sologic
Logical analysis | Powerful solutions

2501 Washington Street
Midland, MI 48642, USA
info@sologic.com

sologic in the media

Evidence Preservation – Step By Step

By Brian Hughes, Vice President of Sologic

A version of this article was featured an issue of *Professional Safety* magazine.

Looking back at your last incident investigation, did you experience anything like this?

- While attending to the needs of injured and distressed employees, time-sensitive evidence was missed.
- While securing the area and bringing it back to a safe mode, circumstances that could have served as evidence had to be altered.
- In the bustle to minimize costly downtime, resuming production rushed the evidence collection process.
- A piece of critical evidence disappeared.
- The legal department wished it had more to demonstrate due diligence.
- A regulatory body's requirement or request could not be fulfilled.

In the rush to return to a state that resembles 'normal,' the importance of evidence collection and preservation can be overlooked or overpowered by other priorities.

Evidence is critical to any incident investigation because it is the data that supports the conclusions of the investigation. The primary intent of an incident investigation is to identify effective solutions. In order to accomplish this, the investigation needs to uncover causes and how they relate to one another. Evidence provides support for what the team concludes to be causes. It cultivates a level of confidence that correlates directly to the quality of the evidence collected. Evidence is the foundation for an investigation – for the investigation team as well as for others reviewing the investigation results and conclusions in the future.

APOLLO A version of this article was published when our team was known as Apollo Associated Services.

Many companies do not have a formal evidence preservation policy in place, so the process is ad hoc – left up to the individual investigator or individuals on the team. Some highly regulated companies, with the nature of their governing regulations, specify requirements for evidence documentation. They tailor their evidence preservation policy to match the requirements of the regulatory agency. But evidence documentation is not necessarily the same as evidence collection or preservation. Certainly regulatory requirements must be considered. However, a policy can be developed that fulfills the objectives of the investigation and the requirements of regulatory agencies.

It's best to decide how to handle evidence *before* an emergency occurs. Develop an evidence preservation policy based upon the needs of your organization and distribute it to everyone who will have the responsibility to carry it out. Include it in training curriculum so people are familiar with the process before they actually need it.

What follows are guidelines that any company can use to develop a simple evidence preservation policy to help ensure evidence is well-managed throughout an investigation.

Step 1: Assess the Significance

Ask a few simple questions in order to document the actual and potential significance of the problem. You don't want to overreact to a relatively benign problem – however, you certainly want to ensure that you accommodate the requirements of an incident that has major significance.

The following questions will help you assess the significance of the problem.

1. Safety: Were fatalities and/or injuries involved?
2. Environmental Impact: Was there a major environmental release?
3. Revenue: What was the impact on revenue? (Money coming into the firm)
4. Costs: What additional expenses were incurred? (Money flowing out of the firm)
5. Frequency: How often has this type of problem happened in the past?
6. Other: Different firms will have unique significance factors to capture, such as regulatory impact, supplier quality rating, employee confidence, drain on customer service department, public image, etc. These should be identified and considered.

P 1.989.835.3402 | TF 1.800.375.0414 | F 1.989.835.3662 | www.sologic.com

Determining risk adds a different, yet potentially important, piece of data to the significance assessment. Risk assessment needs to be balanced with its intended outcome. It can be a complex process involving probabilities and statistics, which yields powerful predictions. Or, it can be a simple process of combining individual scores of probability multiplied by consequence. The simple process is still highly subjective, but is quick and easily understood. However, complexity does not ensure that a model is actually predictive. Either way, remembering that any actual outcome exists within a range of possibilities is important. Simply considering the likelihood that the outcome could have been worse may be enough. For example, if it is reasonable to assume that someone could have been killed, usually this is enough of an assessment to qualify the investigation as being extremely important, upping the ante regarding the formality of evidence preservation.

Impact may also be related to the product or process involved. Will the evidence gathered present a risk to compromising the company's IP? Often, the company has an interest in maintaining confidentiality regarding an incident, and a thorough evidence preservation policy will support this. Assessing the impact allows the investigator to gauge the appropriate approach to preserving evidence. The more significant the event, the more thorough the evidence preservation approach.

Legal has the responsibility to protect the company against litigation, as well as to litigate on behalf of the company. The purpose of an incident investigation is to identify what happened in order to prevent recurrence. These two functions sometimes seem at odds. Legal should not control the course of an investigation. Legal's appropriate function is to control how the information produced by the investigation is managed. The legal department should be involved as soon as possible to ensure the evidence preservation steps align with their responsibility to protect the company.

Step 2: Secure the Scene

When possible, secure the scene of the incident. The purpose is to give the investigation team the opportunity to document evidence and gather information before it is disturbed. This can be crucial to an accurate root cause analysis later. Depending on the incident, you may be required to grant access to additional parties – such as OSHA or the CSB. Get the legal department involved right away to determine those authorized to access the area. Tape the area off and allow access only to authorized personnel. Assign an area gatekeeper responsible for keeping a log of those who enter the controlled area. This log should include the name, company, time in and out, and purpose for entry. If they remove

evidence, document it thoroughly via Step 3 below. Evidence removed may not be physical – it may be pictures or notes. If necessary, identify a secure room to store the evidence.

Step 3: Document and Secure the Evidence

Evidence will come in many forms. Maintain confidentiality and secrecy when required! Ensure that evidence is released only to authorized individuals. Use a log sheet that includes the following information:

- Evidence ID Number: This is a unique identification number that will be associated with this piece of evidence from this point forward.
- Date: What time and date was the evidence collected?
- Location/Source: Where was the evidence collected?
    - Physical Evidence: If dealing with a piece of physical evidence, document as accurately as possible where the evidence was found. Depending on the significance of the event, creating a map of the affected area may be useful. Evidence location can then be documented relative to the incident location.
    - Statements: Statements should be taken from witnesses. Make sure to document each person's name and contact information, as well as their location relative to the incident. This is an initial interview – you may need more information once the formal root cause analysis is under way. However, the interview should be conducted by someone familiar with the root cause analysis process. This will help ensure that questions elicit causes as much as possible and minimize story telling that is jaded by opinion, loyalties, etc.
        - Ensure all proper protocol is followed. Hourly staff may require union representation. Human resources and other departments may need to be involved. There may be protocols for interviewing employees.
    - Computer Data: Ensure that computer data leading up to and following the incident is protected. You may need to identify a system expert to help understand what information

is available and how to interpret it. If possible, get the raw data as well as any screen prints or strip charts. Carefully note the timing of data captures relative to the incident.

- Relative Timing: What was happening relative to the event? Even if the process seems benign at first, you need to know what was happening in the facility leading up to and following the event.
- Procedures: What procedures govern the activities leading up to and following the event? Are these procedures accurate and up to date? Were they followed? Why or why not? It is important to understand the procedural controls and whether or not they are effective.
- Work Orders: What is the state of the maintenance on the system? Are maintenance work orders open or up to date? When was the last time maintenance was performed on the equipment? Was it done to specifications? Were there any changes in parts/materials sourcing? When is the next maintenance activity scheduled?
- Equipment: What is the state of the equipment? Is it in good operational shape? Is it being used in accordance with its intent? If not, why not?
    - Include equipment data, such as asset numbers and other relevant data.
- Photos and Video: Photos and video are extremely useful forms of evidence. Automatic photos or video, such as from a security camera, need to be documented and secured. Take lots of photos – don't worry if you don't use them all. Try to illustrate scale of objects photographed – even compared to something as simple as a hotel key card.
- Samples: Take product samples as soon as possible. This may be helpful later in determining the exact state of the product at the time of the incident.

- Date/Time Checked Out
- Checked Out By: List the person who checked out the evidence. Include contact information. Ensure that only authorized individuals are able to check out evidence.
- Date/Time Checked In: List the date and time the item was checked back in.

P 1.989.835.3402 | TF 1.800.375.0414 | F 1.989.835.3662 | www.sologic.com

- Distribution List: If any item has been copied and distributed, maintain a list of people to whom the item was distributed.

The recommended steps are not exhaustive. Individual companies will find themselves gathering different types of evidence based upon what's pertinent and available. Regardless, an evidence log will be invaluable later if chain of custody needs to be proved, or if the root cause analysis is being reopened for further evaluation or assessment.

Step 4: Destruction of Evidence

Sometimes it is appropriate to destroy evidence after an investigation is completed. While some investigations will require the evidence to be held into perpetuity, most will not. Storing electronic files is easy and doesn't take up much space. However, storing physical parts and equipment may not be necessary. Your legal department should advise regarding evidence maintenance.

Step 5: Refine the Evidence Policy

It is safe to assume that you will not get it right the first time. Conduct a post-investigation review to determine opportunities for improvement. Refine your policy based upon lessons learned and distribute to the organization.

Evidence preservation is crucial to any incident investigation. Approach evidence preservation according to the actual and potential significance of the problem. Developing and becoming familiar with a formal evidence preservation policy tailored to your organization will ensure that you have the data required to complete an accurate analysis – the only path to identifying true causes and pinpointing solutions that effectively reduce risk and prevent recurrence.

Brian Hughes is vice president of Sologic -- provider of root cause analysis consulting, training and software, and of affiliate Artemis Investigations. Brian has led significant incident investigations, including those related to major explosions, chemical releases, consumer product contamination, manufacturing defects and supply chain processes. Brian has helped clients achieve savings in excess of $100 million as well as significant improvements in safety, reliability and quality. For more information, go to www.apollorca.com or contact Brian directly at brian.hughes@sologic.com.

APOLLO A version of this article was published when our team was known as Apollo Associated Services.

Evidence Preservation - 5 Steps

1) **Assess the Significance**
   - How serious is the problem? More serious problems require more stringent evidence management
2) **Secure the Scene**
   - Document and control access
3) **Document and Secure the Evidence**
   - Catalogue evidence and maintain chain of custody
4) **Destroy Evidence?**
   - Most evidence doesn't need to be kept forever. Work with Legal to develop a destruction schedule.
5) **Refine Evidence Policy**
   - Learn from experience - roll lessons into policy - share with others!

APOLLO A version of this article was published when our team was known as Apollo Associated Services.