Preventing Outages by Monitoring, Managing, and Controlling the Data Center Environment

APC BY SCHNEIDER ELECTRIC: NETBOTZ EGUIDE

Data centers are under greater threat than ever. According to the Ponemon Institute, the average cost of a data center outage rose to $740,357 in 2016—an increase of 38 percent since 2010. The increase in the maximum downtime cost ($2,409,991) was even greater, climbing 81 percent over that same time period.[1]

Organizations are losing as much as $100 million per year to downtime related to information and communication technology (ICT), according to Infonetics Research.[2]

While cybercrimes and other network threats make up the fastest-growing sector of data center outages, internal threats such as power/cooling issues, leaks, smoke and fire, accidental errors, and more—threats that can be inherently controlled—continue to contribute significantly. The most common causes of ICT downtime? Failures of equipment (along with software and third-party services), power outages, and human error, reports Infonetics.[3]

In this eGuide, we'll examine some of the greatest risks to data centers—and, ultimately, the business—and how those risks can be mitigated. We'll then explore how one solution—NetBotz 250 from APC by Schneider Electric—can help minimize downtime and business risk.

[1] Source: "Cost of Data Center Outages," Ponemon Institute, 01/2016.
[2] Source: "How Much Is Network Downtime Costing Businesses Today? Infonetics Report and Calculator," Infonetics.com press release, 02/02/2015.
[3] Source: "How Much Is Network Downtime Costing Businesses Today? Infonetics Report and Calculator," Infonetics.com press release, 02/02/2015.

Life Is On

APC by Schneider Electric

Data Center Challenges/ Business Risks

Aside from cyber threats, here are some serious environmental and internal security challenges that can result in data center outages:

Temperature – According to the Ponemon Institute, water, heat and Computer Room Air Conditioner (CRAC) account for 11 percent of all data center outages in 2016.[4] Heat is the enemy of IT equipment, so it must be removed to avoid overheating and damaging the components and preventing an outage.

In many legacy and raised floor environments still in use today, cold air from the CRAC or computer room air handler (CRAH) pressurizes the space below the raised floor. Perforated tiles in front of server intakes allow the cold air to rise up from the plenum. The hot air then returns to the CRAC/CRAH for cooling before being returned back into the environment.

When server densities are low, this system works well enough to cool the environment and eliminate hot spots. But cooling today's higher density environments requires increased power/cooling to handle the corresponding heat output, driving up operating costs.

Humidity – Related to power/cooling is humidity. Low humidity brings with it the potential for electro-static discharge. For IT equipment housed in a chassis, this is less of an issue.

High humidity, on the other hand, can pose a danger to IT equipment, particularly when it goes undetected for an extended period of time. Humidity enables dust in the air to stick to electrical components in the computer, reducing heat transfer and potentially corroding those components. The effect of reduced heat transfer on IT equipment is very similar to that caused by high temperatures.

Contaminants – We've already mentioned that dust can coat electronic components and reduce heat transfer. The Uptime Institute also reports that certain types of dust, called zinc whiskers, found in electroplated raised floor tiles can become airborne and land inside a computer where they can cause shorts in internal components.[5] There are also threats related to gaseous contamination which can be corrosive to the electronic components.

Water/leaks – As we previously mentioned, 11 percent of all data center outages are the result of issues with water, heat, and CRAC.[6] So it's no surprise that water and IT equipment don't mix.

While leaking pipes, faulty structures, and inclement weather create the potential for leaks, many outages can also be the result of spilled beverages. Fortunately, water-related leaks are entirely preventable.

Fire/smoke – While relatively rare, fire- and smoke-related outages can and do occur and must be considered in data center design. These are often the result of over-heated or malfunctioning equipment and must be prevented before they bring down your data center.

Access control – One of the biggest sources of outages in the data center—22 percent, according to the Ponemon Institute—can be attributed to human or accidental error.[7]

While many data centers control access to their buildings/perimeters, they often pay less attention to the enclosures themselves, leaving valuable equipment and data vulnerable to unauthorized intrusion. Even if access to the enclosures is strictly controlled, careless employees may accidentally leave them open, again exposing valuable data and equipment to potential misuse.

In addition, many organizations must comply with strict regulations around data protection—or pay costly fines for non-compliance. So protecting assets all the way down to the rack level is of critical importance to ensure compliance and protect data.

Visibility – While IT professionals have greater visibility into their data centers than ever before, making sense of the data from multiple monitoring and management platforms can be a challenge.

[4] Source: "A Look at Data Center Cooling Technologies," The Uptime Institute.
[5-7] Source: "Cost of Data Center Outages," Ponemon Institute, 01/2016.

Preventing Data Center Outages

So how do you prevent a data center outage? Monitor the physical environment for any deviations from your desired temperature and humidity setpoints and detect the presence of contaminants, water, smoke, fire, and other potential hazards. Control rack-level security so you know who is accessing your servers and what they're doing there. And proactively manage the environment with a single platform to improve operational efficiency.

Monitor the environment – Key to preventing an outage is to monitor environmental conditions within your data center. When temperature and humidity levels deviate from setpoints, you should receive an alert so you can take action. You should also expect to receive alerts when levels exceed set thresholds for the presence of airborne or gaseous contaminants, water or other liquids, smoke and fire, or other potential hazards. Having the ability to monitor the environment in real time allows you to remediate issues before they cause an outage.

Control access – True cybersecurity not only includes controlling access to your network, applications, and the data center itself, it includes controlling access to your physical assets as well. Server racks and enclosures demand the same stringent physical security as the measures used to control access to the data center, your network, and applications. Verifying credentials at the rack and alerting to breached or open doors can prevent costly data breaches. Plus, you should expect a full audit trail to ensure regulatory compliance and avoid compliance penalties. Here are key requirements and standards for controlling access to physical equipment:

- **Healthcare Insurance Portability & Accountability Act (HIPAA)** – The HIPAA Security Rule covers protected electronic health information (EPHI) that is stored, transmitted, or processed. Within this rule are a series of safeguards, including physical safeguards, which are defined as "physical measures, policies, and procedures to protect a covered entity's electronic information systems and related buildings and equipment, from natural and environmental hazards, and unauthorized intrusion." These safeguards protect covered entities' EPHI not only from natural and environmental hazards, but also against unauthorized intrusion. With the value of EPHI on the black market skyrocketing, putting rack access controls in place and having a full audit trail will keep your organization from experiencing the heavy price of penalties and loss of trust.

- **Sarbanes-Oxley Act of 2002 (SOX)** – Physical access to IT infrastructure systems supporting financial reporting must be restricted. Mechanisms to control access could be as simple as a lock and key or as sophisticated as biometric systems. Access to physical systems, such as racks, cabinets, and cages, should be restricted to authorized personnel only and that access should be monitored and reviewed. Having an audit trail showing access to any physical systems that store financial data can facilitate SOX compliance.

- **Payment Card Industry Data Security Standard (PCI DSS)** – Created by the major credit card issuers, PCI DSS applies to any company that accepts, stores, processes, and transmits credit cardholder data. While it can be argued that all PCI DSS requirements touch the physical components of the data center in some way, Requirement 9 specifically relates to controlling physical access to cardholder data or systems that house cardholder data. In other words, any opportunity for individuals to access or remove devices or data should be appropriately restricted. Requiring individual badged access and other controls for employees, contractors, visitors, and any other persons who can come into direct contact with equipment (such as server racks) that accepts, stores, processes, or transmits cardholder data—and having an audit trail—is key for PCI DSS compliance.

Manage the environment – Having a single monitoring and management platform, such as a data center infrastructure management (DCIM) solution, can help consolidate information from multiple sensors. With this data, you can proactively manage the infrastructure to improve energy and operational efficiency and ensure ample availability.

Our Solution:

APC by Schneider Electric NetBotz 250

One solution—the NetBotz 250 from APC by Schneider Electric—allows you to deploy all three capabilities for a comprehensive, real-time environmental monitoring, management, and access control solution. Whether you have a single rack or 100, the NetBotz 250 offers a cost-effective alternative to other environmental management solutions for the data center. You can also integrate with StruxureWare Data Center Expert for a single management platform that helps you holistically protect IT assets from threats and prevent outages.

Environmental monitoring

Out of the box, you can remotely monitor humidity, temperature, door contact, and other environmental conditions and create user-defined alerts so you know when deviations occur. This wireless-enabled appliance features six onboard universal sensors, A-links for expansion sensor pods, relay output, dry contacts, and a switched output outlet, as well as options for up to 47 wireless sensors per appliance. These monitoring and alerting capabilities deliver a full picture of your environment at any point in time.

How does it work?

Keeping it Cool: Environmental Monitoring

1. Magnetically mounted on front of an enclosure, the NetBotz wireless temperature sensor reports a high temperature.
2. The NetBotz 250 recognizes the temperature is outside the configured threshold, notifies the relevant users, and turns on power to its onboard switched outlet.
3. The switched outlet on the NetBotz 250 turns on and powers the roof fan tray installed in the enclosure. The roof fan pulls the excess heat out of the enclosure and away from IT equipment.
4. When the wireless temperature sensor reports that the enclosure has been sufficiently cooled, the NetBotz 250 turns off the roof fan and resumes normal operation.

Access control

Retrofit an existing APC rack by removing the handles and installing one of APC's rack access control kits. The NetBotz 125 kHz rack access handles allow the use of existing HID proximity cards, while the 13.56 MHz rack access handles read higher encryption Mifare and iClass cards. Each NetBotz 250 appliance supports two handles, which plug directly into the appliance to detect, log, and control rack access and provide a full 24/7 audit trail.

You can even use the remote lock/unlock function to allow users without cards to access enclosures on an as-needed basis.

Because it relies on NetBotz architecture, APC's rack access solutions provide ample investment protection from theft and unauthorized access.

How does it work?

Keeping It Secure: Rack Access

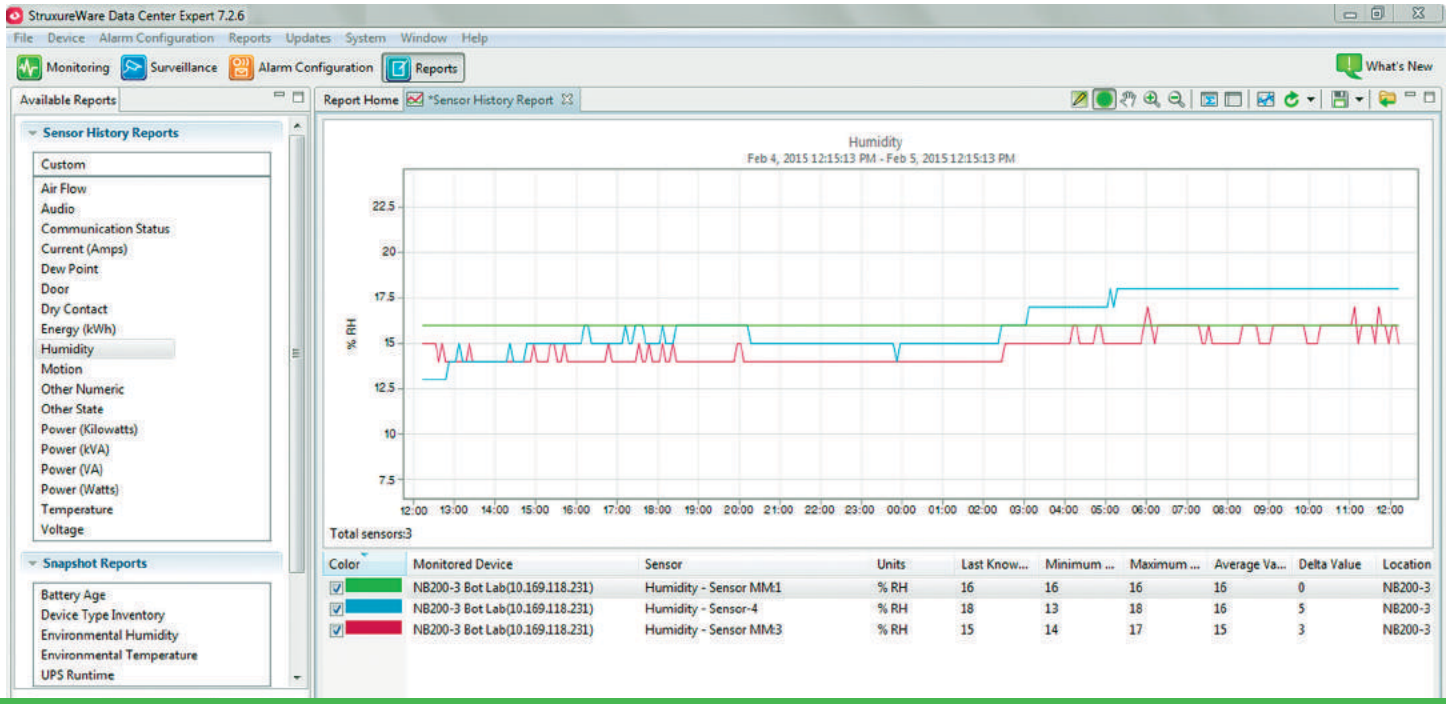
tinyurl.com/SEnetbotz

Streamlined environmental management

NetBotz 250 integrates with Data Center Expert for a comprehensive centralized monitoring solution of the environment with full audit trails for compliance with key regulatory initiatives, such as HIPAA, PCI DSS, and SOX.

This centralized repository can be accessed by multiple users from anywhere on the network, creating a consolidated view of the physical data center infrastructure. Images and alerts from around the company can be instantly viewed and managed, trends analyzed, and problems averted for unparalleled physical threat management. Audit trails tied to alarms and instances can easily be stored and searched for compliance purposes.

This open and flexible architecture expands with changing business needs through additional device licenses, add-on surveillance (with sorting and searching of video clips), and integration with enterprise and building management systems.



How Your Organization Can Benefit from NetBotz 250

NetBotz 250 offers multiple benefits to your organization, including:

- **Easy Integration** – Integrates with APC PDUs, servers, enclosures, and Data Center Expert for easy deployment, configuration, and management.
- **Compliance-Ready** – Provides a complete audit trail on who is accessing your enclosures so your organization can easily comply with data security regulations.
- **Reduced Cabling** – Features wireless sensors to reduce the clutter and expense of cabling.
- **Affordable** – Delivers the most compelling environmental monitoring and access control solution for its price.

NetBotz 250 delivers a cost-effective and comprehensive, real-time environmental monitoring, management, and access control solution for companies of any size in any industry. With Data Center Expert, you can holistically manage and protect IT assets and minimize outages.

For more information on NetBotz 250 from APC by Schneider Electric, please visit:

apc.com/struxureware/us/en

Life Is On | APC by Schneider Electric