# SYSTEM DOWN TIME

**Jason Andersen** *explains the risks to an organisations' assets during unexpected down time*

**The constant threat of terrorist attacks and the increasingly sophisticated activities of organised criminal gangs has meant that more than ever it is crucial for security systems to be continuously available and effective. The consequential losses are often far greater than any immediate financial loss when access control, building management, fire, intruder alarm, perimeter protection, PSIM or video management systems suffer downtime.**

The days have long passed when an investment in an electronic security system was regarded as a grudge purchase, quite often to accommodate insurers. The commercial world is now very much aware of the need to proactively protect itself. Senior managers that want to sleep well at night are not hesitating to support security personnel by investing in physical security systems that utilise the latest advances in technology to help them keep one step ahead of those involved in a wide range of criminal activity.

Although I hesitate to be the instigator of nightmares and at the risk of stating the obvious, it's simply not enough to install electronic security systems. They need to be working as close to 100 percent of the time as possible and yet, with IP network-based Access Control, video surveillance, as well as fire, intruder and perimeter protection increasingly reliant on software-based management, even a well-designed and maintained system is vulnerable to downtime because of a simple server fault.

Picture credit: Getty

**Many sporting events with the general public in attendance cannot take place unless the safety officer can certify that the venue's security system is 100 percent operational**

What are the consequences of say, having just 0.05 percent (one 20th of a percent) of downtime in a year? It is a question that could easily keep any security manager up at night that's tasked with ensuring the protection of their company or organisation's assets, people and property. The answer is approximately five hours!

## UNPLANNED DOWN TIME

While protection of people, assets and property is of paramount importance, with video surveillance and access control increasingly being used in support of compliance issues, any unplanned downtime could have a major impact on operational activity. Indeed, in some cases it may result in a temporary but costly closure. Government regulations and local licensing laws, for example, will in many countries stipulate that a sporting event with the general public in attendance cannot take place unless the safety officer can certify the venue's video surveillance system is operational and 100 percent effective, and the same rules are understandably applied to night clubs and other environments where large numbers of the public are likely to gather.

Health and safety compliance is no less an issue within the industrial/production world. Let's consider the requirements of a food processing plant where an access control system – in addition to being used for general security purposes – is also relied upon to ensure compliance with hygiene regulations. The consequences of anyone with an expired certificate being allowed to work in a food processing plant could be huge. An inspector might even insist that all onsite foodstuffs are put on the rubbish tip and all machinery cleaned to avoid the slightest risk of contamination. Integration with Microsoft's active directory functionality means access control systems utilising the latest advances in technology have the ability to effortlessly generate a report that lists staff that are in need of refresher training or whose hygiene certificate is due to be renewed. The system, though, needs to be working effectively 24/7.

The IT industry offers a wide range of options to keep your security software applications running or to quickly restore them. Perhaps the simplest approach to server availability is to have basic backup, data-replication and failover procedures in place, which will help speed the restoration of an application and help preserve data following a server failure. However, if backups are only occurring daily, there may only be a guarantee of 99 percent availability, resulting in up to 87.5 hours of unplanned downtime per year.

High availability systems can deliver 99.95 percent to 99.99 percent uptime, but only continuous availability solutions are able to deliver 99.999 percent uptime, which is the equivalent to approximately just five minutes of downtime per year.

Supported by specialist continuous availability software, two servers are linked and continuously synchronised via a virtualisation platform that pairs protected virtual machines together to create a single operating environment. If one physical machine fails, the application or software platform will continue to run on the other physical machine without any interruptions. In-progress alarms and access control events, as well as data in memory and cache are preserved. Continuous availability means that no single point of failure can stop a security software platform from running and, unlike high availability, backup and failover solutions, there is no restart or reboot required and so, no downtime.

If a hardware component fails, a continuous availability solution will substitute the healthy component from the second system until the failed one is repaired or replaced. Most importantly, manufacturers that specialise in continuous availability, such as Stratus, are able to offer the option to provide you with automatic monitoring and diagnosis of your security solution so that potential problems can be anticipated before they occur.

It is a solution that it likely to be popular among installers of electronic security systems that may have limited IT knowledge. As well as being quick and simple to install, no application, software or server modifications are needed to provide continuous availability out-of-the-box.

The physical security sector is starting to recognise the significance of the Internet of Things (IoT). It presents installers and system integrators with opportunities to generate new revenue streams, while offering end-user clients maximum benefit and high ROI by delivering truly integrated solutions. The emergence of smart buildings has created a need to monitor and control so many disparate systems – security, IT, lighting, HVAC and more. Virtualised platforms are really the only cost-effective means of accomplishing all of this, but this could mean businesses are opening themselves up to having a single point of failure, which could be their downfall. Here lies just one of many reasons why a continuous availability solution should be considered.

**ELECTRONIC SECURITY SYSTEMS NEED TO BE WORKING CLOSE TO 100 PERCENT OF THE TIME**

## MAKING A DIFFERENCE

Worldwide, there are some excellent examples of where continuous availability has made a significant contribution to providing security and operations management with peace of mind and keeping those nightmare scenarios at bay. These include an international airport, which all too often experienced unplanned downtime of its access control and badge tracking system and there were also issues with the system deployed to help with the screening, storage, sorting and transportation of arrival, departure and transfer baggage. These outages required costly human intervention in order to maintain customer service levels, minimise safety risks and ensure compliance with Federal Transportation Security Administration (TSA) requirements.

When the access control system failed, the airport was forced to deploy personnel to monitor every door in the airport's secure areas and alert the Airport Control Centre of any potential security issues. In addition to labour costs for extra personnel, a system failure could result in TSA fines and penalties, potentially including the shutdown of operations and associated revenue losses for the airport and airlines.

Since the deployment of a continuous availability solution, the airport has enjoyed zero unplanned downtime of the two systems. Even when it opened a new terminal, increasing its potential annual capacity to approximately 55 million passengers, the solution played a key role in allowing the IT staff to seamlessly scale the physical security and baggage handling systems to meet the expanded requirements, while ensuring continuous availability.

## AROUND THE CLOCK PROTECTION

A hydroelectric dam in the Pacific Northwest region of the US is another good example of a mission-critical security system being supported by a continuous availability solution. In order to meet NERC CIP (North American Electric Reliability Corporation Critical Infrastructure Protection) compliance, the dam required around-the-clock protection and this meant that a fault-tolerant platform for the security and event management system was crucial. Working in support of the C•CURE 9000 system, the continuous availability solution negated the risk of up to $1 million per day in penalties, which comes with compliance failure.

Northwestern University upgraded to a continuous availability solution, having previously used a traditional fail-over configuration where a second server was used as a standby in the event that the primary server failed.

Northwestern had been using a popular failover and recovery software solution, but found that it lacked the level of stability and reliability needed to keep its mission-critical systems up and running all the time. The University is now benefiting from continuous availability of its building control applications and is enjoying a high level of seamless facilities management needed by a leading research institution.

Your response to the following questions will go a long way to helping you decide whether or not an investment in a continuous availability solution is required: what failures do you need to be protected from? How much unplanned downtime can you tolerate? What skills are you are willing to acquire to manage the solution properly?

If your mind is still not made up, download a free copy of the *Availability for Dummies* handbook (go.stratus.com/availability-for-dummies). As well as helping you select the option that best matches your needs, the handbook also describes how the latest computing trends, such as virtualisation and the cloud are impacting on availability and increasing the need for bulletproof downtime prevention strategies and solutions ●

**Jason Andersen** is Vice President of Business Line Management at Stratus Products and Services. He has a deep understanding of both onsite and cloud-based infrastructure for the industrial internet.

**Security systems can ill afford the risk of missing something when the system goes down**

Picture credit: Stratus