REPORTING FRAMEWORK: GLOBAL EDITION

Cyber Threat Alliance

Institute for Security and Technology

Chainalysis

Ciphertrace

CREST

Cybera

Cybercrime Support Network

CyberPeace Institute

MARCH 2023

Last fall, multiple industry organizations led by the Cyber Threat Alliance (CTA) and the Institute for Security and Technology (IST) came together to provide input regarding cyber incident reporting for US entities This group identified a set of principles and developed a model reporting format that the Cybersecurity and Infrastructure Security Agency (CISA) could use as the foundation for its incident reporting regulations. The updated, global edition of the framework presented here builds off that first document that CTA and IST released in November 2022, and adds significant contextual discussion. It develops a model reporting format that cybersecurity authorities and other government authorities worldwide could use as the foundation for their national reporting frameworks and regulatory language. CTA and IST wish to thank the contributing organizations, including the drafters and co-sponsors of the documents.

Table of Contents

Section 1: Purpose, Expectations, and Definitions **4**

- Audience 4
- Deciding whether to require reporting 4
- Purpose 5
- Expectations 6

Section 2: Principles **8**

Section 3: Incident Reporting Fields **10**

- Layer 1: General information fields applicable to all incidents 11
- Layer 2: Incident-specific information fields (fields change based on incident type) 12
- Layer 3: Additional technical information fields (NCAs should designate this section as optional or provide guidance as to which entities must provide this information) 15

Appendix A: Why national cybersecurity authorities would request the information in the proposed Cyber Incident **16**

Appendix B: Example Incident Report **23**

Section 1: Purpose, Expectations, and Definitions

Audience

This guide to national cybersecurity incident reporting provides input to national cybersecurity authorities (NCAs) and legislative bodies as they consider implementing a range of mandates and voluntary reporting procedures for cybersecurity incidents. As used in this guide, the term national cybersecurity authorities (NCAs) refers to the primary national government entity that has responsibility to support the cybersecurity practices of private sector entities and/or government ministries, departments, and agencies. NCAs may have a range of different titles, mandates, and legal authorities, and their choice of whether or not to implement a reporting requirement will depend on those authorities, as well as the capacity of relevant incident handling teams and the maturity of cybersecurity threat information sharing.

This guide may also be useful for government entities that have mandates relating to reporting data breaches, such as national data protection agencies and ministries of communication, and those that have a role to play in the cybersecurity of specific sectors (e.g., banking regulators). Regional organizations that share best practices and/or create regional cybersecurity regulatory mandates for their member states may also find this guide useful. We encourage all governments to work towards a harmonized national and global approach to cybersecurity incident reporting.

Deciding whether to require reporting

Governments considering a reporting requirement should be aware of the likely tradeoffs and that effective reporting frameworks require substantial investments in national incident report response capabilities. When determining whether to implement a reporting requirement, policymakers should consider whether the below conditions are in place. Requirements for reporting without these conditions may lead to poor quality in reporting and reduce the openness of the multistakeholder community to collaboration.

The first condition is trust between government and private industry. This means that all entities respect commitments with regard to the confidentiality of information, such as adherence to policies like the Traffic Light Protocol (TLP) and implementation of effective anonymization before sharing vulnerability data. NCAs should build both procedures and policies that promote trust between actors in the system before implementing a mandatory reporting framework.

Second, reporting entities should feel confident that reporting will do some good. In order for the reporting requirement to provide mutual benefit, the government entity receiving the reporting should have both the technical capacity and the trusted relationships to use the information in a way that will be beneficial to the overall cybersecurity community. Such benefits include activities like sharing information about vulnerabilities (so long as it does not cause unexpected exposure of sourcing) within voluntary groups, industry-specific computer security incident response teams (CSIRTs), or information and analysis centers (ISACs). Implementing such processes may require substantial investment in government cybersecurity capacity, most importantly investment in workforce development.

In many cases, governments may find that encouraging voluntary exchange of information may be more helpful than instituting reporting mandates for advancing national cybersecurity goals, either for a capacity-building period or over the long term.

This document is intended to facilitate discussions when governments have decided to implement a mandatory requirement. We encourage governments to consult with the entire multistakeholder community, including private industry, the technical and academic community, and civil society, before deciding to move forward with implementing a mandatory reporting requirement.

Purpose

Incident reporting can serve multiple purposes. We recommend that NCAs identify the goals and purposes of any reporting requirement in advance of developing these requirements. The purposes and goals of the requirement should be consistent with national law, as well as global best practices for information sharing between cybersecurity network defenders. Since different purposes for implementing reporting requirements require the collection of varying degrees of granularity of information, NCAs should specify the use cases as part of the description of the reporting requirement. Such purposes can include:

Trend Identification: Collecting data across multiple incidents at multiple companies could allow governments to better understand adversary activities in the aggregate and identify trends in adversary activities, such as victim, mission, and sector targeting.

Indication and Warning: Reporting could allow governments to warn similarly situated organizations about impending threats.

Response: Reporting could be used to drive asset and/or threat response activities (such as those described by national cybersecurity incident response plans, e.g. the U.S.'s Presidential Policy Directive-41 and the French Critical Infrastructure Protection Program) and inform policy discussions including about the effectiveness of deployed strategies.

Assessing Impact and Harm: Reporting could contribute to a better understanding of the

harm cyber incidents cause to targeted organizations, individuals, and society.

Expectations

NCAs should provide guidance surrounding any cybersecurity incident reporting mandates with the goal of setting clear expectations on several topics.

What Happens After Reporting an Incident: NCAs should acknowledge that the report has been received, and organizations should expect to receive such confirmation. Beyond this acknowledgement, however, guidance should also make clear what will not necessarily happen; for example, just because a company reports an incident does not mean that law enforcement agencies will open a case. If the government's response does not align with expectations, the reporting requirement could be seen as a failure.

Information Distribution and Handling: NCAs should indicate to the reporting entity how they will use the data, how they will protect any information provided (including the identity of the reporting entity), and what other government entities could receive the reported data under what conditions.

Scope of Reporting Mandates

In defining which entities should be covered by a reporting mandate, NCAs may wish to consider a variety of factors. Whether an entity is part of critical infrastructure, as defined by national cybersecurity strategies or other foundational policy documents, should be a primary area of consideration. Additionally, NCAs should consider the size of the entity and their ability to access and implement cybersecurity best practices. Determination of the scope of reporting mandates should be done in consultation with relevant industry leaders and sector-specific government regulators; governments may also benefit from broad public consultation to best scope the mandate. Governments should also send clear signals that they welcome voluntary reporting from non-covered entities and indicate how to make such voluntary reports.

Consistent with this approach, we offer one possible definition of a covered entity:

> *A covered entity is an entity that owns or operates an information technology (IT), operational technology (OT), other digital system, or social media account in one or more of the critical sectors defined by the published national cybersecurity strategy and has:*
>
> - *"More than 50 employees,*
> - *More than 1,000 customers, or*
> - *Revenues greater than a nationally relevant threshold.*

Beyond the definition, ensuring that every organization knows whether or not it is a covered entity is a challenge. National cybersecurity authorities, ideally in collaboration with sector-specific government entities, should implement broad awareness campaigns among

business leaders and relevant trade councils to inform as many organizations as possible about their reporting obligations. Further, some organizations may ask the government to provide them with guidance about whether they are a covered entity, so NCAs should be prepared to handle such inquiries.

Determining Which Incidents to Report

A key issue in incident reporting is determining which ones should be reported. Reporting too many incidents generates too much "noise" and obscures the signal; reporting too few incidents risks missing important events or trends. Therefore, governments should carefully consider what threshold to set for incident reporting.

To strike the right balance, governments should generally exclude cyber events that do not cause any or very minimal harm (such as a failed login attempt). Governments want to capture the incidents that matter, both to the affected organization and a region or country as a whole. The term used for such occurrences is a "significant" or "substantial" cyber incident. We offer two potential definitions for consideration below.

As part of the U.S. Department of Homeland Security request for information process, we offered the following definition of substantial cyber incident:

> *A substantial cyber incident is one that causes:*
>
> - *An undesired effect on an IT, OT, or other digital system; and,*
> - *Material loss of, compromise in, unauthorized access to, or denial of access to:*
>   - *Sensitive non-public data, personally identifiable information, intellectual property, or trade secrets;*
>   - *Revenue, income, or assets;*
>   - *Business operations or system functionality; or,*
>   - *Brand or corporate reputation.*

An alternative formulation, based on definitions used in the United Kingdom and in accord with the EU NIS 2 definitions, would be:

> *A substantial cyber incident is one in which:*
>
> - *The availability, authenticity, integrity or confidentiality of stored, transmitted or processed data or of the services offered by, or accessible via, network and information systems is compromised; and*
> - *One of the below thresholds is met:*
>   - *Service was unavailable for a nationally relevant number of user hours, where user hours are defined as the number of users domestically who were unable to access the service for a duration of 60 minutes;*
>   - *The incident resulted in a loss of integrity, authenticity or confidentiality of the data your service stores or transmit, or the related services you*

offer or make available via your systems, and this affected a nationally relevant threshold of users;
- *The incident caused loss of intellectual property or trade secrets of at least one domestic user;*
- *The incident created a reasonable risk of harms to public safety, public security, or loss of life; and/or*
- *The incident caused material damage to at least one domestic user and the damage to that user exceeded a nationally relevant monetary threshold.*

Section 2: Principles

In developing incident reporting requirements, we recommend that NCAs and sector-specific regulators incorporate the following principles. Following these principles will advance the quality, quantity, and utility of the reporting while minimizing the burden on the covered entities.

Reporting Culture: NCAs should encourage all businesses to report substantial cyber incidents, regardless of whether they are subject to the mandatory reporting requirement. Implementing this recommendation will require sustained public engagement and awareness efforts, as well as a commitment to demonstrate the value of reporting through providing follow up and benefits in the form of ongoing exchange of information between governments and non-government entities. NCAs should also be explicit in their public-facing documents, such as reporting checklists, that they welcome voluntary reporting.

Sharing Between Relevant Government Entities: NCAs should consider explicit mandates in their reporting structures to share information between NCAs and other relevant government entities, such as sector specific regulators and national ministries of communication. Any guidance should make clear how that information will be shared between government entities, in order to increase transparency and trust between government and entities that make reports. Governments should commit to following these guidelines, and build out mechanisms to facilitate this sharing securely.

Equivalence and Interoperability: Many organizations are subject to multiple reporting requirements, both within and between countries. NCAs should standardize incident reporting forms across government agencies to the maximum extent possible; however, for governments that have substantial existing reporting requirements, such as requirements under user data protection commissions or similar entities, achieving such standardization will take time. These governments may wish to allow organizations to submit incident reports using the format required by other agencies to reduce the burden on entities that are suffering from a breach.

Harmonization: All NCAs should promote harmonization of reporting requirements domestically and internationally. Greater standardization would make it easier to aggregate data, analyze trends, and recover ransoms; it would also reduce the burden on reporting

entities. As the number of countries with reporting requirements increases, having internationally recognized standards would be extremely beneficial to companies operating in multiple jurisdictions. Such standardization would also enable intelligence sharing among countries.

Usability and Accessibility: Incident reporting forms should be as easy to use and accessible as possible (such as having drop down fields or pre-populated defaults). Having the forms be available and filed through an on-line portal is critical, as well as having mobile versions and an application programming interface (API) for machine readable submissions. Many organizations lack access to sophisticated cybersecurity practitioners, and those experiencing a significant cyber incident have limited time and capacity to meet reporting requirements. Governments should minimize the burden on covered entities in these situations. Further, the shorter and easier the incident reporting form is to fill out, the more likely non-covered entities are to voluntarily report cyber incidents.

Security and Confidentiality: NCAs should secure the incident reporting system and associated data, incorporating minimization, anonymization, and aggregation as appropriate. NCAs should also specify whether any information in the reporting system falls under existing or additional levels of protection, such as Protected Critical Infrastructure Information (PCII). In addition, NCAs should be transparent about the mechanisms to maintain privacy for any information shared as part of the incident reporting process. NCAs should also specify how long they will retain the reported information and at what level of detail. This system should have a comprehensive security audit before launch. Finally, since organizations should not report incidents from networks reasonably believed to be compromised, allowing reports to come from alternative channels, such as forensic investigators or relevant computer security incident response teams or industry groups, will be beneficial.

Automation: The incident reporting process should be automated using accepted government and industry standards, such as the Structured Threat Intelligence eXchange (STIX) or the U.S. National Information Exchange Model (NIEM). Parties involved in automated intelligence sharing should routinely meet to provide feedback on the quality of information exchanged and review effectiveness.

Relevance: NCAs should develop a limited, core set of fields that every reporting entity must answer. Beyond the core questions, the reporting form should have different fields depending on the incident being reported. Finally, formats should be expandable to include additional technical fields, based on criteria such as the size and/or technical capability of the reporting entity, the severity of the reported incident, or other factors. If NCAs determine that the scale and impact of the reported incident warrants follow up, then guiding principles and practices should allow it to request additional information from the reporting entity.

Timing of Mandated Reports: While existing government reporting requirements vary between jurisdictions, NCAs should consider tradeoffs between short reporting periods, which allow for quick reports with limited details, or a longer period before reporting is mandated, which allows for more thorough reporting. In considering timeframes, NCAs should strongly consider harmonizing with existing reporting requirements from relevant neighboring governments or key

trading partners. For example, governments within a digital single market should consider harmonizing timeframes to allow companies to provide reporting to multiple national governments at the same time. Examples of existing reporting requirements include the United States, which will require reporting to CISA within 72 hours from the time the entity reasonably believes the incident occurred; and the European NIS 2.0, with a 24 hour reporting requirement.

Iteration: The details regarding a cyber incident will evolve over time and the affected organizations will learn more as the incident response continues. Therefore, NCAs should expect that incident reports will change over time, sometimes substantially from the initial one. The reporting process should incentivize organizations to update their previous reports as they learn more. Updates should be made upon discovering a material shift in previously reported information. NCAs should consider whether to set subsequent reporting deadlines in the regulation, such as requiring a final report no more than six months after an incident is considered resolved.

No Third-Party Liability or Obligations: The implementing regulation should clarify that third parties have no obligation to report a cyber incident independent of the covered entity. NCAs should also clarify whether reporting to a national CSIRT will continue to count as reporting the incident in sectors where such reporting has been the standard in the past.

No Automatic Trigger: NCAs should make clear that filing a report under a mandatory incident reporting framework does not necessarily trigger other reporting requirements under separate regulations or mandates. Organizations will have to determine whether to file reports with other regulatory bodies or agencies based on those reporting requirements, not just because the incident qualified for a report under this NCA reporting framework.

Section 3: Incident Reporting Fields

Consistent with the principles in Section 2, the incident reporting system forms should have multiple layers. The first layer should contain fields applicable to all incidents and that could be filled out by non-experts. The second layer should contain incident specific fields that would differ depending on the incident type. The third layer should contain fields to collect technical information from cybersecurity professionals; this layer would be optional depending on whether the reporting entity has access to the requisite expertise. This framework provides sample fields for consideration by NCAs.

NCAs should provide definitions and guidance for the fields included in the incident reporting forms, ideally harmonized with the definitions used by global industry standards and other relevant national and international guidance. This guidance will be particularly important for small and medium enterprises who may not have access to cybersecurity expertise. Information on the types of malicious activity covered in the reporting form should be discussed upfront in non-technical language to help reduce the potential of accidental and false reporting.

Layer 1: General information fields applicable to all incidents

A) Victim Information

- Organization name and other identifying information (state of incorporation, legal trade names, headquarters location or incident location, etc.)
- Entity type (corporation, LLC, nonprofit; or sub-national government entity)
- Point of contact information (name, title/position, telephone, email)
- Business sector (e.g., manufacturing, healthcare)
- Organization size (number of employees or annual revenue or budget)
- Are you working with any of the following:
    - A private incident response (IR) service, consultant, or firm?
    - A sub-national or national government resource or task force?
    - A global or regional entity (e.g. regional CSIRT)?

  If so, please provide the responding organizations' name and contact information.

B) Incident Type *(This selection will determine what section in layer 2 the reporting entity should fill out; reporting organizations should be able to choose more than one)*:

- Business Email Compromise
- Ransomware or other extortion
- Data Theft (credentials, personally identifiable information, intellectual property, trade secrets, etc.)
- Financial theft
- Service Theft (e.g., cryptojacking)
- Denial of Service/availability attack
- Disruptive or destructive attack
- Data manipulation or integrity loss
- Branding/reputation attack
- Unauthorized access to mission critical information or systems (OT, SCADA, or ICS)
- Other

C) Incident Information

- Assessed time span of incident (date first malicious activity occurred [if known] and date/time incident detected)
- Date reported
- Description of the incident (include as many details as are known at the time of the report, such as number of systems affected, whether data was lost, whether the incident affected any specially protected information such as health records, operational impacts, etc.)
- Description of the business impact (including anticipated down time, revenue loss, effect on customers)

- Description of whether this incident was detected by the organization or reported by a third party, and if so, what the role of the third party has (e.g. financial institution, managed security provider, independent security researcher, etc.)
- Have you reported this incident to any other government agency? If so, which ones? Please provide any report, receipt, or confirmation number received.
- Is the incident on-going?
- Is this an update to a previous report?
- Is this the final report on this incident? Do you expect to file additional reports?

D) Threat Actor Information

- Threat actor communications, if any (examples include emails, email addresses, internet destinations such as domain names or TOR information, social media posts, text messages, voicemails, phone records, etc.)

Layer 2: Incident-specific information fields (fields change based on incident type)

Business Email Compromise:

- Copy of email (including header information)
- Amount requested
- Amount paid
- Requested funds transfer method
- Victim bank name, address, and name(s) on account, and relevant account numbers
- Recipient bank/wallet address, contact info, routing information, and account name and number (if possible)
- Information regarding the compromise of internal accounts (e.g., mailbox takeover, email forwarding or deleting rules were created, etc.)

Ransomware or Other Extortion:

- Screenshot of ransom/extortion note or copy of the email
- Ransomware variant used (if known)
- Ransom amount demanded
- Type of currency demanded
- Did you pay? If yes, please provide:
    - Cryptocurrency address(es)
    - Cryptocurrency type(s)
    - Date of Payment (if any)
    - Transaction ID (e.g., transaction hash), if known
    - Transaction amount
    - Victim bank name, address, and name(s) on account, relevant account numbers
    - Recipient bank/wallet address, contact info, routing information, and account name and number (if possible)
- What factors led to the decision to pay the ransom?

- Did you receive the keys in return? If yes:
    - Did the keys work? What approximate percent of the files were recoverable?
- Was any data exfiltrated? If yes, please describe the type of data stolen.
    - Did the criminals leak any stolen data (to the best of your knowledge)? If so, where?
    - Did the criminals use any other pressure tactics, such as contacting clients to inform them of the compromise?

Data Theft:

- Type of Data Stolen:
    - Personally identifiable information for:
        - Employees
        - Customers
    - Health Records
    - Financial information for:
        - Customers (including Payment Card Industry Data Security Standard)
        - Company
    - Intellectual Property
    - Negotiation information
    - IT/OT/ICS network information
    - Employee credentials
    - Internal communications
    - Business records
    - Other non-protected, non-sensitive data
- Specific information categories within the stolen type (e.g., name, address, national or regional identification numbers, passwords, etc.)
- Volume of stolen information
    - For PII, number of records or individuals affected
- Value of stolen information (if known or estimable)

Financial Theft (e.g., banking trojans)

- Type of money stolen
- Financial method used (e.g., cryptocurrency, wire transfer, ATM withdrawals, etc.)
- Amount stolen
- Technical method of theft (e.g., banking trojan, Man in the Middle attack, etc.), if known
- Were any funds recovered?

Service Theft

- What type of service was stolen? (e.g., communications, computer processing power, or other functions, etc.)
- How was it used? (e.g., to send spam, conduct a denial of service attack, mine cryptocurrency, etc.)
- Duration
- Impact on business operations, IT systems, or OT systems

Denial of Service / Availability Attack:

- Impact on business operations or IT systems
- Duration of Outage
- Were mitigation techniques used and/or successful?

Disruptive or Destructive Attack

- Type of system(s) affected (e.g., IT, OT, SCADA, or ICS systems)
- Extent of damage (number of endpoints, number of customers affected, etc.)
- Type of malware used to carry out the attack (if known)
- Operational impact of attack
- Estimated time until recovery

Data Manipulation or Integrity Loss

- Type of data affected (customer records, business records, etc.)
- Extent of damage (number of records, customers, or systems affected)
- Type of malware used to carry out the attack (if known)
- Operational impact of attack
- Estimated time until recovery

Branding/Reputation Attack

- What is the attack type (e.g., account takeover, social media account takeover, mirrored or fake website, etc.)
- What was the impact?
- Was recovery successful?

Unauthorized Access to Mission Critical Information or Systems (OT, SCADA, or ICS systems)

- Type of system or data accessed
- Assessed extent of access
- Potential impact if affected system(s) were disrupted or data were stolen
- Has the adversaries' access to the affected systems been terminated? If not, when do you anticipate eliminating their access?

Layer 3: Additional technical information fields (NCAs should designate this section as optional or provide guidance as to which entities must provide this information)

Provide the following technical information associated with the incident to the extent known:

- Victim IP address or address range
- Actor group(s)
- MITRE ATT&CK categories, functions, and subfunction(s) used by malicious actors
- Malware type(s)/name(s) employed
- Technical indicators of compromise (IOCs)/indicators of attack (IOAs)
- Tactics, tools, techniques, or procedures associated with the incident not captured in the ATT&CK information
- Vulnerabilities exploited during the incident
- Technical parameters for Denial of Service incidents, including volume, duration, and type.
- Narrative: Provide additional technical details to understand the incident more fully. Is there anything we missed?

Appendix A: Why national cybersecurity authorities would request the information in the proposed Cyber Incident Reporting Form

In developing an incident reporting framework, NCAs have to balance several competing priorities. NCAs should seek to collect sufficient information to achieve the goals of mandatory incident reporting while limiting the burden placed on organizations at a highly stressful time. In our recommended framework, we have attempted to strike that balance. The following sections lay out our reasoning for collecting this information through the cyber incident reporting process.

Layer 1: General information fields applicable to all incidents

A) **Victim Information** is needed to support all the incident reporting purposes, from trend identification to response. The fields in this section help uniquely identify the reporting entity. In addition to expected fields such as business name and sector, the proposed format also includes a question regarding whether an incident response organization is involved with the incident. Providing the name of the incident response organization**,** if relevant, can enable the government to work with the preliminary response entity to avoid redundancy and maximize response efficiency.

B) **Incident Type** is critical to identifying the relevant information to be collected. It will also allow the government to more easily prioritize, categorize, store, track, and use the report for trend analysis.

C) **Incident Information** fields provide the basic parameters of what happened during the incident to the extent known at the time of the report. The eight suggested fields in this section do not require technical expertise to answer so that organizations without access to cybersecurity expertise can still file a report.

D) **Threat Actor Information** can assist any criminal investigation into the incident. It also enables threat analysis and trend development.

Layer 2: Incident-Specific Information Fields

We anticipate that organizations will primarily file a cyber incident report through a web portal or other online access point; therefore, the format can dynamically change depending on the incident types being reported and only display the fields relevant to those types.

Business Email Compromise

- **Copy of email** (including header information) provides information critical to understanding the incident and investigating it further. It allows the government to associate the incident with a particular actor group or on-going campaign.
- **Amount requested** assists with trend analysis.
- **Amount paid** assists with trend analysis.
- **Requested funds transfer method** can help the government investigate an incident further.
- **Victim bank name, address, and name(s) on account, and relevant account numbers** can enable the government to work with the financial institution to halt the transfer of funds, or to identify, track, and possibly recover those funds if the transfer has already occurred.
- **Recipient bank/wallet address, contact info, routing information, and account name and number (if possible)** can enable the government to work with the financial institution to halt the transfer of funds, or to identify, track, and possibly recover those funds if the transfer has already occurred.
- **Information regarding the compromise of internal accounts** (e.g., mailbox takeover, email forwarding or deleting rules were created, etc.) can help the government understand the incident, connect it with other incidents, and improve indication and warning.

Ransomware or other extortion

- **Screenshot of ransom/extortion note or copy of the email** provides information critical to understanding the incident and investigating it further. It allows the government to potentially associate the incident with a particular actor group or on-going campaign. It can help identify the nature and extent of the incident, shape the threat analysis, and support trend development.
- **Ransomware variant used** helps responders understand the incident. It can enable law enforcement and private sector entities to identify decryption keys (if they exist), which can provide an alternative to paying ransom without losing encrypted data. This information can also enable threat analysis and trend development.
- **Ransom amount demanded** can help further identify and potentially retrieve the ransom payment.
- **Type of currency demanded** can help identify and trace victim payments, and aid

analysts in establishing trends about the threat.

- **Did you pay** – understanding the number of entities paying ransoms is critical to understanding the breadth and depth of the ransomware problem, as well as knowing whether the total number of entities paying is going up or down over time.
  If you did pay, then:
    - **Cryptocurrency address(es)** are critical to the ability of blockchain analysts to track payments on the blockchain, and increase the possibility of ransom recovery.
    - **Cryptocurrency type(s)** help further identify and trace victim payments, and aid analysts in establishing trends about the threat.
    - **Date of payment** can enable law enforcement and blockchain analysts to identify, track, and potentially recover paid ransoms.
    - **Transaction ID or hash** is a unique transaction identifier. This critical piece of payment information is one of the most effective ways to identify, trace, and potentially recover a payment.
    - **Transaction amount can** help further identify and potentially retrieve the ransom payment.
    - **Victim bank name, address, and name(s) on account, and relevant account numbers** can enable law enforcement to work with the financial institution to halt the transfer of funds, or to identify and track that transfer if it has already occurred.
    - **Recipient bank/wallet address, contact info, routing information, and account name and number** can help identify malicious actors, and can aid in the tracking and potential seizure of ransom payments.
- **What factors led to the decision to pay the ransom?** This information helps the government craft policies to enable more organizations to avoid paying ransoms.
- **Did you receive the keys in return?** Can help law enforcement identify the type of ransomware utilized. If yes:
    - **Did the keys work? What approximate percent of the files were recoverable?** This information can aid in threat analysis and trend development.
- **Was any data exfiltrated? If yes, please describe the type of data stolen.** This information can help identify the severity of an incident and aid in threat analysis and trend development. It also alerts governments to potential compromise of personally identifiable information or intellectual property theft, enabling warnings for similarly situated organizations.
- **Did the criminals leak any stolen data (to the best of your knowledge)? If so, where?** This information can help identify the severity of an incident and can aid in threat analysis and trend development.
- **Did the criminals use any other pressure tactics, such as contacting clients to inform them of the compromise?** This information can help aid in threat analysis and trend development.

Data Theft

- **Type of data stolen** can help identify the nature and severity of an incident and aid in threat analysis and trend development. It would enable NCAs to identify the other elements of the government who should receive the incident report.
- **Specific categories of information within the stolen type** (e.g., name, address, passwords, etc.) can help identify the nature and severity of an incident and aid in threat analysis and trend development.
- **Volume of stolen information** can help identify the severity of an incident, whether broader response activities are warranted, and aid in threat analysis and trend development.
- **Value of stolen information** (if known or estimable) can help identify the severity of an incident and aid in threat analysis and trend development.

Financial Theft (e.g., banking trojans)

- **Type of money stolen can** help identify and trace victim assets, and aid analysts in establishing trends about the threat.
- **Financial method used** (e.g., cryptocurrency transfer, wire transfer, ATM withdrawals, etc.) can enable law enforcement to work with the financial institution to halt the transfer of funds, or to identify and track that transfer if it has already occurred.
- **Amount stolen** can help further identify and potentially retrieve the payment.
- **Technical method of theft** (e.g., banking trojan, Man in the Middle attack, etc.), if known, can help law enforcement investigate an incident.
- **Were any funds recovered?** Answering this question can help law enforcement investigate an incident.

Service Theft

- **What type of service was stolen?** (e.g., communications, computer processing power, or other function, etc.) can help identify the nature and severity of an incident and aid in threat analysis and trend development.
- **How was it used?** (e.g., to send spam, conduct a DDoS, mine cryptocurrency, etc.) can help identify the severity of an incident and can aid in threat analysis and trend development.
- **Duration of outage** can help identify the severity of an incident and can aid in threat analysis and trend development.
- **Impact on business, operations, IT, or OT** can help identify the severity of an incident and can aid in threat analysis and trend development. It helps the government categorize the incident and shape its response actions.

Denial of Service / Availability Attack

- **Impact on business operations or IT systems**
- **Duration of outage** can help identify the severity of an incident and can aid in threat analysis and trend development.
- **Were mitigation techniques used and/or successful?** This field indicates whether the incident is on-going or whether the reporting entity has successfully managed or mitigated the availability attack.

Disruptive or Destructive Attack

- **Type of system(s) affected** (e.g., IT, OT, SCADA, or ICS systems) can help identify the severity of an incident and can aid in threat analysis and trend development.
- **Extent of damage** (number of endpoints, number of customers affected, etc.) can help identify the severity of an incident and can aid in threat analysis and trend development.
- **Type of malware used to carry out the attack** (if known) can aid in law enforcement investigations, threat analysis and trend development.
- **Operational impact of attack** can help identify the severity of an incident and can aid in threat analysis and trend development.
- **Estimated time until recovery** can help identify the severity of an incident and can aid in threat analysis and trend development. It also provides an understanding of how long the reporting entity expects the incident to last.

Data Manipulation or Integrity Loss

- **Type of data affected** (customer records, business records, etc.) can help identify the nature and severity of an incident and aid in threat analysis and trend development.
- **Extent of damage** (number of records, customers, or systems affected) can help identify the severity of an incident and can aid in threat analysis and trend development.
- **Type of malware used to carry out the attack** (if known) can aid in law enforcement investigations, threat analysis and trend development.
- **Operational impact of attack** can help identify the severity of an incident and can aid in threat analysis and trend development.
- **Estimated time until recovery** can help identify the severity of an incident and can aid in threat analysis and trend development.

Branding/Reputation Attack

- **What is the attack type (e.g., account takeover, social media account takeover, mirrored or fake website, etc.)?** This information narrows down the particular type of branding or reputation attack.
- **What was the impact?** This field helps identify the severity of an incident and can aid in threat analysis and trend development.
- **Was recovery successful?** This field provides insight into how severe the incident was

for the reporting entity, as well as whether the incident remains ongoing.

Unauthorized Access to Mission Critical Information or Systems (OT, SCADA, or ICS systems)

- **Type of system or data accessed** can help identify the severity of an incident and can aid in threat analysis and trend development.
- **Assessed extent of access** can help identify the severity of an incident and can aid in threat analysis and trend development.
- **Potential impact if affected system(s) were disrupted or data were stolen** can help identify the severity of an incident and can aid in threat analysis and trend development.
- **Has the adversaries' access to the affected systems been terminated? If not, when do you anticipate eliminating their access?** These fields provide insight into whether the incident is ongoing, whether the government should avoid communicating with the reporting entity through certain channels, and how difficult the incident is proving to be for the entity to manage.

Layer 3: Additional technical information fields

The fields in this layer provide technical insight into the incident. Organizations will only report these fields if they have technical cybersecurity capabilities in-house, a cybersecurity provider with these capabilities, or brought in an incident responder. These fields will enable the government to make comparisons, share indicators of compromise,

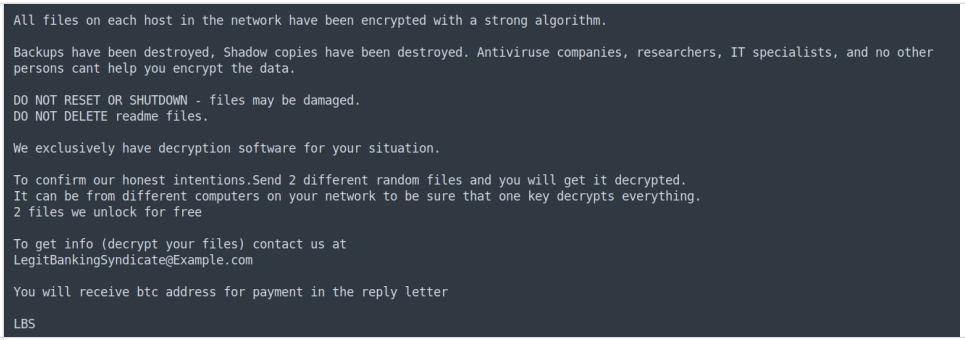
- **Victim IP address or address range** can enable law enforcement and partners to identify threat actor TTPs, and will identify the access points that need to be secured.
- **Actor group(s) when relevant,** can help law enforcement and other responders pinpoint attack methods and possible decryption keys, when relevant. It also provides a basis for further investigation.
- **MITRE ATT&CK categories, functions, and subfunction(s) used by malicious actors.** ATT&CK is a curated knowledge base that tracks cyber adversary tactics and techniques used by threat actors across the entire attack lifecycle. The framework can be used to collect data about an incident, and also to strengthen an organization's security posture in the aftermath of an attack
- **Malware type(s)/name(s) employed** can aid in law enforcement investigations, threat analysis and trend development.
- **Technical indicators of compromise (IOCs)/indicators of attack (IOAs) associated with the incident**, like copies of identified malware, phishing messages, and identified attacker infrastructure, can help law enforcement investigate an incident. It can enable the government to warn other companies what to watch for to prevent the same incident from happening to another company.
- **Tactics, tools, techniques, or procedures associated with the incident not captured in**

the ATT&CK information can help build a better understanding of the threat, and account for the fact that ATT&CK is constantly being updated.

- **Vulnerabilities exploited during the incident** allows investigators to understand whether the adversary used well-known tools and techniques or whether the adversary used novel capabilities. This information would also contribute to trend analysis and prioritization of patching.
- **Narrative** allows victims or responding entities to include any other information that they might deem important.

Appendix B: Example Incident Report

Layer	Section	Field	Example
Layer 1: General Information Fields Applicable to All Incidents		Organization name and other identifying information	Acme Corp (Formerly A Company Making Everything LLC)
		Entity type	Corporation
		Contact information (name, title/position, telephone, email)	Alice Bobson Incident Response Lead
		Business sector	Manufacturing
		Organization size	2,523 employees; $500 million in annual revenue
	A (Victim Information)	Are you using any of the following: A private incident response (IR) service, consultant, or firm? A national or local government resource or task force? Other government agency or entity? If so, please provide the responding organizations' name and contact information.	Yes, we are using IncidentResponseCompanyA. We have also filed a report with the national police's local office, who we are having weekly calls with to brief on the current status of the investigation.
	B (Incident Type)	Data Theft (credentials; personally identifiable information; intellectual property; trade secrets; etc)	Ransomware or other extortion
	C (Incident Information)	Assessed time span of incident (When the first intrusion may have occurred, when the incident was detected)	February 10, 2022 - February 18, 2022
		Date reported	February 19, 2022
		Description of the incident (include as many details as are known at the time of the report, such as number of systems affected, whether data was lost, whether the incident affected any specially protected information such as health records, operational impacts, etc.)	Attackers are believed to have first gained acccess on February 10th, 2022 using CVE-2018-13382 to gain access to our VPN Appliance. From this access, the attackers were able to remotely connect to our network and move laterally to our Active Directory server. Ransom operations began on February 18, 2022. Our initial investigation identified 35 business critical servers were impacted by the ransomware and data from our central storage server had been exfiltrated. Data on our storage server does not include customer information and the contents obtained are believed to be related to business and manufacturing processes used here at Acme Corp.
		Description of the business impact (including anticipated down time, revenue loss, effect on customers)	Due to the disruption of key servers, production has been halted at both of our manufacturing facilities. We are expecting this incident to result in at least 4 days of production downtime. We have issued a notice to our customers informing them of the breach and that their information is not believed to have been stolen, however, we cannot effectively measure reputation impact.
		Have you reported this incident to any other national or local government entity or agency? If so, which ones?	Yes, this has been reported to the cybercrime unit of the national police.
		Is the incident on-going?	At this time, we do not beleive the ransomware actors are still present on our network. We have conducted a company wide password reset, removed the VPN appliance and are actively working to further verify the eviction of the actor.
		Is this an update to a previous report?	No
		Is this the final report on this incident? Or Do you expect to file additional reports?	Additional reports may be filed if we discover additional details or inaccuracies are found in our current understanding of the situation
	D (Threat Actor Information)	Threat actor communications, if any (examples include emails, email addresses, internet destinations such as domain names or TOR information, social media posts, text messages, voicemails, phone records, etc.)	A text file, containing recovery instructions, was identified on each of the ransomed servers. In this note, the actor instructed us to email "LegitBankingSyndicate@Example.com" to discuss decryption. In coordination with our incident response provider, legal team and senior leadership, we contacted the actor who requested we send "$2kk USD to the Bitcoin wallet 1A1zP1eP5QGefi2DMPTfTL5SLmv7DivfNa". Given the high ransom demand and our ability to recover from backups, we decided not to pay the ransom. A copy of this email thread has been provided to our FBI contact.

Layer 2: Incident Specific Information	**Rasomware or Other Extortion**	Screenshot of ransomware/extortion note or copy of the email	
		Ransomware variant used (if known)	Hidden Tear
		Type of currency demanded	US Dollar
		Did you pay? If yes please provide:	No
		Cryptocurrency address(es)	
		Cryptocurrency type(s)	Bitcoin
		Date of payment (if any)	
		Transaction ID if known	
		Transaction amount	
		Victim Bank Name, address, name(s) on account, and relevant account numbers	
		Recipient bank/wallet address, contact information, routing information, and account name and number (if possible)	1A1zP1eP5QGefi2DMPTfTL5SLmv7DivfNa
		What factors led to the decision to pay the ransom?	Recovery of assets
		Did you recieve the keys in return? If yes:	
		Did the keys work?	
		What approximate perentage of the files were recoverable?	
		Was any data exfiltrated? If yes:	
		Please describe the type of data stolen.	Yes, Internal business and manufacturing process documentation
		Did the criminals leak any stolen data (to the best of your knowledge)?	No, it does not appear that this ransomware group uses a dedicated leak site (DLS) in which our data was posted
		If so, where?	
		Did the criminals use any other pressure tactics, such as contacting clients to inform them of the compromise?	
	Data Theft	Type of Data Stolen	Intellectual property
		Specific categories of information within the stolen type	Internal business and manufacturing process documentation
		Volume of stolen information	35Gb
		For PII, number of records or individuals affected	0

		Value of stolen information (if known or estimable)	
Layer 3: Additional Technical Information Fields		Victim IP Address or Address Range	240.129.21.0/24
		Actor group(s)	LegitBankingSyndicate
		MITRE ATT&CK categories, functions, and subfunction(s) used by malicious actors	T1190, T1059, T1136, T1562, T1070, T1018
		Malware type(s)/name(s) employed	LegitBankingSyndicateRansomware
		Technical indicators of compromise (IOCs)/indicators of attack (IOAs)	Ransomware Payload: aae523c5b488302020067109ab5ea04a98974766e2ca19157f3986a6cbe20a2e
		Tactics, Tools, Techniques, or Procedures associated with the incident not captured in the ATT&CK information	
		Vulnerabilities exploited during the incident	CVE-2018-13382
		Technical parameters for Denial of Service incidents, including volume, duration, and type.	
		Narrative: Provide additional technical details to understand the incident more fully. Is there anything we missed?	