Data Spills

Introduction

Screen Text/Images: Computer monitor with six pairs of hands, each holding a smartphone. On the monitor it reads, "This presentation contains classified information." On the bottom of the monitor it reads, "Unclassified Computer System."

Narration: There are many examples of sensitive information falling into the wrong hands.

Screen Text/Images: A globe with dots bouncing throughout the globe to give the appearance of data jumping from one place to another. A banner appears over the globe which reads, "Prevent data spills in your organization. Know how to respond."

Narration: When data spills occur, they can cause irreparable harm. Adversaries are always listening, waiting for us to make a mistake. What can you do to prevent data spills in your organization? How do you respond when security measures fail?

What is a Data Spill Incident?

Screen Text/Images: A data spill incident is when classified data is introduced to an unclassified computer system or a system authorized at a lower classification. Any data spill will involve an Administrative Inquiry (AI) for the facility concerned.

A document marked secret with an arrow pointing to laptop, tablet, and smart phone. A second document marked secret with an arrow pointing to a computer.

Narration: Data spills occur when classified data is introduced to an unclassified computer system or a system authorized at a lower classification. 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.

Screen Text/Images:

A text box appears. In the text box are four images; an email icon, a man standing in a server room, paper that is marked Top Secret, and a man at a copy machine.

A text box with the following text on it:

Examples of situations that can result in a data spill include:

- Emails
- Mismarked files on servers
- Improperly marked hard copies or media
- Copying of classified documents on an unclassified copier

Narration: Examples of situations that can result in a data spill include:

- Emails
- Mismarked files on servers
- Improperly marked hard copies or media
- Copying of classified documents on an unclassified copier

Knowledge Check

Screen Text/Images:

Knowledge Check

Which of the following situations should be treated as a data spill?

Select all that apply, then select Submit.

A. □ An article in an online forum that contains unmarked classified information.

B. □ A document marked SECRET is received on an information system classified and marked as TOP SECRET.

C. □ An email marked SECRET is received on an unclassified system.

D. □ A server classified at the SECRET level stores files marked TOP SECRET.

Knowledge Check with answers and feedback

Which of the following situations should be treated as a data spill?

Select all that apply, then select Submit.

A. ☑ An article in an online forum that contains unmarked classified information.

B. □ A document marked SECRET is received on an information system classified and marked as TOP SECRET.

C. ☑ An email marked SECRET is received on an unclassified system.

D. ☑ A server classified at the SECRET level stores files marked TOP SECRET.

Correct Answer: The correct answers are an article in an online forum that contains unmarked classified information, an email marked SECRET is received on an unclassified system, and a server classified at the SECRET level stores files marked TOP SECRET.

Categories of Data Spills

Screen Text/Images: Select each category.

Narration: There are three types of data spills; Inadvertent, Willful, and Negligent.

Screen Text/Images: Three tabs on the screen named Inadvertent, Willful, and Negligent.

Inadvertent Tab: An incident is inadvertent if the person did not know or had no reasonable basis to know that the security violation or unauthorized disclosure would occur.

Willful Tab: An incident is willful if the person purposefully disregards or circumvents DoD security or information safeguarding policies or requirements.

Negligent Tab: An incident is negligent if the person acted unreasonably in causing the spillage or unauthorized disclosure.

Narration: Regardless of how the data spill occurs, it has the potential of causing grave damage. An inadvertent data spill does not have any less potential to cause damage than a willful data spill.

Simulation Exercise

Screen Text/Images: Bob sitting at his desk.

Narration: Bob’s workstation is unclassified.

Screen Text/Images: Close-up view of Bob monitor with Outlook running.

Narration: He receives an email from another coworker and opens it.

Screen Text/Images: Bob is on the phone. A magnified view of Bob's phone that reads, "Not a secured line."

Narration: Bob's phone is on an unsecured line.

Screen Text/Images: A pop-up with a picture of Mary. The text says, "Hello Bob. What can I do for you?"

Narration: Hello Bob. What can I do for you?

Mary: Hello Bob. What can I do for you?

Screen Text/Images: A pop-up with a picture of Bob. The text says, "Mary, can you come to my office. I have an email I need your advice on."

Narration: Mary, can you come to my office. I have an email I need your advice on.

Screen Text/Images: Mary standing in Bob's office, next to his desk.

Narration: Mary, I just received an email and it indicates the contents are secret. What should I do? Should I delete the email, forward it to IT, what?

Learning Activity

What is the first thing Bob should do?

Select the correct response, then select Submit.

A. ○ Immediately delete it.

B. ○ Immediately forward the email to his IT support personnel.

C. ○ Immediately report it.

D. ○ Immediately contact the originator to alert them of their mistake.

Learning activity with answer and feedback:

What is the first thing Bob should do?

Select the correct response, then select Submit.

A. ○ Immediately delete it.

B. ○ Immediately forward the email to his IT support personnel.

C. ● Immediately report it.

D. ○ Immediately contact the originator to alert them of their mistake.

Correct Answer: Immediately report it.

Responding to Data Spills

Screen Text/Images: Mary standing in Bob’s office.

Narration: Mary: Bob, you should never delete the files or email of a data spill until you are directed to do so. It will be important to have the file during the investigation of the data spill. Nor should you forward the data spill file or email to IT as this may further the spill. It is important to contain any data spills. Our incident response plan provides guidance on how to contain a data spill. The first thing you should do is to report the data spill.

Bob: Who should I report the incident to?

Mary: You will find that in the Incident Response Plan.

Screen Text/Images: The binder on Bob’s desk is highlighted to indicate this is a hot spot. Selecting the binder gives a close-up view of the binder that reads, “Incident Response Plan, which opens to the table of contents.” A pop-up appears that reads, “REPORTING AND NOTIFICATION.” This pop-up is highlighted to indicate it is a hot spot

Narration: Next, select the Reporting a Data spill from the table of contents.

Screen Text/Images: A pop-up appears which contains the REPORTING AND NOTIFICATIONS information including who to report the spillage to and this person’s phone number. A pop-up in the lower left corner of Bob’s phone which says “Not a secure line” appears.

Learning Activity

Screen Text/Images: Bob calls the Activity Security Manager to report the data spill incident. What information should he provide the Activity Security Manager?

Select all that apply, then select Submit.

A. □ The time the data spill incident occurred.

B. □ The location of the data spill.

C. □ The nature of the data spill.

D. □ How the data spill incident was discovered.

Learning activity with correct answer and feedback.

Bob calls the Activity Security Manager to report the data spill incident. What information should he provide the Activity Security Manager?

Select all that apply, then select Submit.

A. □ The time the data spill incident occurred.

B. ☑ The specific location of the data spill.

C. ☑ The nature of the data spill.

D. □ How the data spill incident was discovered.

Feedback:

Since Bob is not on a secure line, he should not provide the Activity Security Manager the specific location of the data spill and the nature of the data spill.

Reporting Data Spills

Screen Text/Images:

Data Spills

- Immediately report the data spill.
- Do not delete or forward the classified data.
- Isolate the system to minimize damage and preserve evidence.
- Use caution when discussing the incident over the phone.
- Consider that the location and nature of the spill may be classified.

To learn more, select each reporting procedure.

Narration: 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. 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. The location and nature of the spill may also be considered classified. To learn more, select each reporting procedure.

Screen Text/Images: Interactive images of a soldier on the phone and the image of a civilian on the phone. Image of the soldier on the phone is labeled DoD Reporting; image of the civilian on the phone is labeled Industry Reporting.

DoD Reporting popup: DoD personnel report to the appropriate authorities:

- Original Classification Authority (OCA)

- Information owner/originator
- Information System Security Manager (ISSM)
- Activity Security Manager
- Activity Computer Incident Response Center

Industry Reporting popup: Industry personnel report to the appropriate authorities:

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

Scenario Exercise, cont.

Screen Text/Images: Bob sitting at his desk, talking on the phone.

The phone rings.

A pop-up with an image of someone from the Office of the Activity Security Manager. The pop-up reads, “Office of the Activity Security Manager. How can I help you?”

Narration: Office of the Activity Security Manager. How can I help you?

Screen Text/Images: A pop-up with an image of Bob. The pop-up reads, “I want to report a data spill incident.”

Narration: I want to report a data spill incident.

Screen Text/Images: A pop-up with an image of someone from the Office of the Activity Security Manager. The pop-up reads, “What is the nature of the data spill?”

Narration: What is the nature of the data spill?

Screen Text/Images: A pop-up with an image of Bob. The pop-up reads, “I am not calling on a secure phone line. I am located in Building 101. I’ll meet someone from your office in the lobby.”

Narration: I am not calling on a secure phone line. I am located in Building 101. I’ll meet someone from your office in the lobby.

Screen Text/Images: A pop-up with an image of someone from the Office of the Activity Security Manager. The pop-up reads, “That’s fine. I will send someone there immediately. In the meantime, notify the sender and recipients of the suspected spillage without going into too much detail so they won’t send it further.”

Narration: That's fine. I will send someone there immediately. In the meantime, notify the sender and recipients of the suspected spillage without going into too much detail so they won't send it further.

Screen Text/Images: The scene changes to the lobby of the building. Bob and Ron, from security personnel are now in the lobby shaking hands. A pop-up appears that reads, "Hi, I'm Ron from the Activity Security Manager's office. I was sent to investigate the data spill."

Narration: Hi, I'm Ron from the Activity Security Manager's office. I was sent to investigate the data spill.

Screen Text/Images: A pop-up with an image of Bob. The pop-up reads, "Hi Ron, I'm Bob. Let's go upstairs to my office."

Narration: Hi Ron, I'm Bob. Let's go upstairs to my office.

Screen Text/Images: The scene is not inside the elevator looking at Bob's and Ron's backs. The elevator door closes. Then, the elevator door opens with a different scene in the background. Next, the scene changes to Bob's office with Bob sitting at his computer. Ron is standing next to Bob.

The next scene is in Bob's office with Bob at his computer and Ron standing next to him. A pop-up appears that reads, "Can you please log into the system so I can take a look? I will need to access your computer to investigate the incident."

Narration: Can you please log into the system so I can take a look? I will need to access your computer to investigate the incident.

Screen Text/Images: The scene now is Ron sitting at Bob's computer and Bob is standing next to Ron. A pop-up appears that reads, "Once I identify the data spill, I will need to conduct a risk assessment before I can take further action."

Narration: Once I identify the data spill, I will need to conduct a risk assessment before I can take further action.

Assessing Risk

Screen Text/Images: Bob and Ron are at Bob's desk. Now, the image is faded.

Assessing Risk

- Follow any special guidelines provided by the data owner.
- Remind user of potential consequences.

Activity Security Manager/Facility Security Officer (FSO)

- Coordinate and plan investigation and cleanup.
- If compromise is confirmed, submit initial report via secure channels. If secure channels are unavailable, do not report specific location or classification of the spill.

Narration: Once the data spill is reported, the appropriate personnel will 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 general public.

Once the extent of the spillage is determined and the exact location of information systems is known, the Activity Security Manager or FSO will immediately coordinate with the data owner 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 administrated 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 secured channels. If secure channels are not available, the initial report will not include location and/or classification of the spill.

Cleanup

Screen Text/Images: Ron is sitting at Bob's workstation. A pop-up appears that reads, "The risk assessment shows there is contamination from the data spill. We will have to initiate cleanup actions." (Ron speaking)

Narration: The risk assessment shows there is contamination from the data spill. We will have to initiate cleanup actions.

Screen Text/Images: A pop-up appears that reads, "Is this going to take long?" (Bob speaking)

Narration: Is this going to take long?

Screen Text/Images: A pop-up appears that reads, "Since the workstation is within DoD agency-controlled space, the cleanup shouldn't take too long."

Narration: Since the workstation is within DoD agency-controlled space, the cleanup shouldn't take too long.

Screen Text/Images: The screen grays out.

Cleanup

- Assign or work with appropriately cleared personnel.

Per Security Plan, only cleared personnel may:

- Initiate cleanup actions

- Quarantine impacted systems and peripherals
- Continue cleanup actions

Two buttons appear on the screen. One reads, “DoD Cleanup”, the other button reads, “Industry Cleanup”

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

According to the defined Security Plan, only cleared personnel should initiate cleanup actions, quarantine impacted systems and peripherals, and continue cleanup actions of all contaminated systems and peripherals.

Specific cleanup procedures vary between the DoD and cleared defense contractor.

To learn more, select each procedure.

DoD Cleanup

Screen Text/Images: Data Spill within DoD Agency-Controlled Space. An aerial view of the Pentagon.

Unless otherwise determined by the information owner, sanitization is not required until the affected systems are removed from DoD agency control.

- Ensure spillage is isolated and contained.
- Ensure unauthorized access is precluded (e.g., overwrite affected data).
- Sanitize the media once the media is released from agency control.
- Once the extent of the spillage is determined and exact location of information is known, submit final report.
- Cooperate in resulting investigation.

Narration: 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 preluded, 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 spillage of classified information are promptly reported and that personnel render full cooperation in any investigation.

Industry Cleanup

Screen Text/Images: A couple of modern looking buildings. Data Spills within Industry

Properly sanitize all nonvolatile devices containing offending file(s), control and/or destroy as appropriate.

Prior to sanitization:

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

Sanitation:

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

FSO:

- Get written statements from all personnel involved in actual incident and the resulting cleanup.
- Submit final report.
- Coordinate storage and transfer of classified material and evidence.

Narration: Properly sanitize all nonvolatile devices containing offending file(s), control and/or destroy as appropriate.

Before sanitization can occur, approved procedures must be on file 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. The use of NSA and NIAP-approved software products are the only authorized software products that can be used.

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.

Knowledge Check

Screen Text/Images: You discover files marked SECRET on a server accredited to store CONFIDENTIAL material. You've reported the incident and Risk Assessment concluded it should be cleaned up immediately. What should the appropriate personnel do now?

Select the correct response, then select Submit.

A. ○ Enlist all the help they can get to ensure a quick cleanup.

B. ○ Ensure that personnel performing the cleanup are appropriately cleared.

C. ○ Leave cleanup duties to IT personnel.

Knowledge Check with answer and feedback

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

Select the correct response, then select Submit.

A. ○ Enlist all the help they can get to ensure a quick cleanup.

B. ● Ensure that personnel performing the cleanup are appropriately cleared.

C. ○ Leave cleanup duties to IT personnel.

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

Summary

Screen Text/Images: Ron and Bob standing it Bob's doorway shaking hands. To the right is an image of magnified Word document marked SECRET. An image of a piece of paper marked SECRET with an arrow pointing to a computer.

The image of Ron and Bob grays out with the following text appearing on the screen:

We discussed:

- Who to contact if you discover a data spill
- Response procedures that follow.
- How to spot a real or potential data spill
- The process of assessing the damage
- The process for cleaning the data spill.

It is imperative that anyone working with classified information be diligent in handling such information and know exactly how to respond to a data spill.

Narration: Data spills, whether inadvertent, through neglect, or a willful act can all have the same devastating effect on national security.

This course provided an introduction to data spills for DoD military, civilian, and contractor personnel. It described who to contact if you discover a data spill and the response procedures that follow. The course discussed how to spot a real or potential data spill and the actions necessary to quickly prevent further spread of the contamination and the processes of assessing the damage and cleaning the data spill before our adversaries can get hold of and exploit this vital information.

It is imperative that anyone working with classified information be diligent in handling such information and know exactly how to respond to a data spill.

Conclusion

Screen Text/Images: Ron and Bob standing in Bob's doorway. The image is grayed out. A pop-up appears that reads, "Congratulations! You have completed the Data Spills Course."

Narration: Congratulations! You have completed the Data Spills Course.