

From: [Steve Elliot](#)
To: selliot@gmail.com;
CC:
Subject: Business Survival Tips from Elliot Consulting Services
Date: Monday, November 06, 2006 7:32:11 AM
Attachments:



Elliot Consulting Services - Business Survival Tips

Technical Decontamination & Equipment Restoration

November 2006

Greetings!

The real loss to a company's computer and technical equipment occurs *AFTER* the fire is extinguished!

The difference between a "minor disruption" and a "catastrophe" is often times determined by the assessments and decisions (or lack of) made within the first 24 - 48 hours following a fire incident. Understanding the vulnerability of facilities and equipment assets exposed to the perils of fire and the resources to combat them, is often overlooked during the critical stages of the recovery effort. One thing is certain, the first 24 - 48 hours are critical and irreplaceable. The purpose of this article is to provide a general guide to uncovering the unique hazards of equipment damage due to fire and then maximizing the recovery efforts of those assets.

This month's newsletter article on technical decontamination and equipment restoration was written by [Michael Mies](#), General Manager, Technical Services for [Interstate Restoration Group](#). We thank Michael and the entire team from Interstate Restoration for their permission to re-post this article for our readers.

Steve Elliot, CBRM
President and CEO
Elliot Consulting Services

Copyright 2006. Elliot Consulting Services, Inc.

In this Issue

- [Equipment Damage Assessment](#)
- [Useful Links](#)
- [About Elliot Consulting](#)



Interstate
Restoration Group

Equipment Damage Assessment



Consider this scenario:

Beneath the raised floor of a data center's server room, an electrical short within a power distribution box fails to trip a supply breaker and rapidly overheats. Within seconds, the intensity of the heat is sufficient to melt a bundle of cables draped over the box. With ample supply of oxygen provided by the data center's downflow environmental control system, the now smoldering cables emit smoke that overwhelms the entire data center before the smoke alarm is triggered. Within minutes, the main power disconnected is switched off to the computer room and initial response phase of the E-continuity plan is implemented by the on-site IT Manager.

While critical applications are automatically redirected to the pre-established offsite redundant server, the onsite staff begins to clear the affected areas of smoke, powering down the equipment still serviced by the UPS system and taking stock of apparent damages. Within just an hour, it appears that they have a handle on the damage/critical issues and begin to outline a strategic plan to remedy each challenge. The IT Manager and facility management superintendent jointly present an initial incident report to corporate management. The "fill-in-the-blanks" report basically concluded that it was a "nonevent" since damages were essentially limited to an inexpensive power distribution box and replacing the bundled cables feeding a rack of patch panels. The report additionally noted the need to have the data center professionally cleaned and a system-wide equipment check to be conducted by the onsite hardware technicians and contracted service vendors. With an estimated cost of approximately \$15,000 and less than three days to complete repairs with available personnel, the incident barely gets the attention of management.

By the end of the day, additional maintenance and a professional janitorial firm were enlisted and began to remove the smoke residues that blanketed the entire data center and contents. Concurrently, hardware technicians and system engineers were feverishly working to replace the damaged cables and systematically clean the equipment and structure surfaces within the secured computer room. By all accounts, expectations were high for a quick and effective recovery – still considered a "non-event" when everyone met in the morning for a status briefing.

Three days later, the minutes from the status briefing meeting declared total recovery and "business as usual". While still celebrating the "victory", the IT Manager and system engineers continued to combat the system glitches common to emergency shutdowns and re-commissioning. As the last local server was brought back online, the frequency of unusual problems increased dramatically - it became evident that something was seriously wrong.

What went wrong...

Unfortunately, the significance of the "white" residues and "light" smoke contamination was not acknowledged in time to arrest the corrosive reactions and resulting damage. To complicate matters, the cleaning efforts employed by the recovery personnel actually accelerated the corrosive process.

What you need to know . . .

Electronic equipment is particularly susceptible to damage due to heat, water, and combustion by-product residues. A common combustion byproduct of fires in computer and control facilities is hydrogen chloride (HCl). HCl is produced when polyvinyl chloride (PVC)

cable insulation or plastic hardware is exposed to high temperatures. The HCl rapidly reacts with the galvanized zinc encountered in most electronic circuitry and components to form a layer of zinc chloride (ZnCl₂) on the surface of the equipment. Zinc chloride is extremely hygroscopic, and picks up moisture from the surrounding air at as low as 10% RH to form an extremely corrosive zinc chloride solution.

Electronic components are also susceptible to damage from particulates produced by smoldering materials. For example, computer disk drives are susceptible to damage from particulates as small as 0.5 microns in diameter. Smoldering or slow growth fires, characteristic of electrical fires, can produce sizable nonconductive soot particulates (> 0.5 microns) which generally deposit horizontally on equipment. These deposits can form an insulating layer on equipment, impacting contacts and/or cause overheating conditions. In the case of more rapidly growing fires, the amount of organic volatiles produced from the fire is small due to efficient combustion, and conductive soot particulates are then formed. These deposits are comprised of small particulates (< 0.5 microns) and deposit on both vertical and horizontal surfaces. The conductive particulates can lead to electrical shorting.

What could have happened...

Provided the personnel responding to the incident were cognizant of the unique hazards and responded accordingly, most of the equipment could have been successfully restored for a fraction of the cost and downtime that is associated with acquiring and installing replacements.

What needed to be done...

After ensuring that all hazards and life safety issues have been appropriately addressed, the following events should have become priority:

1. Comprehensive Assessments – Attempt to establish total scope of smoke exposure and corrosive potential of residue.
2. Containment - Isolate the affected area and initiate all reasonable measures to prevent migration to other unaffected areas.
3. Preservation – Provide ambient environmental conditions and application of targeted preservation solutions to arrest possible corrosive reactions.
4. Decontamination – Once suitably contained and preserved; a systematic, appropriate and thorough decontamination process must be performed on all equipment and structures harboring residues.
5. Restoration/Repair - Replacement equipment and/or components (those exhibiting indications of actual damage) must not be reinstalled until the facility and enclosures are appropriately decontaminated. Properly conducted, the decontamination process will identify all actual and “suspect” damage at the component level.
6. Re-commissioning – Conduct extensive diagnostic testing and controlled “burn-ins” of equipment as it becomes available after the restoration processing. Where appropriate, engage the OEM or contracted service vendor to inspect, test and re-certify the systems to “pre-incident” status.

Lessons Learned...

A message from the expert

As a twenty-year veteran of the equipment restoration and loss consulting industry I've noticed that this scenario is being played out more frequent over the past few years. Unfortunately, it seems that I routinely receive the call too late to do much more than provide "post-mortem" reports. Aside from the increased venerability of current technologies, it appears that the primary reason for the trend is associated with insurance premiums!

The increased premiums have forced many corporations to assume skyrocketing deductibles. Regrettably, the shift to higher deductibles has outpaced corporate abilities to effectively manage the "self-insured" portion of losses. Just a few years ago, deductibles were so low that almost **ANY** loss triggered a call to the insurance company. Armed with the knowledge of past "lessons learned" and regular access to experienced consultants, the Adjusters were in a position to raise the red flag and take control of the loss **WHEN** needed. Providing "first responders" a little education and awareness of the initial recovery phase of losses will minimize the chances of "non-events" mushrooming to "catastrophic" events.

One disaster is enough -- knowing what to do and who to call early in the loss may determine the difference between a minor disruption and catastrophe!

[Interstate Restoration Group](#) is the country's most respected, independently owned, restoration company specializing in commercial, industrial and medical mitigation due to fire, smoke, wind and water damage. Headquartered in Fort Worth, Texas, with additional response centers throughout the US, Interstate is within hours of any loss in North America. For more information about Interstate Restoration please call 800-622-6433.

Call to action: For more information on equipment damage assessments, technical decontamination & equipment restoration, loss mitigation emergency services, and the full spectrum of restorative services please contact [Michael Mies](#), General Manager, Technical Services for Interstate Restoration, or call him directly at 803-547-8805.

Useful Links

- [Dept of Homeland Security / FEMA](#)
- [Institute for Business and Home Safety](#)
- [Florida Division of Emergency Management](#)
- [National Hurricane Center](#)
- [Tampa Bay Hurricane Guide](#)

About Elliot Consulting



Elliot Consulting Services is a 3 year-old consulting firm based in the Tampa Bay area which specializes in business survival solutions. We help companies create, develop, and implement business continuity plans which are designed to protect their vital business resources and operational processes. ECS will also review, audit, and help modify a company's existing disaster recovery



model to ensure that the essential components of the organization will continue to function in the event of an unplanned disruptive incident. Finally, the team from Elliot Consulting can assist with disaster recovery training exercises to test the thoroughness of a company's preparedness model. Our consultants are certified business continuity planners and business resiliency specialists with Fortune 500 experience. Additional information can be found on the [ECS website](#).

Previous Newsletters

- [Previous Newsletters](#)

email: info@elliott-consulting.com
phone: 813-792-8833
web: <http://www.elliott-consulting.com>

[Forward this newsletter](#)

SafeUnsubscribe®

This email was sent to selliot@gmail.com, by info@elliott-consulting.com
[Update Profile/Email Address](#) | Instant removal with [SafeUnsubscribe™](#) | [Privacy Policy](#).

Powered by



Elliot Consulting Services | 10238 Woodford Bridge Street | Tampa | FL | 33626