Environment, Power and Security Management

A White Paper compiled by
Ecl-ips

Why Monitor the Physical IT Environment?

It's not complicated, if you have visibility of all the devices in your IT Environment/Comms Room/Data Centre (however you want to term it), you can ensure the minimum amount of downtime of your IT network. If your equipment is monitored you will get alerts and early warnings to help you avoid any major issues and downtime.

Losing your IT network for any length of time, whatever the size of your business, will have an impact on your service delivery and will ultimately cost you a lot of money.

In this white paper we will examine the risks, explain some of the terminology and look at some of the benefits to monitoring your IT environment.

What are the Risks?

1. **Human Error**
   Untrained staff could switch off or unplug the incorrect device

2. **Air Conditioning Failures**
   Leading to overheating of equipment

3. **High Temperatures**
   Could lead to servers shutting down due to overtemperature

4. **High or Low Humidity**
   Could cause issues if the air is too dry or too wet within electronic devices

5. **Water Leaks**
   Could lead to power failures or equipment damage

6. **Fire and Smoke**
   Fire and Smoke are a potential threat to any server room or data centre and could be damaging to the rest of the building

7. **Power Failures**
   Downtime for users on the network

8. **Dirty Power**
   Power spikes or uneven power could shorten the life of power supplies

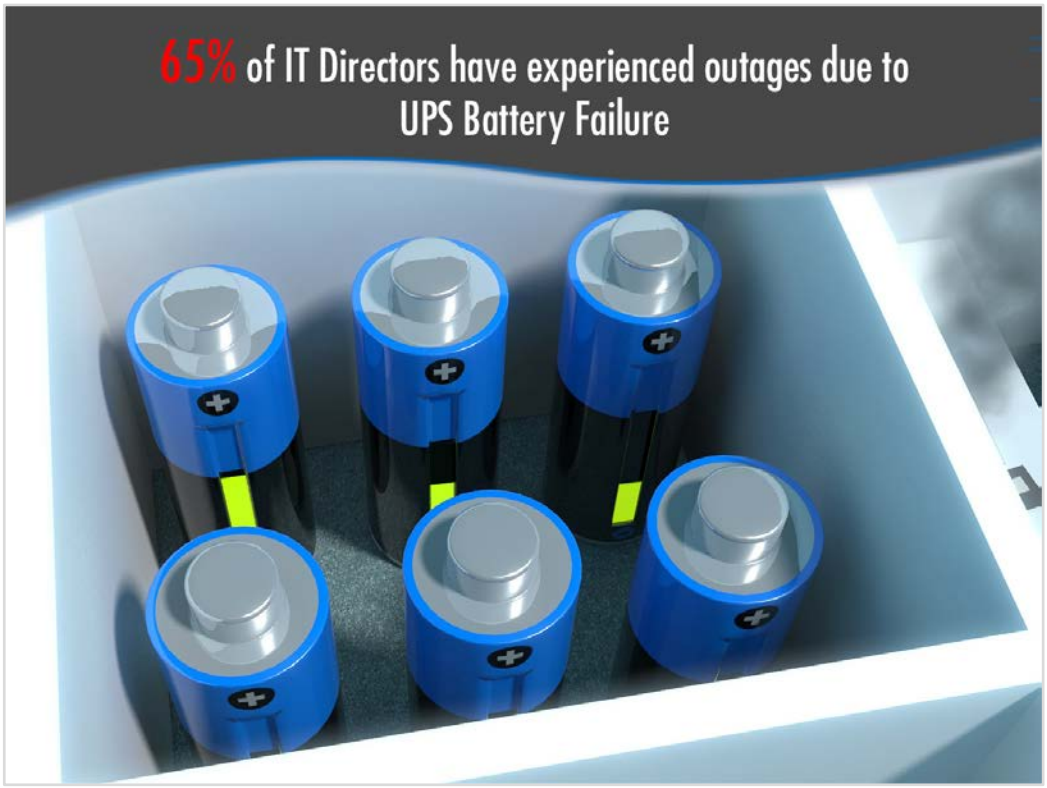
9. **Poorly Maintained UPS devices**
   They don't work when you need them to

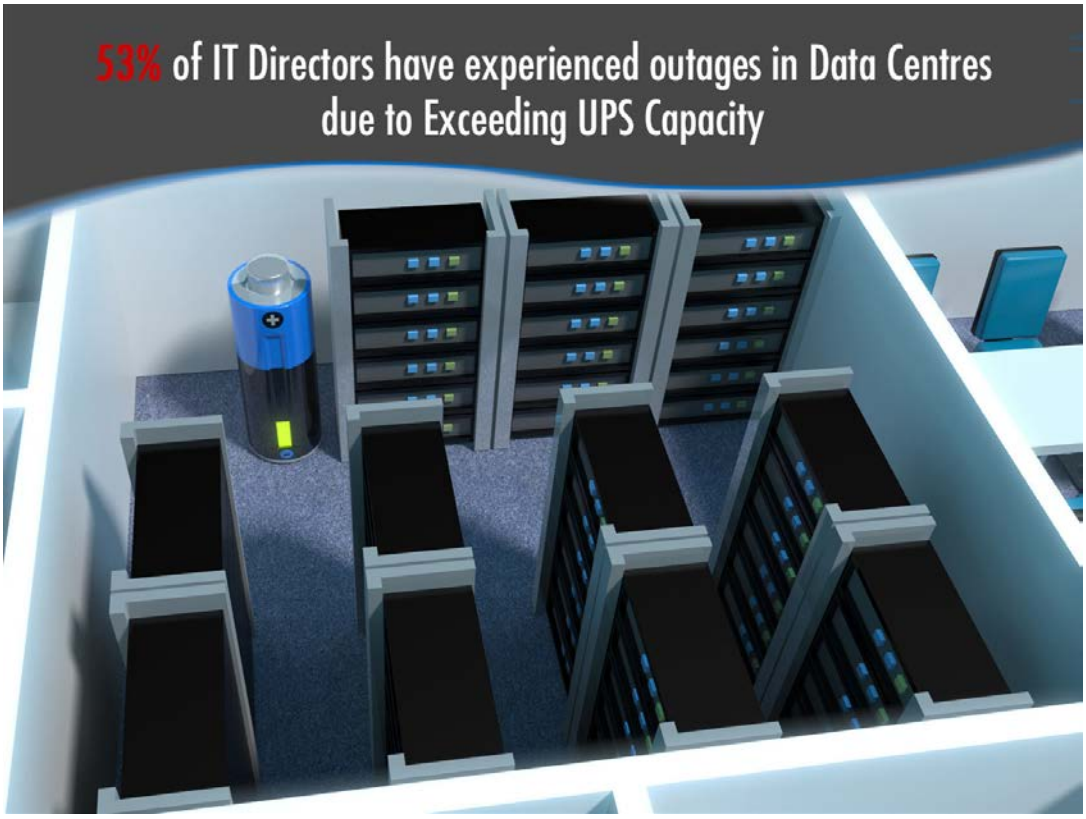
10. **Faulty Servers overheating cabinets**
    Would lead to the devices shutting down

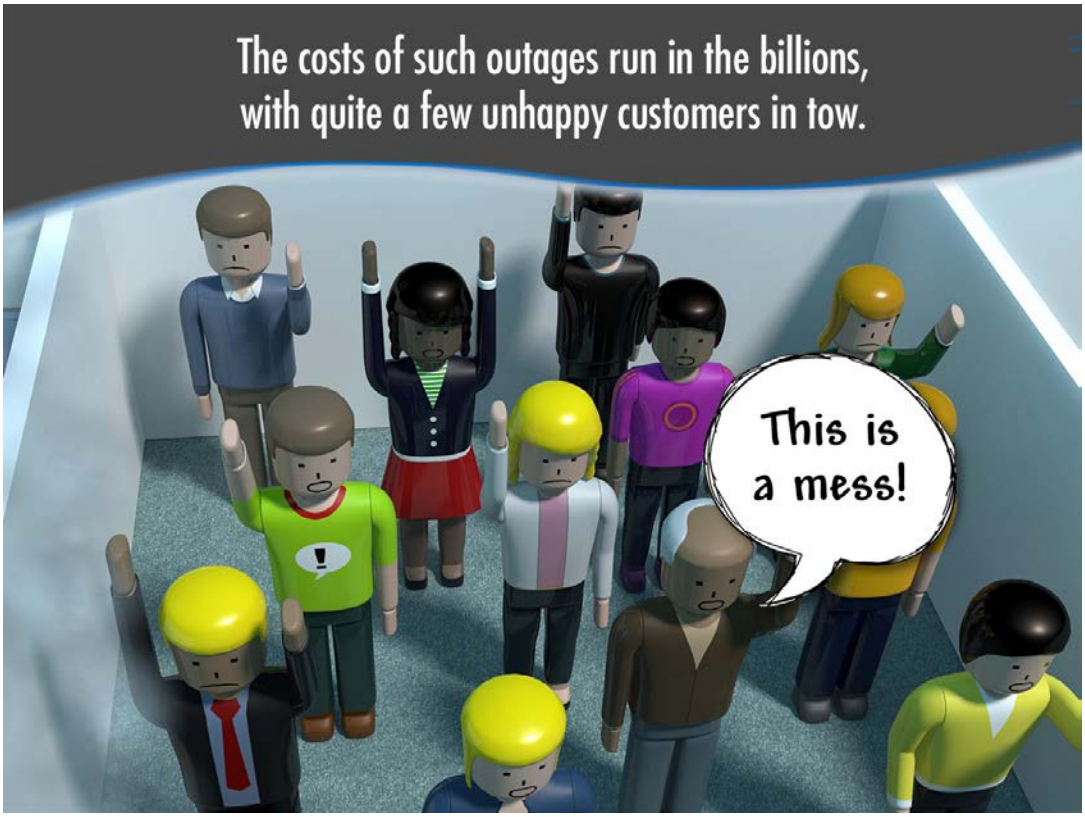
11. **UPS Overload**
    No battery back up in the event of a power failure

12. **Faulty Batteries**
    No battery backup in the event of a power failure and could be a fire hazard

These are the hard facts:







The estimated cost of IT outages in 2009 was $26.5 Billion in North America alone.

What is an IT Environment?

An area, room or building that information technology equipment, such as servers, routers, switches and network storage devices operate, usually within data cabinets.

These areas vary in size from single wall mount or free standing cabinets in communication rooms, to several floor standing cabinets in server rooms and multiple rows of floor standing cabinets in data centres.

Whatever the size of these areas they are critical and are at the hub of any business, any amount of down-time will have an adverse effect and cost.

Physical IT monitoring enables businesses to pre-empt possible failures of IT equipment due to external sources ie; human error, malicious behaviour, burst fluid pipe, air conditioning failure, fire etc. Physical threats are just as important and can have the same devastating results as cyber threats. Many businesses spend a great deal of time and money to track viruses, spyware and network threats and often don't take into account environmental threats such as humidity, high or low temperatures, air flow, smoke and quality of power.

So what's Environmental Monitoring?

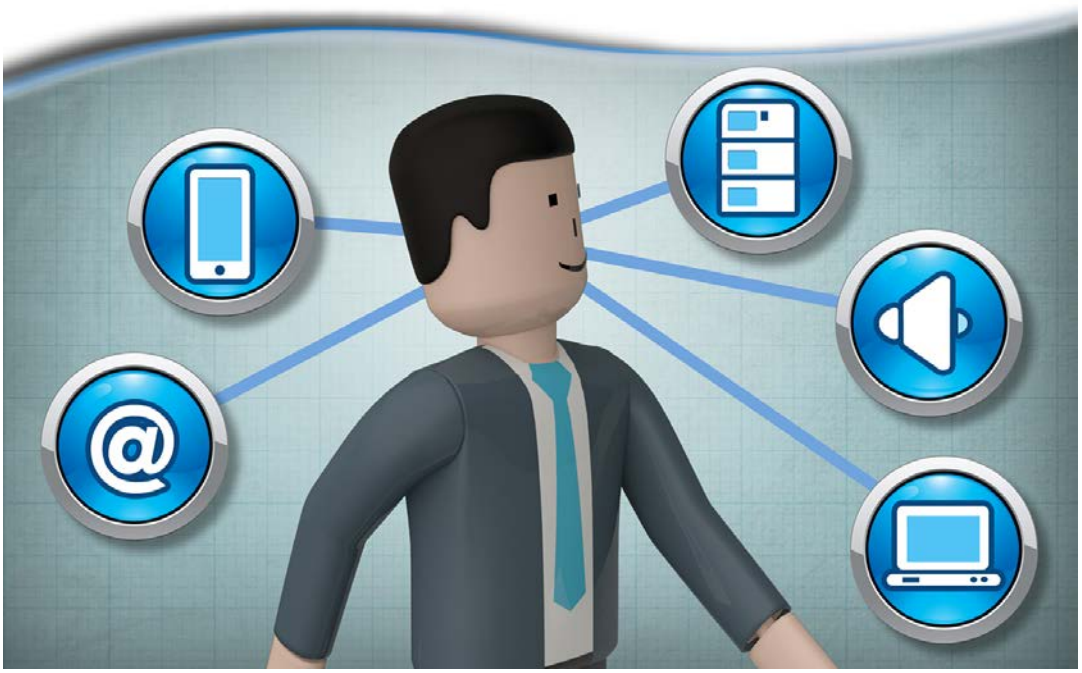
Environmental monitoring within the IT environment provides reading, data capture and alerting mechanisms for early warning of potential threats to the IT system. Physical IT monitoring includes cameras for visual verification and third party integration to interrogate critical devices either across an Ethernet network, BMS network or via a physical cable connection.

Another factor to take into account is unmaintained equipment, this is where any IT physical environment supporting equipment, such as air conditioning units or back up power units (UPS) are in place and not monitored or maintained.

Businesses expect them to work but often don't have a maintenance contract in place, as they become older the likelihood is that problems could occur and in many cases an IT failure highlights the issue and causes downtime and ultimately loss of revenue.

How should physical IT monitoring work?

- It should be deployed across all IT environments ie; not just in the data centre or comms room.
- Each monitored device or monitored area should have a built in web server to allow verified easy access and communication for outgoing alerts.
- The system should have multiple access levels.
- Reporting functionality for analysis of information over a period of time.
- Multiple levels of alerting policies with automatic escalation.
- Notification via Email, SMS, SNMP or Audio.
- The system should include cameras within the same system.



What are the main factors requiring a physical IT monitoring system?

A system can be as cost effective or as feature packed as your budget will allow. To decide on the best system for your business you need to consider the perceived physical threats.

As a starting point we would suggest the following:

- Temperature
- Power
- Moisture
- Human intervention
- Open doors
- Supporting equipment

What are the main components of a physical IT monitoring system?

- **Temperature sensors**
  These can be either wireless or wired and will be measure at various points within the IT environment. Generally just one temperature sensor does not give the granularity required, therefore a number of sensors are required. Many points of IT environments whether they be hot aisle or cold aisle will have different readings.

- **Humidity sensors**
  Again these can be wireless or wired and measure the humidity of the air. The most effective way of measuring humidity is to measure the dew point.

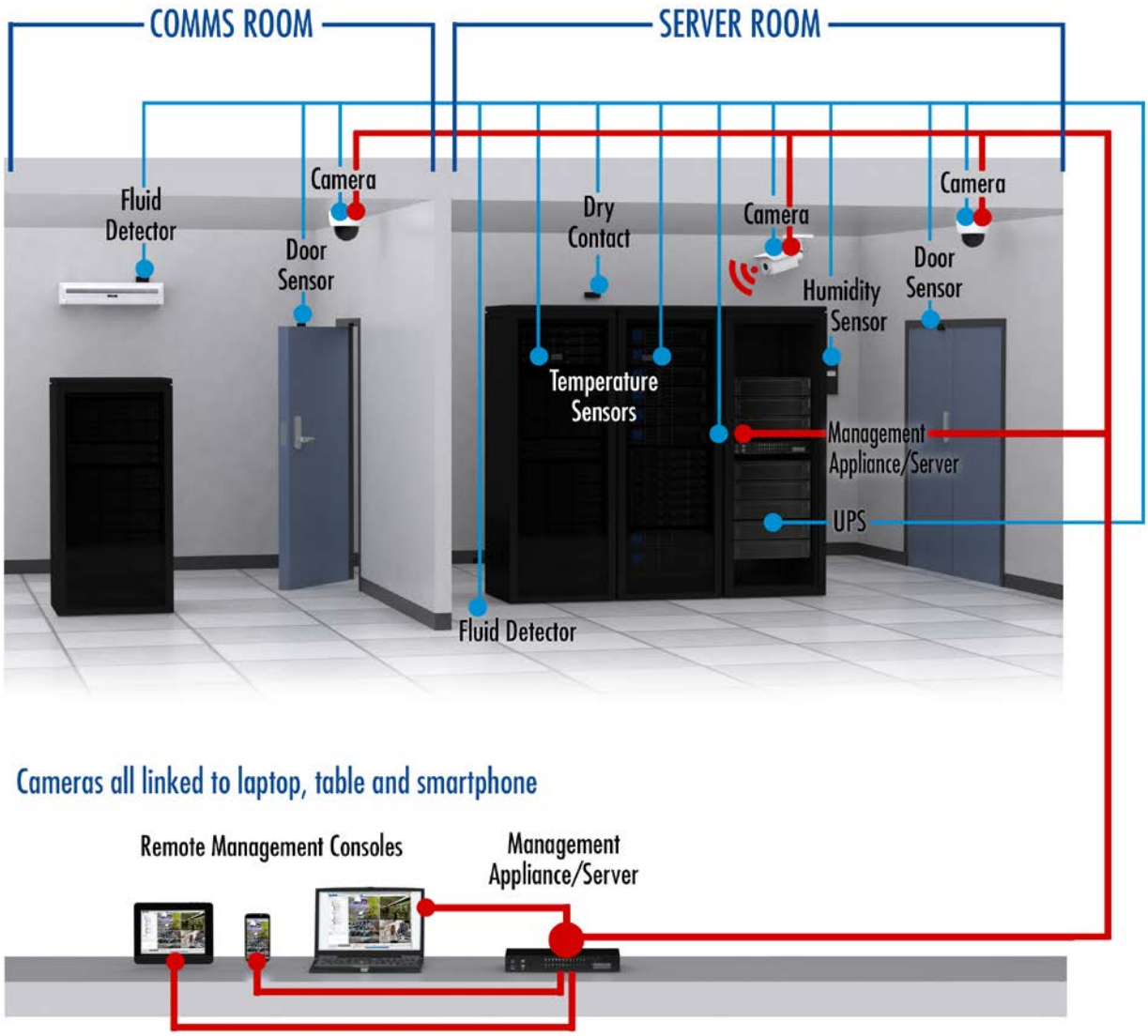
- **Fluid sensors**
  There are two main forms of fluid sensors: a spot fluid sensor that will provide coverage for a small area i.e. air conditioning drip tray and rope sensors that would cover a large area such as a raised floor in a server room or data centre.

- **Smoke sensors**
  These would provide early warning of a fire or someone smoking in a monitored area. These could be positioned in the room or even in each cabinet.

- **Power monitoring**
  This is available to monitor the quality and quantity of power consumed within the IT environment. Very often UPS devices are deployed with very little monitoring therefore when the battery is required to provide back up power it is not available and renders the UPS ineffective. Also understanding how much power you use is now a critical factor for any IT director.

Intelligent Monitoring

Human error reduction can be accomplished through intelligent monitoring at multiple levels, as illustrated in the image below:



Conclusion

IT Environments are areas that can be overlooked as far as active monitoring is concerned especially distributed server rooms and communication rooms. In many circumstances the IT or Facilities departments do not actively monitor these distributed rooms and therefore a server or PoE switch overheating can cause major down time and be the first sign of a failed air conditioning unit.

A real-time monitoring system can provide a proactive link to enable companies to monitor and plan effects on the IT equipment and see any trends associated with additional equipment being deployed. These distributed rooms do not have local IT staff and monitoring these systems can provide the 'Eyes and Ears' for an important link to Regional or Branch offices.

If you don't monitor your IT equipment then you are likely to suffer more downtime – can you afford to take that risk?

About the Author

Aaron Kernaghan, MD has been working in the monitoring environment for over 15 years and in that time has heard all sorts of stories from customers and prospective clients about the issues they have experienced. He has helped a number of organisations, including Local Government, Enterprise and Blue chip to implement real time monitoring systems and alerting processes, ensuring these integrate into their existing systems.