## Student Guide

# Data Spills Short

### *Introduction*

There are many examples of sensitive information falling into the wrong hands. What's the *worst* that can happen? …The worst *has* already happened.

When data spills occur, they can cause irreparable harm. Adversaries are always listening, waiting for us to make a mistake. Sometimes the consequences can be immediately seen. Other times, they take time to reveal themselves.

What can you do to prevent the worst from happening again? How do you respond when security measures fail?

### *What is a Data Spill?*

Data spills, also known as contaminations or classified message incidents, occur when classified data or controlled unclassified data (CUI) is introduced to an unclassified computer system or to a computer system accredited at a lower classification level than the data being entered.

This may occur either by someone within the organization originating the offending file or files or by someone within the organization receiving the offending file or files.

Examples of situations that can result in a data spill include emails, mismarked files on servers, and improperly marked hard copies or media.

### Categories

Data spills may be inadvertent, willful, or negligent. Regardless of how the data spill occurs, it has the potential of causing grave damage – that is, an *inadvertent* data spill does not have any less potential to cause damage than a *willful* data spill.

Keep in mind that willful and negligent data spills are also classified as *Negligent Discharge of Classified Information* and there are grave consequences for personnel who willfully or negligently engage in a data spill.

Commanders and supervisors at all levels must consider and implement appropriate administrative, judicial, contractual, or other disciplinary actions in any case related to the improper handling of classified information.

| Category | Description | Example |
|---|---|---|
| **Inadvertent** | An incident is *inadvertent* if the person did not know, and had no reasonable basis to know, that the security violation or unauthorized disclosure was occurring. | Reasonably relying on improper markings |
| **Willful** | An incident is *willful* if the person purposefully disregarded DoD security or information safeguarding policies or requirements. | Intentionally bypassing a known security control |
| **Negligent** | An incident is *negligent* if the person acted unreasonably in causing the spillage or unauthorized disclosure. | Careless lack of attention to detail or recklessly disregarding proper procedures |

## *Responding to Data Spills*

Investigation and reporting of classified spills involves use of guidelines for conducting Security Inquiries and Administrative Inquiries (AIs). Organizations should proactively have in place a detailed data spill reaction plan, based upon the appropriate guidance and with approval from the data owner.

The activity security manager or contractor Facility Security Officer (FSO) and associated security personnel are primarily responsible for mitigating data spills, in close coordination with cybersecurity staff. However, *all* personnel working within a classified environment should be aware of the potential for serious threat due to data spills and must know what to do should they occur.

## *Report*

When a potential data spill occurs, immediately report it.

Do not delete the classified data, and do not forward it to anyone else, including security personnel, or you may further the data spill.

Isolate the systems to minimize damage and to preserve evidence that may be required for damage assessment, risk assessment, law enforcement, or counterintelligence purposes.

Be careful when discussing such incidents over unsecured telephones so as not to further endanger any classified information that may be at risk on unclassified systems.

The location and nature of the spill may also be considered classified.

Also note that your participation does not end at reporting. You should actively participate in security incident meetings and response efforts.

### DoD Reporting

DoD personnel report to the appropriate authorities:

- Original Classification Authority (OCA)
- Information owner/originator
- Information System Security Manager (ISSM)*
- Activity Security Manager
- Responsible Computer Incident Response Center

**Formerly known as Information Assurance Manager (IAM)*

### Industry Reporting

Industry personnel report to the appropriate authorities:

- Facility Security Officer (FSO)
- Information System Security Manager (ISSM)
- Information System Security Officer (ISSO)

### *Assess Risk*

Once the data spill is reported, the appropriate personnel assess possible risks as a result of contamination, and follow any special guidelines provided by the data owner.

When assessing risk, it is also important to remind users of the potential consequences of data spills: Information could end up with adversaries or in the public domain.

The activity security manager or FSO will immediately coordinate and plan the investigation/cleanup considering detailed information such as: the sender and recipient(s), subject, time and day sent, and the potentially affected systems and peripherals.

If the security inquiry or administrative inquiry confirms that a loss, compromise, or suspected compromise of any classified information occurred, the activity security manager or FSO will submit an initial report distributed via secure channels. If secure channels are not available, the initial report will not include location and/or classification of the spill.

### *Clean Up*

Once the risk assessment is complete, those in charge of the data spill will assign or work with appropriately-cleared personnel during the clean-up effort.

Per the defined Security Plan, only cleared personnel should: Initiate clean-up actions, quarantine impacted systems and peripherals, and continue clean-up actions of all contaminated systems and peripherals.

Specific clean up procedures vary between the DoD and cleared defense contractors.

**DoD Clean Up**

Unless otherwise determined by the information owner, in cases where the spillage occurred within DoD agency-controlled space, sanitization is not required until the affected systems are removed from DoD agency control.

In such cases, the activity security manager ensures spillage is contained and that unauthorized access is precluded, which may include software overwriting of affected data sectors.

Once the media *is* released from agency control, sanitization is required.

The activity security manager must ensure that all known or suspected instances of spillages of classified information are promptly reported and that personnel render full cooperation in any investigation.

Data Spills within DoD Agency Controlled Space

- Ensure spillage is contained
- Ensure unauthorized access is precluded (e.g., overwrite affected data)
- Sanitize the media once the media is released from agency control
- Report instance
- Cooperate in resulting investigation

Industry Clean Up

Industry personnel must properly sanitize all non-volatile devices containing offending files, control, and/or destroy as appropriate. Before sanitization can occur, approved procedures must be on file with DSS and the data owner must provide written authorization. The FSO should conduct a cost analysis prior to undertaking sanitization of the contaminated system hard drives. Sanitization can be time-consuming, the utility may be cost-prohibitive, and it may be more cost-effective to address contaminated drives through degaussing and/or destruction. If it is determined that sanitizing the hard drives is an acceptable method, sanitize the involved hard drives in accordance with National Security Agency (NSA) and National Information Assurance Partnership (NIAP) authorized procedures, and with use of NSA and NIAP-approved software products.

Tag all sanitized hard drives so that they may be tracked and destroyed at the end of their life cycle. In addition, the FSO should receive a written statement from all personnel who sent or received the offending file or files and all cleared IT personnel who sanitized the devices. The FSO must then submit a final report of findings, determinations, clean-up activities, and other pertinent information. The FSO also coordinates storage and transfer methods of classified information and other evidence with applicable security personnel.

*Note:* Procedures for clean-up of Top Secret spills must adhere to government contracting activity (GCA)-approved procedures, but, at a minimum, should include the procedures included here.

Prior to sanitization:

- Ensure approved procedures are on file with DSS and data owner approves
- Conduct cost analysis to determine if degaussing and/or destruction is more cost effective

Sanitization:

- Use NSA and NIAP-authorized procedures and products
- Tag all sanitized hard drives

FSO:

- Gets written statements from both personnel involved in actual incident and the resulting clean up
- Submits final report
- Coordinates storage and transfer of classified material and evidence

### *What Would You Do?*

Question 1: *Which of the following situations should be treated as a data spill?*

- ☐ A printed report's cover page is marked CONFIDENTIAL. The report contains information marked SECRET.
- ☐ A document marked SECRET is received on an information system accredited and marked as TOP SECRET.
- ☐ An email marked SECRET is received on an unclassified system.
- ☐ A server accredited at the SECRET level stores files marked TOP SECRET.

Question 2: *You receive a classified document in an email on an unclassified system. What should you first do?*

- ○ Immediately delete it.
- ○ Immediately forward the email to your IT support personnel.
- ○ Immediately report it.
- ○ Immediately contact the originator to alert them of their mistake.

Question 3: You discover files marked SECRET on a server accredited to store CONFIDENTIAL material. You've reported the incident and the risk assessment concluded it should be cleaned up immediately. What should the appropriate personnel do now?

- ○ Enlist all the help they can get to ensure a quick clean up.
- ○ Ensure that personnel are appropriately cleared.
- ○ Leave clean up duties to IT personnel.

## *Answer Key*

Question 1: *Which of the following situations should be treated as a data spill?*

- ☑ A printed report's cover page is marked CONFIDENTIAL. The report contains information marked SECRET.
- ☑ An email marked SECRET is received on an unclassified system.
- ☑ A server accredited at the SECRET level stores files marked TOP SECRET.

***Feedback****: Data spills can occur in emails, mismarked server files, or improperly marked hard copies or media.*

Question 2: *You receive a classified document in an email on an unclassified system. What should you first do?*

- ⊙ Immediately report it.

***Feedback****: Immediately report all instances of data spills or suspected data spills. Do not delete the information or forward it.*

Question 3: You discover files marked SECRET on a server accredited to store CONFIDENTIAL material. You've reported the incident and the risk assessment concluded it should be cleaned up immediately. What should the appropriate personnel do now?

- ⊙ Ensure that personnel are appropriately cleared.

***Feedback****: Per the defined Security Plan, only cleared personnel should be involved in clean up actions.*

## *Summary*

This Short examined the procedures for addressing data spills. It is important you are vigilant in following these procedures ensuring the protection and safeguarding of classified information… and ensuring that the worst does not happen once again.