

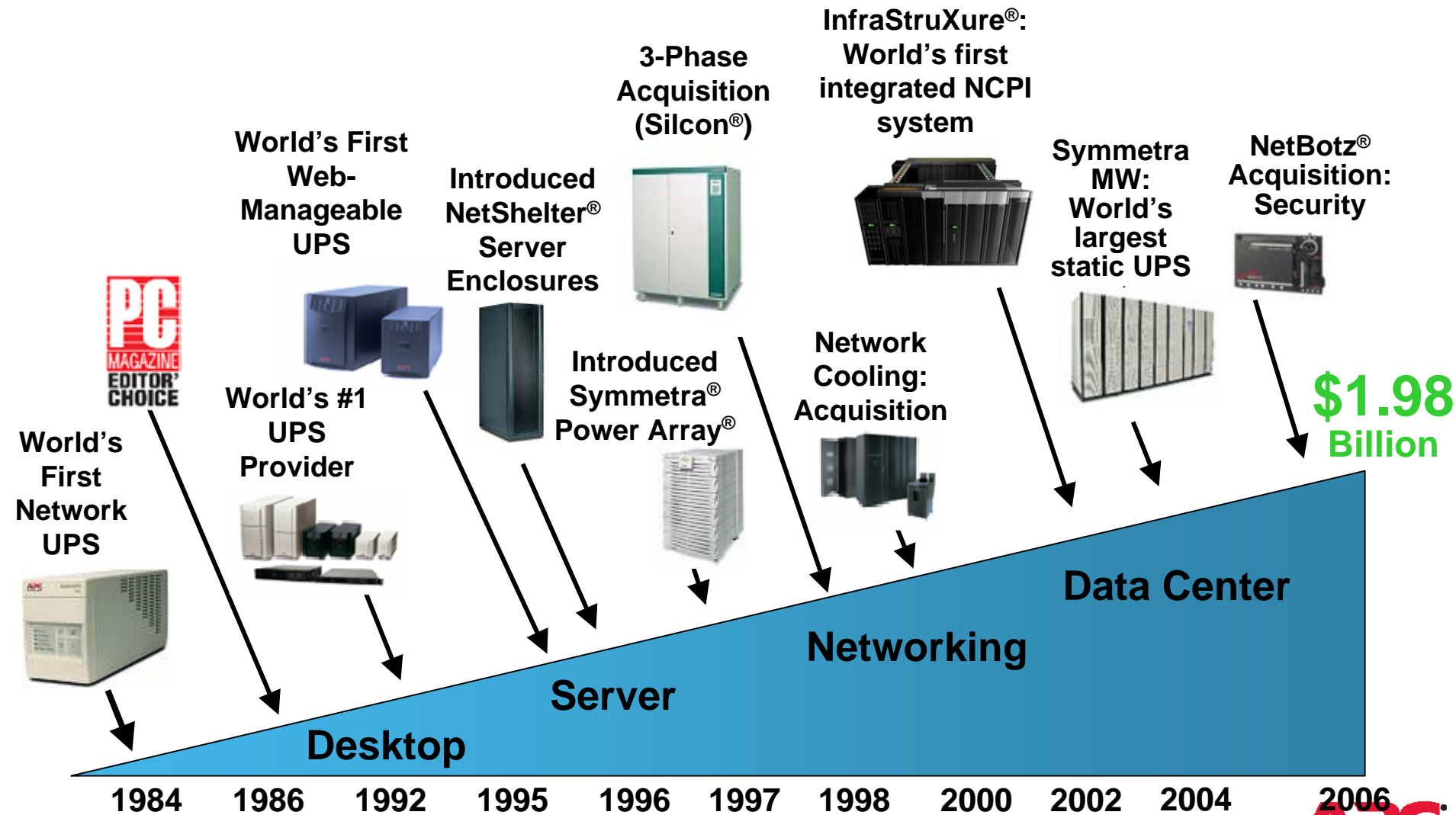
AFCOM – A Conversation about Security and Environmental Monitoring

Scott Cassidy
November 19, 2008

Agenda

- Who am I and Who is APC by Schneider
- Managing the Layers
- Disaster Management and Business Continuity
- Market Trends
- Security and Environment Monitoring
- Compliance and Regulatory – What has that got to do with anything?
- “My Building Management System has me covered”
- Q&A

APC's Progress



Schneider Electric - A Global Company

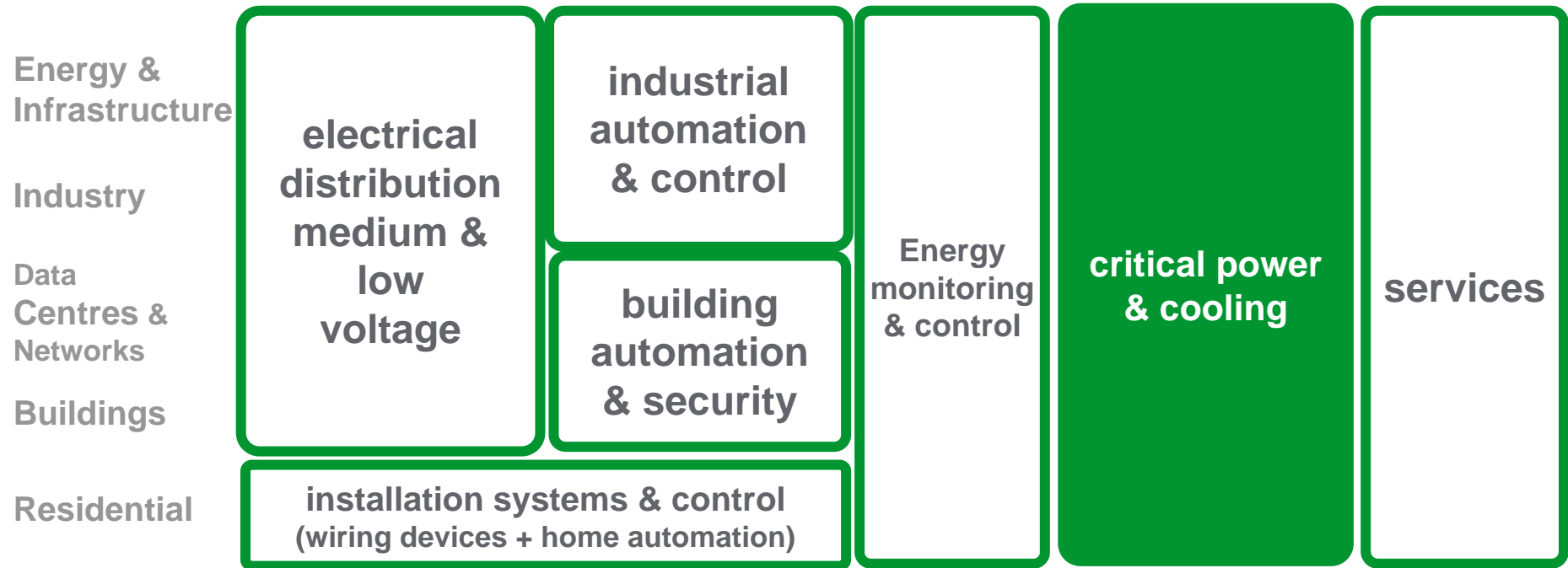
€17.3 billion sales in 2007 (+26% vs. 2006)

120,000 people in more than 100 countries

>200 factories around the world

R&D centres in 25 countries

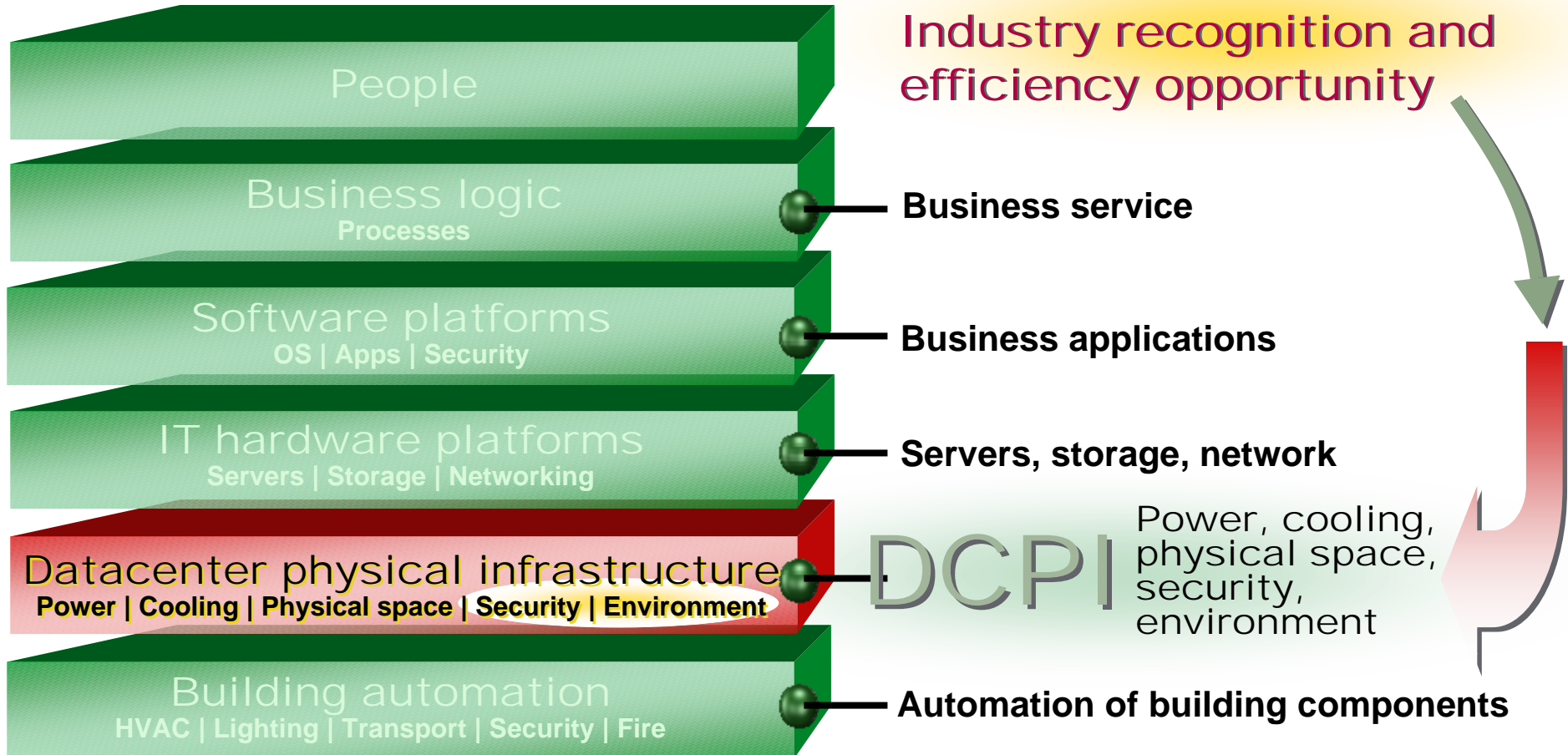
An integrated and balanced portfolio



Test

- Your child says “I’m cold”
 - What do you do?
 - Two options
-
- Give them a blanket
-
- Crank the thermostat

Managing the layers – Physical infrastructure needs attention!



Industry recognition and efficiency opportunity

Why Manage & Monitor the Layers?



A



B

- Need gasoline, oil, brakes, basic engine functions to get to Point B



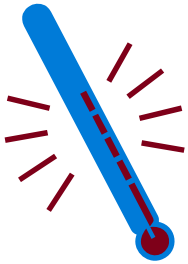
- Gauges alert you to major threats that may prevent you from reaching destination

Why Manage & Monitor?



Goal: Run a "five-nines"
E-Commerce Server

Visibility to Threats to commerce in one place



• Blade Server #3 threatened
due to **Temperature** accelerating
beyond threshold in rack #2

• Physical **Security breach** detected
in network closet
within leased bldg #3



• UPS on battery-
5 minutes runtime
remaining



• SAN threatened
by **water leak** detected
beneath rack #5

Disaster Recovery vs. Business Continuity

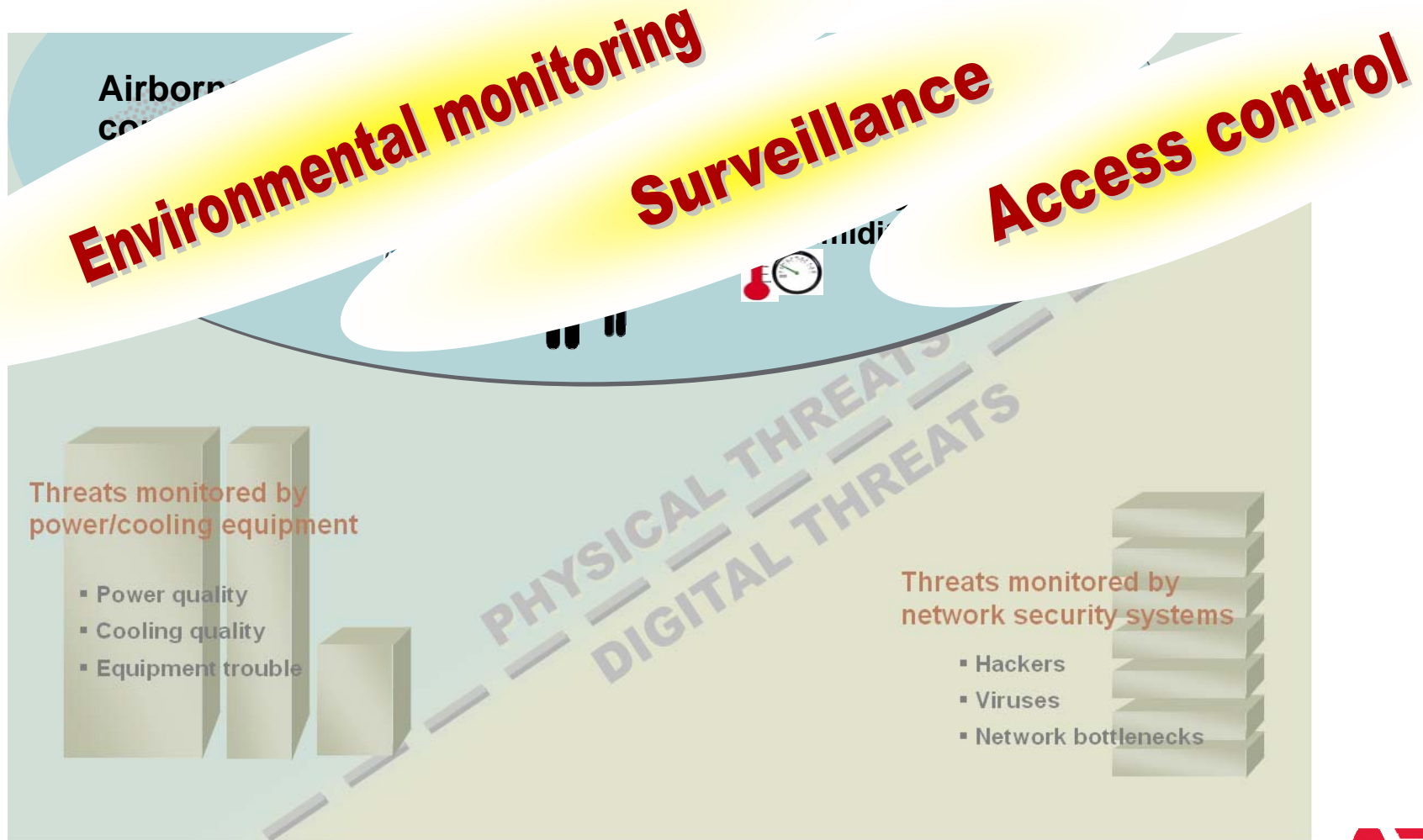
- Disaster Recovery

- Response to an interruption in IT operation by implementing a disaster recovery plan to restore an organization's critical business functions
- Disaster recovery is your plan of action to restore critical functions after a disaster

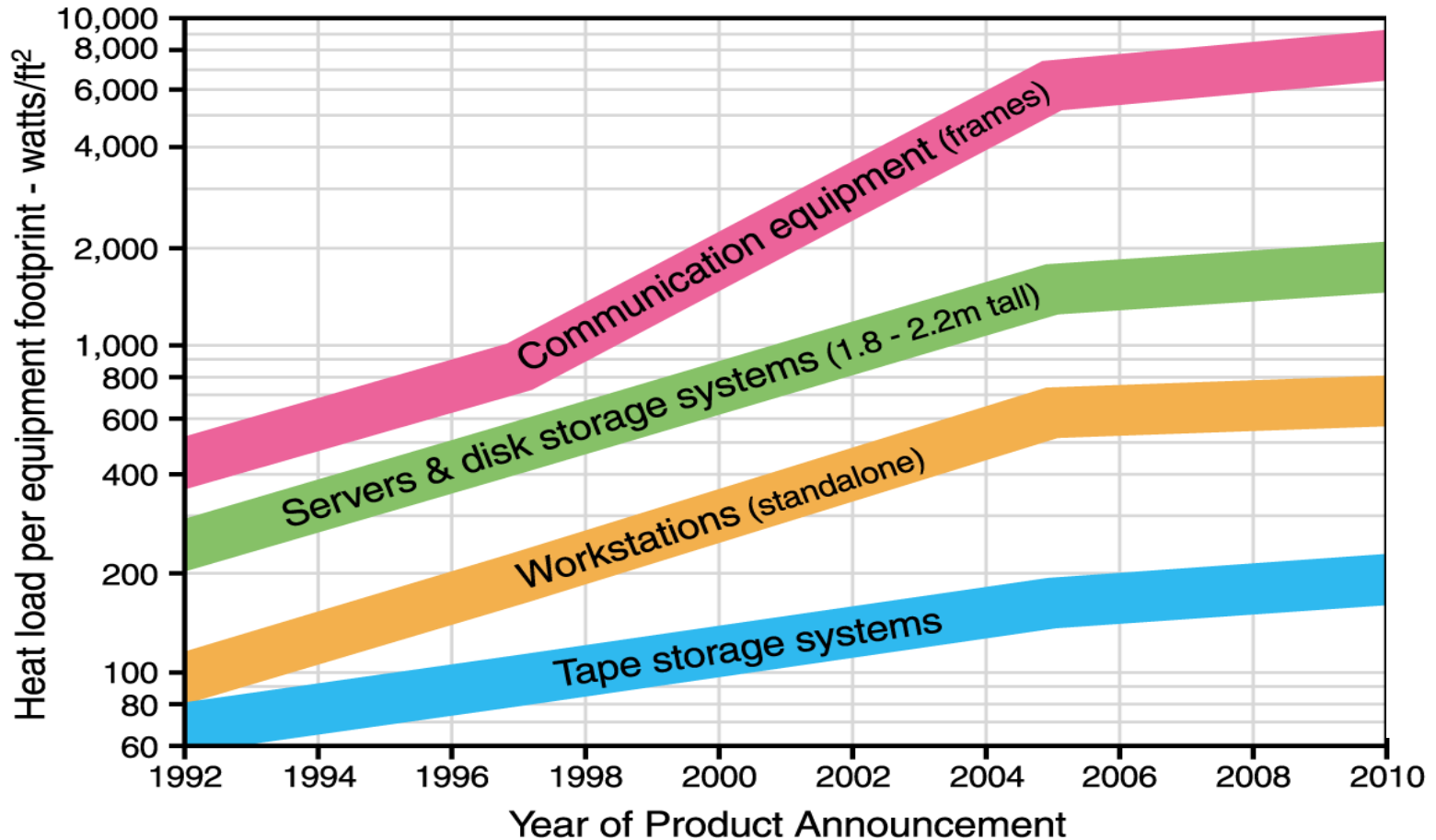
- Business Continuity

- The ability of an organization to ensure continuity of service and support for its customers and to maintain its viability before, during, and after an event
- Builds on Disaster recovery to help you support customers and stay in business

Physical Threats vs Digital Threats



Heat Density Trends

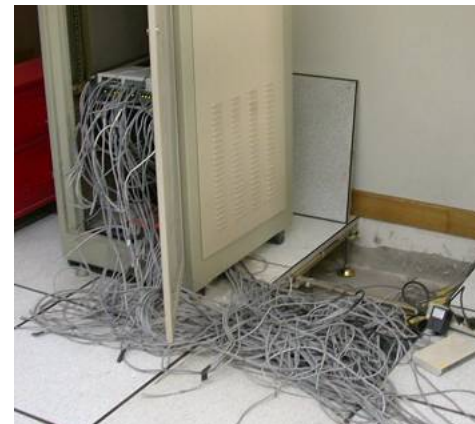


Converged Networks demand higher power consumption & new levels of monitoring.

Source: 2000 The Uptime Institute - Reprinted with permission from a White Paper titled "Heat Density Trends in Data Processing, Computer Systems, and Telecommunications Equipment" v1.0

Environment Poses a Risk to Availability

- Racks were already hot in 2005
 - “10% of all racks are already too hot and fail to meet industry standards for maximum IT reliability and performance.” (Uptime Institute)
 - Virtualization is forcing more processing power out of a smaller space, causing hot spots (Forrester 2008)
 - Need to monitor at rack level is more important because of variance within single rack.
- “For every 15 degrees over 75 degrees your equipment is subjected to, its lifetime being cut in half” (Uptime Institute)
- Technology exists for manufacturers to validate operating condition, compliance
 - Particle sensors, leak sensors



If you cannot verify you are running within operating specifications you will shorten the life of your equipment.

Network Closets are Business Critical

- Power consumption has increased 10X over the past 10 years* (Cisco 2008)
 - VOIP, Network Convergence, PoE
- 97% of all IT spaces are network closets and server rooms
 - Over 2.2 M in NAM alone (IDC 2006)
- VOIP is growing at 26% annually (IDC); \$2.2B market in 2008
- Companies are realizing the criticality of IT spaces (Forrester 2008)
 - 42% percent of IT managers said business continuity and disaster recovery are very important, up from 33 percent from last year.

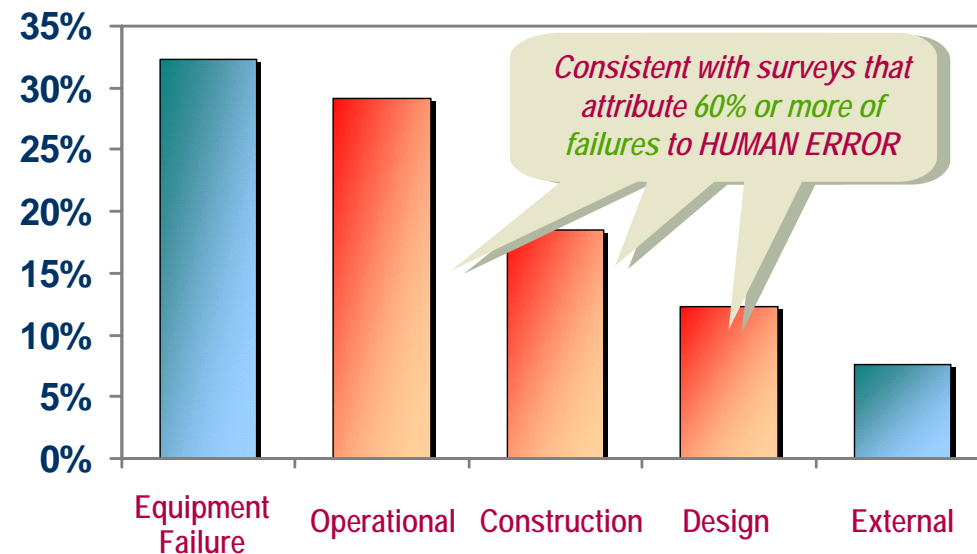


Business critical applications are running in suboptimal environments.

Security is Increasing in Criticality

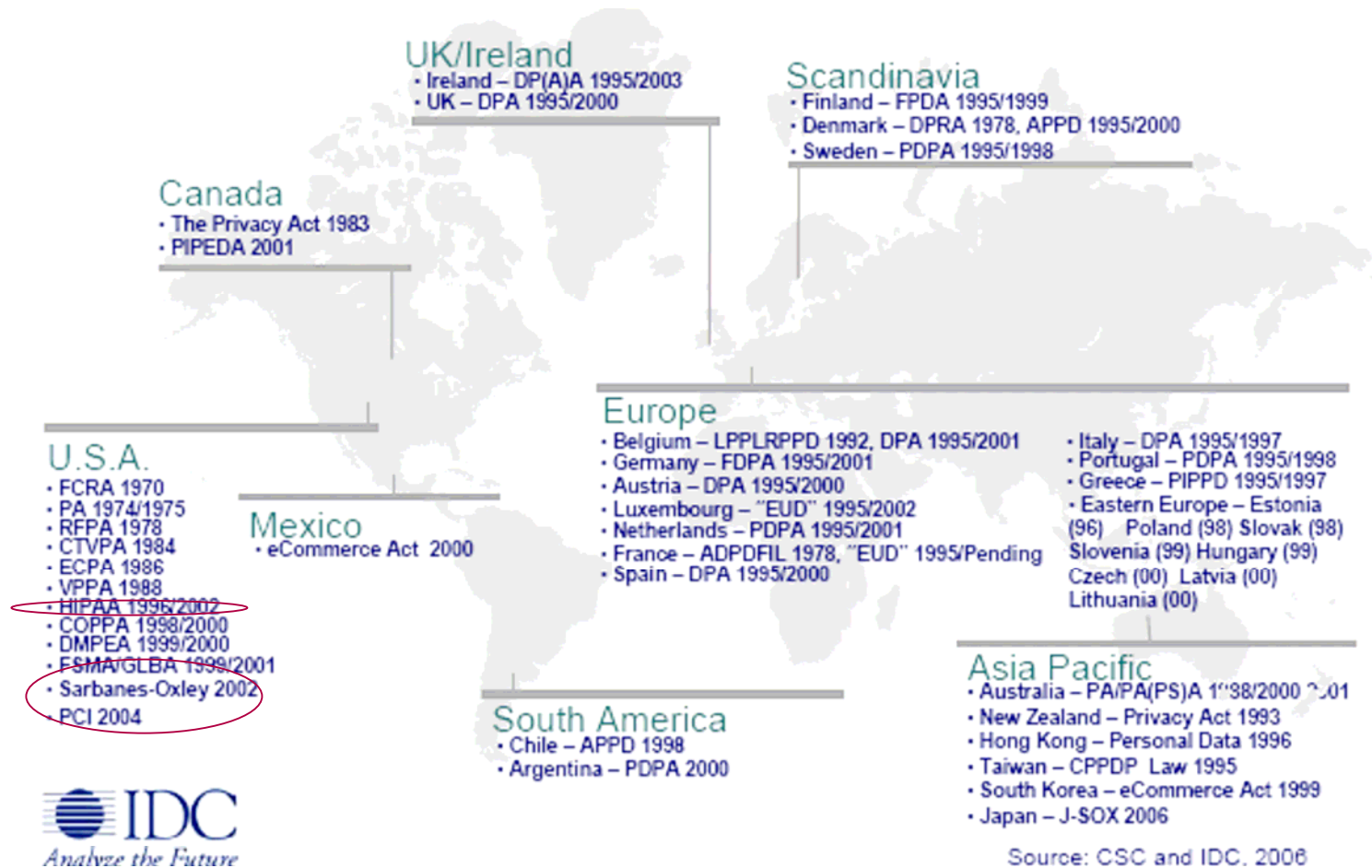
- Security is a top issue with customers
 - 76% of security decision makers expect to either maintain or increase their IT security budget for 2009 (Forrester 2008)
 - Security makes up 10 percent of overall IT operating budgets in 2008, up from 8 percent last year.
 - **Over 60% of downtime is caused by human error** (Uptime Institute)
 - Cost of downtime increased 3X in last 10 years (Wall Street Journal 2008)
- Stringent Access control procedures are enforced in Data Centers
 - Sisters of Mercy only allows IT personnel in Data Center when it is physically necessary
 - Switch Communications enforces that only one of three redundant power distribution paths can be down for maintenance at any given time
- Regulatory Compliance forces a focus on security

Root Causes



Knowing who accessed your Data Center or Network Closet is best practice.

Compliance around the World



Regulatory compliance is a global physical security concern.

Regulatory Physical Security Threats

- **Physical Safeguards from HIPAA Act Title II**

- Controlling physical access to protect against inappropriate access to protected data
- Controls must govern the introduction and removal of hardware and software from the network. (When equipment is retired it must be disposed of properly to ensure that PHI is not compromised.)
- Access to equipment containing health information should be carefully controlled and monitored.
- Access to hardware and software must be limited to properly authorized individuals.
- Required access controls consist of facility security plans, maintenance records, and visitor sign-in and escorts.
- Policies are required to address proper workstation use. Workstations should be removed from high traffic areas and monitor screens should not be in direct view of the public.
- If the covered entities utilize contractors or agents, they too must be fully trained on their physical access responsibilities.

HEALTH INSURANCE PORTABILITY and ACCOUNTABILITY ACT

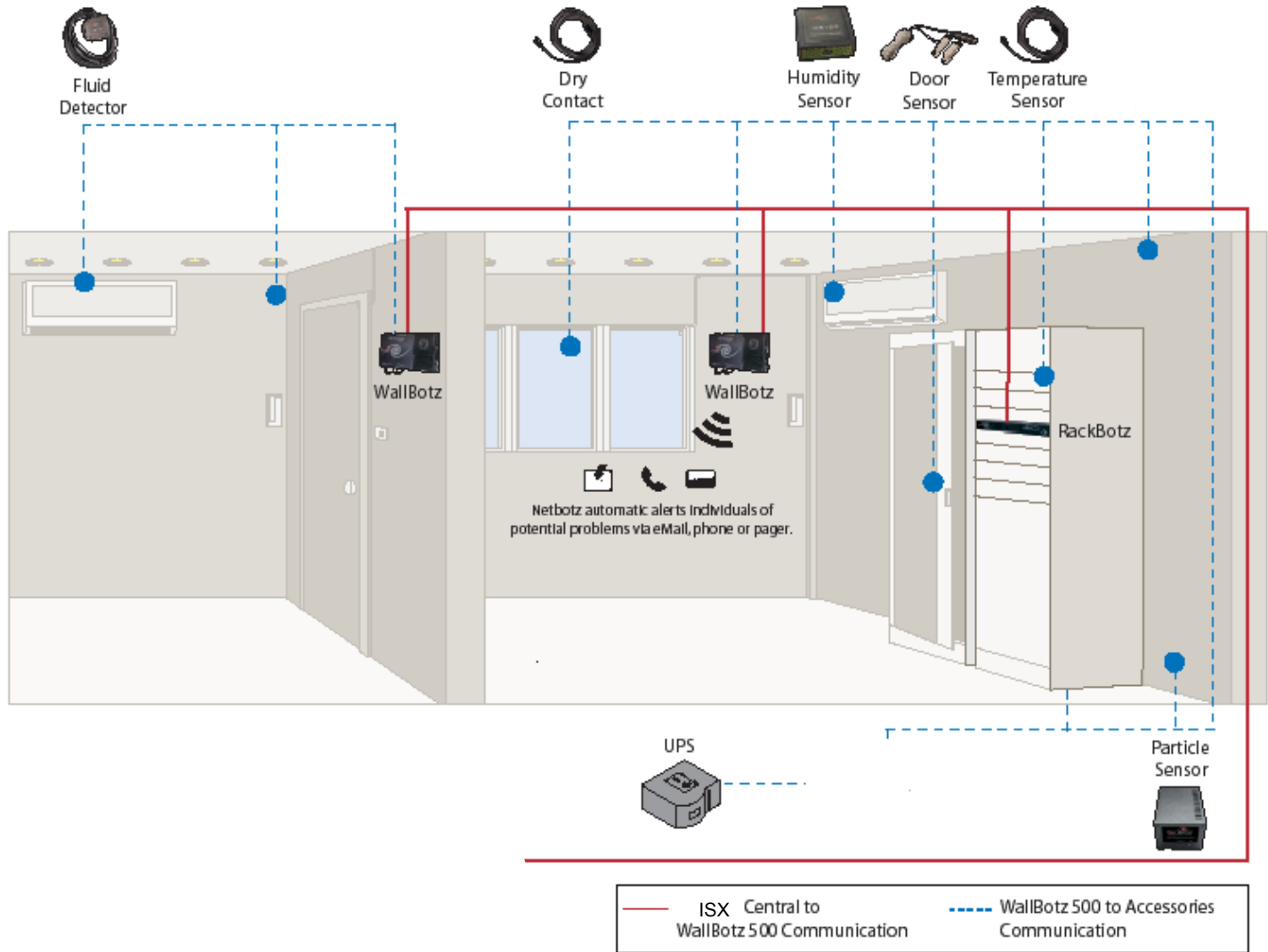
HIPAA

**ADMINISTRATIVE SIMPLIFICATION:
PRIVACY, SECURITY, TRANSACTIONS**



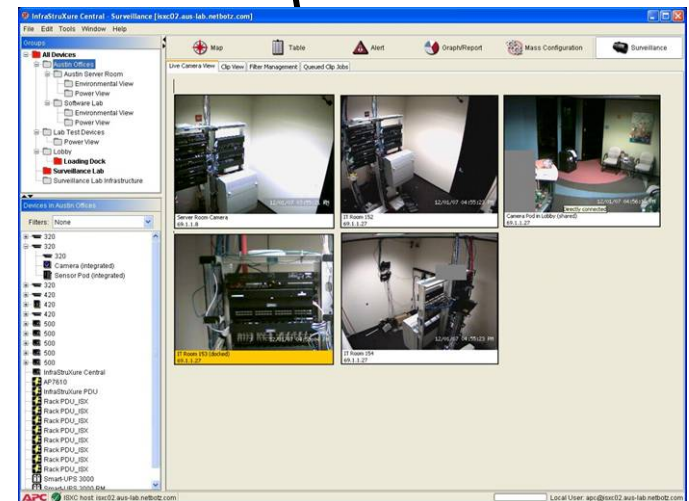
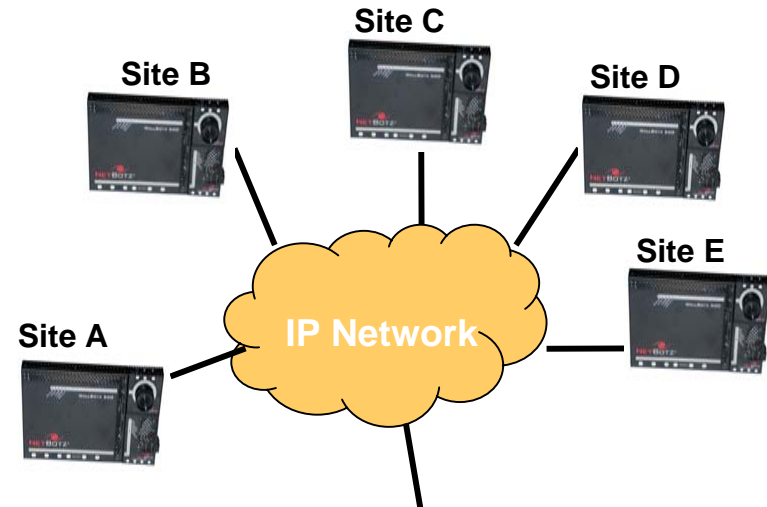
Access Control and Surveillance applications provide tools to help ensure compliance with these Safeguard Requirements.

Sample Deployment



Centralized Management

- Advanced alert customization capabilities:
 - Warning alerts, critical alerts, and alert escalation
 - Multiple notification methods
 - Scheduling
 - Graphing
 - Video attachments
- If deployment is bigger than 2 NetBotz appliances use InfraStruXure Central to optimize management efficiency
- NetBotz Surveillance nodes allow consolidated camera views through InfraStruXure Central

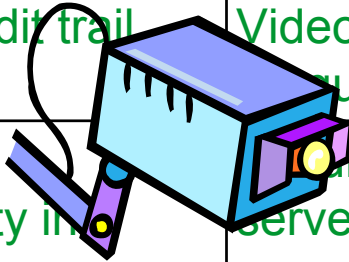
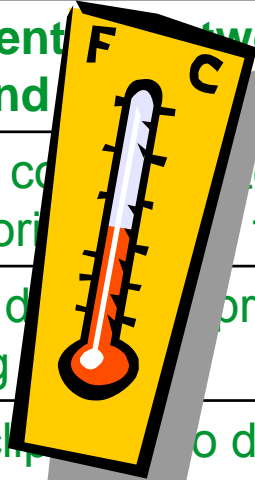


Key Takeaways

- Security and Environmental Monitoring is a core part of your Physical Infrastructure that is critical to your availability.
- Easy to deploy, easy to use, part of an overall management solution
 - ✓ Solutions are optimized for quick installation in network closet and data center environments
 - ✓ Intuitive User Interface make NetBotz easy to use
 - ✓ NetBotz Security and Environmental Monitoring are a part of the overall Datacenter Physical Infrastructure
- Schneider and APC
 - ✓ Part of a broad portfolio of product and services to connect the “building” and the data center

“My Building Management System has me covered”

Automated Building Systems	Data Center Network Closet Security and Environment Systems
Access control systems prevent unauthorized entry for	Access control systems prevent unauthorized entry for racks
Fire protection systems provide life safety	Smoke detectors provide early warning
Video surveillance creates audit trail	Video clips to door access provides quick response analysis
Security guards provide an instantaneous boost of security in normally unattended areas	Security and environmental monitoring serve as constant electronic security guards
HVAC systems maintain a healthy climate	Environmental monitoring alerts on thresholds
Sump pumps protect the lower levels of a building from seeping water	Leak detectors prevent damage



Additional Information

- Sales and Marketing Resources (www.apc.com)
 - Online Product Demo
 - White Papers
 - WP #102 – Monitoring Physical Threats in the Data Center
 - Application Notes
 - AN #91 – Alternative Network Options for NetBotz Monitoring Appliances
 - AN #93 – Security Features of APC's NetBotz Appliance
 - AN#134 – Using SeaLevel Equipment with NetBotz 500 and 420.
- Product Data Sheets



The screenshot shows the APC website interface. At the top, the APC logo is displayed next to the text "United States [Change]" and "by Schneider Electric". Below this, a dark banner contains the text "Does your UPS battery need replacing?" followed by a promotional message: "Upgrade using the APC Trade-UPS program and get up to a 35% discount on a new UPS with a full warranty and all the latest features." A link "Click Here to learn more!" is provided. On the right side of the banner, there is an image of a black APC UPS unit. At the bottom of the page, there is a navigation bar with four tabs: "Home / Home Office" (highlighted in orange), "Small / Medium Business", "Large Corporations", and "Resellers".

System Failure

- How are you notified if a chiller line bursts in your data center or network closet?
- How are you notified that a window broke at one of your remote network closet sites?
- How do you know if a spill has occurred in closet space shared with the janitor?

Human Error

- How are you notified that a problem happens?
- How can you access your system once you get an alert?
- What kind of data does your monitoring system provide?
- What kinds of analysis tools does your system offer to help diagnose the error?

Thank You