Framework for Cyber Incident Reporting

Cyber Threat Alliance
Institute for Security & Technology

CREST
CipherTrace
Coveware
Cybera
Cybercrime Support Network
Open Cybersecurity Alliance
SolarWinds

Framework for Cyber Incident Reporting

Multiple industry organizations have come together to provide input regarding cyber incident reporting. This group has identified a set of principles that the incident reporting regulation should incorporate, and we have developed a set of model reporting formats the Cybersecurity and Infrastructure Security Agency (CISA) could use as the foundation for the reporting forms. The report falls into 3 sections:

1. Purpose, Expectations, and Definitions
2. Principles
3. Incident Reporting Fields

Section 1: Purpose, Expectations, and Definitions

Purpose

Incident reporting can simultaneously serve multiple purposes. We recommend that the Cybersecurity and Infrastructure Security Agency (CISA) identify the reporting requirement's purposes, consistent with the underlying statute. Since these purposes differ in the granularity of information required, CISA should specify the use cases as part of the regulation. Such purposes can include:

***Trend identification*:** collecting data across multiple incidents at multiple companies could allow the Federal government 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 the Federal government to warn similarly situated organizations about impending threats.

Response: reporting could be used to drive asset and/or threat response activities (as defined in Presidential Policy Directive-41) and inform policy discussions including about the effectiveness of deployed strategies.

***Assessing impact and harm**:* reporting can contribute to a better understanding of the harm and impact cyber incidents cause to both targeted organizations, individuals, and society.

Expectations

CISA should use the regulation to set clear expectations on several topics.

What happens after reporting an incident: CISA should acknowledge that the report has been received, and organizations should expect to receive such confirmation. Beyond this acknowledgement, however, the regulation should also make clear what will not necessarily happen; for example, just because a company reports an incident does not mean that law

enforcement agents will open a case. If the Federal response does not align with expectations, the reporting requirement could be seen as a failure.

Information distribution and handling: CISA 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 Federal entities could receive the reported data under what conditions.

Definitions

The statute directs CISA to define a "substantial cyber incident" and "covered entity" in the regulation. We offer the following definition of substantial cyber incident for consideration:

A substantial cyber incident is one that causes:

- An undesired effect on an IT, OT, other digital system, or social media account **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

In addition to the requirement to consider consequences and threats contained in Section 2242(c)(1) in defining "covered entities," we recommend excluding very small companies from the definition. Consistent with this approach, we offer the following exclusion for consideration.

A covered entity is an entity that owns or operates an IT, OT, other digital system, or social media account in one or more of the critical sectors defined in Presidential Policy Directive-21 and has:

- More than 50 employees,
- More than 1,000 customers, or
- Revenues greater than $5 million.

Beyond the definition, ensuring that every organization knows whether it is a covered entity is a difficult challenge. CISA should consider a public awareness campaign to make sure as many organizations understand their obligations as possible. Further, some organizations may ask CISA to determine whether they are a covered entity, so CISA should be prepared to handle such inquiries.

Section 2: Principles

In developing the incident reporting regulation, we recommend that CISA and similarly situated organizations incorporate the following 10 principles. Following these principles will advance the quality, quantity, and utility of the reporting while minimizing the burden on the covered entities.

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 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. The government 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: CISA should take appropriate steps to secure the incident reporting system and associated data, including minimization, anonymization, and aggregation when appropriate. It should also specify when it would consider incident reporting information to be Protected Critical Infrastructure Information (PCII). In addition, CISA should be transparent about how it will maintain privacy for any information shared as part of the incident reporting process. CISA should also specify how long it 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 an ISAC, will be important.

Automation: The incident reporting process should be automated within the government and use industry standards, such as the National Information Exchange Model (NIEM) or Structured Threat Intelligence eXchange (STIX).

Relevance: CISA 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 CISA determines that the scale and impact of the reported incident warrants follow up, then the regulation should allow it to request additional information from the reporting entity.

Iteration: The details regarding a cyber incident will evolve over time and the affected organizations will learn more as the incident response continues. Therefore, CISA 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. Although the initial reporting deadline is specified in the statute, CISA 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. CISA should also clarify whether reporting to a sector-based Information Sharing and Analysis Center (ISAC) will continue to count as reporting the incident to CISA for those sectors where such reporting has been the standard in the past.

Equivalence and Interoperability: Many organizations are subject to multiple reporting requirements. To the maximum extent possible, the Federal government should standardize incident reporting forms across departments and agencies to better aggregate data, analyze trends, and recover ransoms. However, since achieving such standardization will take time, allowing organizations to submit incident reports using the format required by other agencies (for example, the Securities and Exchange Commission) would reduce the burden on industry. Therefore, CISA should consider those other formats as "equivalent" to the CISA format and treat their submission as meeting the statute's reporting requirement until the Federal government adopts a unified standard. Similarly, we recommend that other agencies adopt CISA's reporting formats as the standard.

Harmonization: Along with equivalence, CISA should promote harmonization of reporting requirements, not only domestically within the US, but internationally. 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.

Reporting Culture: CISA should encourage all businesses to report substantial cyber incidents, regardless of whether they are subject to the mandatory reporting requirement. Implementing this recommendation would involve updating other CISA materials. For example, the CISA Ransomware Response Checklist and the CISA ransomware guide do not include an explicit recommendation to report, and instead only reference reporting as one way to contact CISA regarding anomalous cyber activity**.**

No Automatic Trigger: To the extent allowable under statute, CISA should make clear that filing an incident report under this regulation does not automatically trigger any other reporting action or obligation. Organizations will have to determine whether to file reports with other oversight bodies or agencies based on those reporting requirements, not just because the incident qualified for a report under this statute.

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 CISA's consideration.

CISA should provide definitions and guidance for the fields included in the incident reporting forms. 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; State, Local, Territorial, or Tribal agency)
- 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 using any of the following:
    - A private incident response (IR) service, consultant, or firm?
    - A state or local government resource or task force?
    - National Guard?

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

B) Incident type *(this selection will determine what section in layer 3 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)
- Have you reported this incident to any other Federal, State, Local, Territorial, or Tribal 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(s)
    - 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, SSN, 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 function, 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 (CISA 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?