TLP:CLEAR

Ethics for Incident Response and Security Teams - Case Studies

February 1, 2023

This document describes a set of case studies to help explain the duties as described by the Code of Ethics for Incident Response and Security Teams (EthicsfIRST). These case studies are meant to represent dilemmas faced by security teams. For each of the duties there is one example that captures relevant aspects of that duty. The format of an example is that first the context is described in the *Situation* section, then a suggested *action* is described, followed by a *Resolution* describing how this balances the different duties as described by EthicsfIRST. For ease of reading, this SIG chose to simplify and clarify examples.

There is no specific example for the Duty to Respect Human Rights. EthicsfIRST follows the definitions of Human Rights as outlined by the United Nations, and these are represented throughout the below principle case studies.

Duty of trustworthiness

- **Situation:** A finder reports a security issue to Company X's security operation center (SOC). The organization has a SOC and a product security incident response team (PSIRT). Each team within Company X has their own ingest mechanisms (e.g., emails, website) and manages their own communications, but these separate teams are not obvious to the finder. The SOC consistently disregards correspondence with the finder, and the finder becomes upset. In frustration the finder turns to social media about the bad experience they have had with the organization's PSIRT.
  - **Action:** Each team within Company X should understand the scope and mission of the other team and have established processes to route tasks between them. SOC should pass along the case to PSIRT or product owner in case Company X does not have a full PSIRT who then reaches out to the finder. If the finder is a member of another company that has a PSIRT, Company X should coordinate with the finder's PSIRT to address the poor communications and inform them about the steps being taken to correct the process. The finder removes the blog and tweets. As a result, the company makes improvements to the internal processes for handling vulnerabilities between the SOC and PSIRT.
  - **Resolution:** Providing a clear communications mechanism for finders to report to the correct team reduces the likelihood of confusion and lost correspondence. Building trusted relationships and reputations ahead of the event or interaction is important to address security concerns or incidents in a timely manner. Trustworthiness is built between individuals over time. Having an established trust-network can help to de-escalate and reduce the risk of brand damage.

Duty of coordinated vulnerability disclosure

- **Situation:** An academic researcher finds a vulnerability in certain types of hardware. The issue is prevalent in multiple manufacturers, making it very hard for the researcher to perform coordinated vulnerability disclosure (CVD) across multiple entities.
  - **Action:** The researcher reaches out to their national CSIRT. This organization can help contact the most prevalent vendors, alerting them to the finding. While it is hard to discover all the vendors in this space, the national CSIRT team also reaches out to other CSIRT and vendor teams who may be able to help spread this CVD report.
  - **Resolution:** By acting as a liaison, the national CSIRT coordinates resolving the vulnerability with the producers/manufacturers of the component and alerts the companies that use it. They are able to explain the global context of the CVD, even between vendors that may feel they are not allowed to speak to one another due to market protections. This results in a coordinated, cross-industry collaboration to fix the issue.

Duty of confidentiality

- **Situation:** You receive information from a constituent X about an incident that identifies the source of an attack as coming from another of your constituents.
  - **Action:** You evaluate the individual circumstances of the situation and determine if there is required action based on local and international laws. You reach out to the original reporter, constituent X, and request permission to coordinate with constituent Y. The reporting organization, does not give you explicit permission to share their logs or information from their site with the appropriate contacts at the attack source constituent Y.
  - **Resolution:** Unless you obtain the reporting organization's explicit permission to identify them or their affected system(s) as the source of the report, you should maintain the confidentiality and identity of the reporting source when notifying the appropriate security point of contact at the attack source.

Duty to acknowledge

- **Situation:** A PSIRT team receives a report of a vulnerability that affects their currently supported product. After a week, the finder still has not received acknowledgment that their report has been received. Another email is sent, but still no response. The finder contacts another company's PSIRT team that uses the first company's product to report the issue (or the finder just goes public with the information).
  - **Action:** Incident response teams should always acknowledge receipt of a report as soon as possible. Once they confirm it is a vulnerability, they should alert the finder of this and the action they plan to take (fix it, not fix it as product is no longer supported, fix it next version, etc).

- **Resolution:** To avoid situations like this, incident response teams should have established processes on receiving and acknowledging reports. Coordinated vulnerability disclosure is not a one way street. If teams do not acknowledge reports, they may find they don't receive them.

Duty of authorization

- **Situation:** A CSIRT has a need to investigate an endpoint where the primary user resides in a country that is subject to GDPR.
  - **Action:** Consult with legal experts to evaluate requirements for adherence to local and internal laws. In coordination with legal experts, determine the best course of action for a specific case keeping in mind that all actions must be conducted in accordance with considerations for protecting user privacy, collecting only what is strictly needed to uphold integrity of the environment.
  - **Resolution:** Incident responders act within the scope of their authorization - consulting constituents and relevant stakeholders where feasible prior to engaging.

Duty to inform

- **Situation:** A CSIRT is made aware of an incident. In their environment, there are legal restrictions for sharing data (breach, vulnerability, compromised systems) outside of their constituency. They need to fix the issue, but if it requires customers to take action, they will need to notify their customers. If personal data was affected, then those users would need to be notified.
  - **Action:** After a dating site was breached, a CSIRT decided not to inspect the exposed data for their constituency as it could cause embarrassment to users and their organizations. An assessment needs to be made as to whether the embarrassment is more or less risky to an organization than investigating and notifying affected users.
  - **Resolution:** Users are empowered to make risk based decisions or take actions to mitigate potential negative impacts resulting from a breach of personal information. Potential users are provided information to inform their subscription decisions.

Duty to Team health

- **Situation:** Over the last two years, the incident response team has seen a year over year growth of over 100% for case counts. Each member of the team is regularly working on multiple incidents. They are exhausted and have had no break in several months. The morale has significantly declined. Members are starting to leave the company, increasing the burden on the remaining team.
  - **Action:** To avoid this, teams should make sure that members are recuperating by taking breaks and disconnecting from work. If workload is not diminishing, managers should consider advocating for additional capacity or reprioritizing team responsibilities/services. While following local labor laws and guidelines, teams should consider flexible work arrangements and reasonable accommodations.

- **Resolution:** While teams will have the occasional round of emergencies, this should not be the day to day expectations. Teams need time to rest and "unplug" to remain effective, efficient, happy, and healthy. Teams that continue to push their members with insufficient work/life balance may see high rates of turnover, stress related health issues, and a demoralized workforce.

Duty to Team ability

- **Situation:** A team's services are requested by a constituent organization. The team sends two members to the requesting organization: a new hire and a more experienced member. Both members have strong technical backgrounds, but the new hire has not been trained on the team's standard procedures for handling sensitive information.
  - **Action:** Teams should ensure that all members are properly trained prior to deployment to a constituent site. Teams should consider how many fully trained employees are needed to address onsite needs, then add the new-hire as an apprentice to the team.
  - **Resolution:** In this scenario, it is acceptable to provide on-the-job training to the new hire provided the team can still safely accomplish the needs of the constituent organization. The more experienced team member(s) should provide the new team member with the psychological safety to ask questions ("there are no stupid questions") and pay special attention whenever sensitive constituent information is being handled. New team members shouldn't be expected to "figure it out" on the job.

Duty for responsible collection

- **Situation:** A CSIRT gains legal authorization to collect digital forensics and network diagnostics information from a compromised host within its jurisdiction. The CSIRT begins collection and starts to develop threat intelligence from the data that it has gathered (hashes, network addresses, and malware samples for further analysis). As the project progresses, the team continues to collect data months after the investigation is completed. The team is collecting data past the initial goal of collection, possibly putting the organization at risk for breaking the law.
  - **Action:** To prevent excessive collection, teams should set clear policies for data collection and retention to include time boundaries (collection start and end dates) in advance. If an end date is reached before the goals of the collection have been achieved, the CSIRT may extend the data collection end date in consideration of legal authorization, intended purpose, and eventual disposition.
  - **Resolution:** To avoid this risk, CSIRTs should ensure that collected data is only used for its intended purpose (for example: digital forensic incident response, network diagnostics, vulnerability analysis, or development of threat intelligence). Once collected data has exhausted its usefulness for that intended purpose, it should be handled per established data retention policy in the interests of minimizing the risk of exposure or misuse in the future.

Duty to recognize jurisdictional boundaries

- **Situation:** A web hosting provider in Country A is attacked by an unknown cybercriminal. The criminal is able to compromise the service and extract customer data, including customers from Country X. The team follows the requirements for Country A, but misses the deadline and reporting requirements for Country X. The web hosting provider is then fined by Country X's data protection authority for not following data breach notification requirements.
  - **Action:** Teams should adopt regular reviews of incident procedures and privacy regulations to ensure their practices align with the appropriate laws and requirements. Teams should work with their legal and privacy representatives to develop appropriate plans and documentation for commonly occurring scenarios. If an out of band situation arises, teams would consult legal representation for situation specific advice.
  - **Resolution:** The incident responder must know the reporting procedures required for both the local jurisdiction (Country A) and the data owner's jurisdiction (Country X). Differing regulations on notifications and obligations of the incident responder may occur. If jurisdictional regulations are incongruent, teams should know who and how to consult appropriate legal advice in a timely manner.

Duty of evidence-based reasoning

- **Situation:** An incident response as a service firm is asked to perform an assessment of a victim's cybersecurity posture following an incident. After completing the assessment, the service firm's CSIRT submits its recommendations to the victim organization. One month later, the victim organization claims that it has completed all of the recommended actions and asks the CSIRT for a "clean bill of health." The CSIRT is not sure if they should grant certification or not.
  - **Action:** A CSIRT should independently assess the cybersecurity of a victim organization after an incident OR not provide any endorsement without the evidence to support it.
  - **Resolution:** The service firm should state upfront how the assessment will be done and how remediations will be analyzed. A firm should not provide any endorsement of a customers organization's updated cybersecurity posture without first performing its own assessment to prove whether the recommendations were actually followed.
  - **Optional Explanation**: Assessment findings should be based on transparent and accurate reasoning supported by evidence. Evidence, and therefore conclusions, may change over time. Assessments should be clear about what evidence was collected, how it was interpreted, what evidence might change the assessment, and the extent of uncertainty in evidence collection, interpretation, and gaps.