

***Ethical Dilemma: Incident Report Alteration Request***

This document examines an ethical quandary in which clients have sought modifications to a cybersecurity incident report to mitigate their accountability and portray themselves more positively. The incident pertains to a Distributed Denial of Service (DDoS) attack on Friday, October 18, 2024. This situation presents a conflict between upholding professional integrity and accommodating the client’s desire to lessen the perceived consequences of the security breach.

***Part 1: The Scenario***

The incident report outlines a Distributed Denial of Service (DDoS) attack aimed at the company’s web application, resulting in a substantial outage that persisted for around six hours. Throughout this period, users could not access the client’s services, as the attack inundated the company’s network with harmful traffic from various sources, depleting system resources. Consequently, the attack compromised sensitive data, including personal client information, transaction records, and communication logs.

***Incident Report Summary***

|  |  |
| --- | --- |
| Attribute | Details |
| Incident ID | ***DSA-45A7TY*** |
| Breach Type | ***Denial-Of-Service Attack*** |
| Incident Severity | ***Medium*** |
| Effect of The Incident | ***Loss of Revenue*** |
| Incident Owner | ***Franklin Albert*** |
| Earliest Flagged Evidence | ***Unusual High Traffic in The Network*** |
| Most Recent Flagged Evidence | ***Locked Out of The Company Network*** |
| Type of Incident | ***Deliberate Software Attack*** |
| Date Incident Originated | ***September 1st , 2023*** |
| Date Incident Was Detected | ***September 2nd, 2023*** |
| How Was the Incident Detected | ***Locked Out of Computer Network and Files*** |
| Scope of Incident | ***All Departments, Computers, and Servers*** |
| Date Incident Corrected | ***September 7th, 2023*** |
| Corrective Action Type | ***Reduction Mitigation Strategies*** |
| Time to Resolution | ***5 Days*** |
| Reason for Closure | ***Resolved*** |

***Summary of Incident Symptoms***

|  |
| --- |
| *Symptom Description* |
| *Internet Disconnection* |
| *Slow Access to Files* |
| *Inability to access a specific file* |
| *Excessive Amount of Spam Emails* |
| *Unusual IP Address Activity – Large Number of Requests* |
| *Log Analysis Indicated a Large Spike in Network Traffic* |

***Summary of Incident Type and Scope***

|  |
| --- |
| *Incident Type and Scope* |
| *Employees were locked out of company assets, servers, and computers.* |
| *The attack affected all departments within the company.* |
| *Auditors were unable to access the server system to perform audits.* |
| *Despite some computers being functional, all TechBros files were locked from the network.* |
| *High traffic levels were detected in TechBros’ network system logs during the week of the attack.* |

***Part 2: Options***

*Option 1: Provide a Full and Accurate Incident Report*

*Option 2: Alter the Report to Favor the Client*

*Option 3: Mix Truth with Deception*

*Option 4: Escalate to Management*

*Option 5: Seek External Guidance*

***Part 3: Evaluating the Merits***

***Option 1: Provide a Full and Accurate Incident Report***

1. *Legal Considerations: Complies with cybersecurity regulations and standards, including GDPR, HIPAA, and CFAA, fulfilling all necessary reporting obligations.*
2. *Ethical Standards: Maintains the utmost levels of honesty, integrity, and transparency as mandated by the CISSP Code of Ethics.*
3. *Professional Integrity: Strengthens your standing as a reliable cybersecurity expert, prioritizing precision and integrity rather than immediate benefits.*
4. *Implications: Although this approach may temporarily displease the client, it prevents legal and ethical issues while fostering enduring trust and credibility.*

***Option 2: Alter the Report to Favor the Client***

*1. Legal Considerations: Such actions contravene cybersecurity legislation and regulations, potentially resulting in legal repercussions, monetary fines, or litigation.*

*2. Ethical Standards: Compromising integrity breaches established professional ethical standards and may lead to allegations of professional misconduct.*

*3. Professional Integrity: While this may temporarily satisfy the client, it significantly undermines your professional reputation and could jeopardize your certifications or licensure.*

*4. Implications: Such deceit will likely be uncovered during forensic examinations, leading to serious legal ramifications for you and the client.*

***Option 3: Mix Truth with Deception***

*1. Legal Considerations: Although some accurate information may be presented, excluding essential details constitutes a breach of regulatory requirements and may subject both parties to potential legal liabilities.*

*2. Ethical Standards: This approach undermines ethical standards by introducing elements of dishonesty, thereby obscuring the distinction between acceptable and unacceptable behavior.*

*3. Professional Integrity: While this may provide immediate satisfaction to the client, the act of partial misrepresentation poses a significant risk to your long-term professional reputation.*

*4. Implications: The resulting legal and reputational fallout will far exceed any temporary advantages gained once the excluded information comes to light.*

***Option 4: Escalate to Management***

1. *Legal Considerations: Elevating the matter to management facilitates more informed decision-making and mitigates personal liability when the client may advocate for unlawful modifications.*
2. *Ethical Standards: This process ensures that the final report adheres to legal and ethical guidelines.*
3. *Professional Integrity: Engaging higher authorities reflects responsible behavior in addressing intricate ethical dilemmas.*
4. *Implications: This strategy safeguards you from direct accountability while guaranteeing that suitable measures are implemented at a senior level.*
5. ***Option 5: Seek External Guidance***
6. *Legal Considerations: Engaging with regulatory authorities or legal advisors guarantees that the incident report adheres to applicable laws and industry regulations.*
7. *Ethical Standards: This approach promotes an unbiased resolution emphasizing compliance and equity adherence.*
8. *Professional Integrity: Involving external oversight fosters transparency and professionalism, minimizing the risk of partiality in decision-making.*
9. *Implications: While this may prolong the process, it ensures legal and ethical standards adherence.*

***Part 4: Make a Recommendation***

***Recommended Action: Option 1 - Provide a Full and Accurate Incident Report***

*As a professional in the cybersecurity field, it is a must to adhere to established guidelines and legal frameworks to maintain the industry’s integrity. This encompasses adherence to the (ISC)² Code of Ethics, ISO/IEC 27002:2022, and pertinent regulations such as the General Data Protection Regulation (GDPR) and the Computer Fraud and Abuse Act (CFAA). Upholding transparency and integrity is essential, as providing an accurate report is vital for compliance with these laws and standards. This practice mitigates the risks associated with disseminating false information, aligns with our ethical responsibilities, and ensures that clients, regulators, and the public are adequately informed about the true nature of the incident.*

*While fabricating details in an incident report may temporarily protect the client, such actions will likely be exposed during a forensic investigation. Investigators will reveal the actual circumstances surrounding the breach, and any inconsistencies between their findings and your report will become apparent. This can result in significant repercussions, including damage to reputation, loss of professional credentials, and potential legal consequences such as fines or imprisonment. By committing to honesty and transparency, you safeguard your professional integrity and avert the severe ramifications of misrepresentation.*

***Part 5: Support For My Recommendation***

*With these guidelines and laws, we have clear evidence that supports the decision to report the complete truth. Each of these standards proves why my recommended course of action is not only ethically sound but also legally required:*

1. ***ISO/IEC 27002 Standard:*** *This standard emphasizes maintaining the integrity of information and highlights the importance of accuracy in security documentation. Following this standard ensures that incident reports are factual and reliable. By adhering to ISO/IEC 27002, I am upholding the principle of data integrity, which is essential for an organization’s security posture. Modifying the report would violate this integrity, undermining the trustworthiness of the organization’s security measures.*
2. ***NIST Special Publication 800-61:*** *The NIST SP 800-61 guide stresses the need for accurate documentation during incident response. This guide is a benchmark for incident handling, and falsifying reports contradicts its principles. By following NIST guidelines, I ensure the report is complete, facilitating proper analysis and enhancing future incident response.*
3. ***(ISC)² Code of Ethics:*** *As a cybersecurity professional, adherence to the (ISC)² Code of Ethics is mandatory. The code requires professionals to act with honesty and integrity. The report would violate these ethical standards and damage my personal and professional reputation.*
4. ***False Claims Act:*** *The False Claims Act highlights the legal risks of submitting falsified information, with severe consequences, including legal penalties. If an altered incident report were to be exposed in a forensic investigation, it could lead to lawsuits, fines, or even criminal charges.*

*These guidelines and legal frameworks demonstrate that reporting the incident truthfully is the only responsible course of action. Any deviation from the truth would lead to ethical and professional violations and pose significant legal risks. This evidence collectively supports my position that full transparency and honesty are essential in handling cybersecurity incidents.*

*References*

*Cichonski, P., Millar, T., Grance, T., Scarfone, K., National Institute of Standards and Technology, United States Computer Emergency Readiness Team, & Scarfone Cybersecurity. (2012). Computer security incident handling guide (Rev. 2). NIST Special Publication 800-61.* [*https://nvlpubs.nist.gov/nistpubs/specialpublications/nist.sp.800-61r2.pdf*](https://nvlpubs.nist.gov/nistpubs/specialpublications/nist.sp.800-61r2.pdf)

*(ISC)². (n.d.). (ISC)² Code of ethics.* [*https://www.isc2.org/ethics*](https://www.isc2.org/ethics)

*International Organization for Standardization. (2022). ISO/IEC 27002:2022(en), Information security, cybersecurity and privacy protection — Information security controls.* [*https://www.iso.org/obp/ui/#iso:std:iso-iec:27002:ed-3:v2:en*](https://www.iso.org/obp/ui/#iso:std:iso-iec:27002:ed-3:v2:en)

*Legal Information Institute. (n.d.). False Claims Act. Cornell Law School.* [*https://www.law.cornell.edu/wex/false\_claims\_act*](https://www.law.cornell.edu/wex/false_claims_act)