



# THE REASONS APPLICATIONS FAIL



ProtectedHarbor

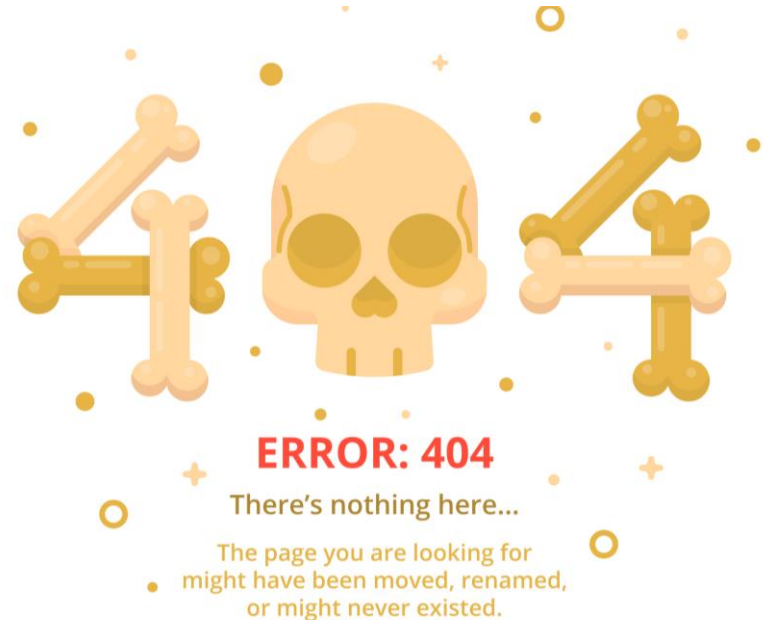
# 99.99% Uptime Is Essential

In today's modern world of Tele-Medicine, application availability and uptime is more critical than ever.

Healthcare workers and patients are accessing applications at all times of the day and night. The days of "bringing the application down for maintenance" every night are over.

Add to this the fact that most healthcare companies are growing, which adds extra load to these already stressed applications.

EMR and other key applications need to be available virtually 100% of the time.



# How Much Does A Single Hour Of Downtime Cost?

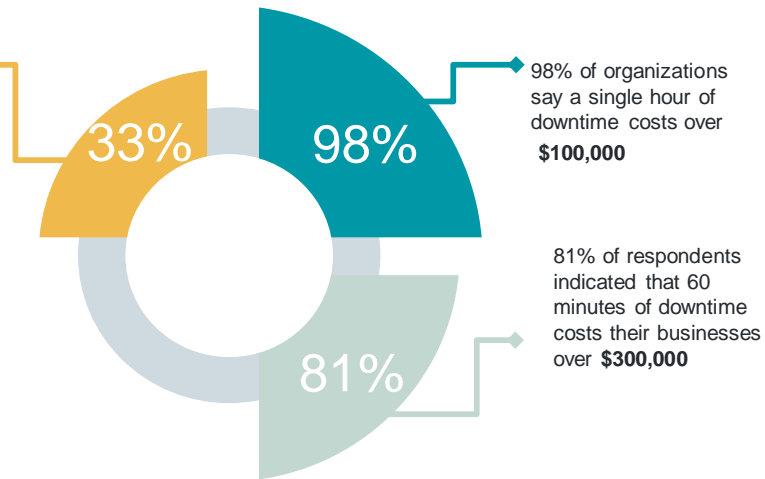
According to an ITIC study this year, the average amount of a single hour of downtime is \$100,000 or more. Since 2008, ITIC has sent out independent surveys that measure downtime costs. Findings included that a single hour of downtime has risen by 25%-30%. 33% of those enterprises reported that one hour of downtime costs their companies between \$1-5 million. 98% of organizations say a single hour of downtime costs over \$100,000. 81% of respondents indicated that 60 minutes of downtime costs their businesses over \$300,000.



Protected Harbor has found the design of data centers plays an essential role in its ability to maintain application availability which translates into company credibility with clients, employees, and ultimately dollars gained or lost.

The purpose of this white paper is to outline the top five mistakes companies make when designing, building, and managing data centers.

33% of those enterprises reported that one hour of downtime costs their companies between \$1-5 million

## DOWNTIME COSTS





It's Much Harder To Manage A Data Center For A Growing Business Than One For A Stagnant Business. This saying has stuck with me over the years. Most of the businesses my company supports are growing companies. They trust we can design, build and manage a data center that will develop with them, and not impede on their growth.

According to a recent article by a top data center management company, only 4% of data center failures are due to IT equipment failure. Only 4%! That leaves 96% of data center failures caused by things outside of your data center equipment, whether it be power failure, cyber-crime, human error, or water/heat.

What does this mean for you? Well, at the inception of designing your Data Center elements that may seem to be innocuous must be considered because these components could have a significant impact on how your data center functions – or doesn't function. Regardless of whether you are building a data center or migrating, it is imperative that you avoid falling into the traps that have ensnared many before you.



“It's much harder to manage a data center for a growing business than one for a stagnant business.”

**RICHARD LUNA**

-CEO, PROTECTED HARBOR

Protected Harbor has enough experience with all the above issues to understand how crippling they can be for small, medium and large organizations. Data centers popularity has increased exponentially over the past decade, and for good reason. They enable a business to expand, while being cost effective and reliable. Recently, a client asked us to list the common mistakes companies make when designing, building and managing their data centers. When compiling this list, we break these mistakes into three major categories; People, Processes and Tools. If you are about to embark down the data center path, make sure you don't tumble into these pitfalls and wind up in a state of confusion and chaos.



ProtectedHarbor



# Five Mistakes Companies Make That Cause Applications To Fail

## PEOPLE: Organizing IT Staff in Vertical Roles vs. Horizontal Roles

**Human error accounts for almost one quarter of all data center outages**

0

We believe this has a lot to do with how IT staff is organized at most companies. IT staffs will have DBA's (both development and production), programmers specific to one system, networking experts, and storage experts, etc. This level of specialization can be a big problem.

In many organizations, managers develop elaborate handoff processes that are confusing and often not followed. The programmer hands off the work to the database expert, who then hands off to the storage person. Often, there is no manager, who understands the big picture, until you get to either an IT Director or the CIO, who is too senior and removed from details to provide real direction. IT staffs lose the ability to view the system horizontally (and holistically), to understand the big picture. Often, steps are missed, mistakes are made, and when the data center crashes, groups point fingers at other groups and the true cause of the outage is not determined, which means it could happen again.

1

We recommend assigning IT process owners, meaning - IT staff members who are responsible for managing IT processes. These individuals first document the process and then put in end-to-end controls to ensure those processes are followed.

Implications: Systems that perform poorly, IT dollars wasted on the wrong equipment, and lack of operational durability or survivability in the event of a failure



Protected Harbor



# Inadequate Redundancy

0

**TOOLS:** Power issues, including issues with the UPS or generator, and other environmental issues, account for over 45% of data center outages

The IT team may understand the need for redundancy but fail to carry it through the entire system. Often, they will ensure redundancy in one network layer (or portion of the system for communicating data). However, the operational stability of the data center requires that multiple networking layers be on-line, all the time.

2

In other words, each layer needs to be redundant. For hardware, that means two mirrored firewalls, two drops, and two core mirrored switches. For software, this means multiple servers performing the same function configured in a primary secondary or in a pool configuration. If a server fails, the workload is migrated or transferred to a redundant server. We allow for redundancy at every level.



Implications: Systems that go off-line frequently and easily, because failures in any one section that is not duplicated can trip system-wide instability



0

## System Software Not Directly Connected To The Firewalls

**TOOLS:** Cyber-crime accounts for over 20% of data center outages

Any data center needs to be worried about external vulnerability to attacks. Companies can buy a high-end firewall package that does advance monitoring. But what happens behind that firewall? Most companies fail to understand the importance of connecting software login to firewall activity. For example, if the organization has RDP servers that cannot determine a legitimate log-in from an invalid log-in, how do you block it? This isn't done automatically, because many of the individual apps being used are customized.

3

The best approach to this problem is to avoid it—design the system the right way, at its inception. For example, deploying a module that after three failed login attempts into a particular app blocks that IP address right at the firewall.



Implications: Higher risk of successful external attacks, greater system vulnerability

# Data System Growth Not Sufficiently Considered In Budgeting

**PROCESS:** Many data centers crash because the data center environment was designed and built for a smaller organization, and cannot handle the increase in load due to company growth.

Many industries and companies see periods of rapid growth, and try to do their best to predict how that might affect operational needs, like sales, marketing, and manufacturing. However, IT often gets left behind in the budgeting dust, and the result is underfunding and an inability of the IT systems or data center capabilities to match the expectations of the rest of the organization.

Typically, this underfunding leads to attempts to cannibalize equipment, exceed their recommended capacities, and go beyond their expected lifespans. It often causes IT staff to find quick fixes to keep the data center operational. Regarding these quick fixes, we often observe a related error: The IT staff forget to remove the bandages that got them past isolated problems. This results in a lost opportunity to go back and properly resolve the underlying problem. There's just no resources available to do it.

We recommend the IT leader work closely with his/her company's leadership team to understand business trends, and works with IT experts to design a data center environment that can grow with the organization. Just like leaders of other departments, the IT leader needs to outline key IT investments that will be needed if the company grows. If a company's core competence is healthcare, they may not want to be in the data center management business.

Implications: IT systems that can't keep up with company growth, trying to get by with old equipment, and inevitable system instability



ProtectedHarbor





0

5

## Not Having Clearly Written Procedures, Designated Lines Of Authority, And As A Result, Accountability

**PROCESS:** When completing a new deployment, the people who understand the system and the way it was designed should compile the procedural manual for how to handle isolated issues, maintenance, and system-wide failures. This should also include lines of authority, which defines areas of responsibility. Only once these are delineated, can one expect accountability of the individuals on the IT team. Too often, organizations are barely organized, and these vital documents do not exist (or staff are unaware of their existence).

We recommend that procedures are created, documented, and followed in a specified way, guiding appropriate deployment of IT assets. Clearly stated lines of authority are required to make it work.



Implications: Confusion and perhaps even panic during outages, lack of leadership, and useless, wasteful finger pointing



## We Are Here to Help!

If you are an IT executive, director or decision maker and are concerned your company is falling prey to any of the aforementioned problems, let Protected Harbor help you navigate through them by implementing a comprehensive, secure and durable strategy.

Protected Harbor helps organizations and businesses across the US address their current IT needs by building them secure, custom and protected long term solutions. Our unique technology experts evaluate current systems, determine the deficiencies and design cost-effective options. We assist all IT departments by increasing their security, durability and sustainability, thus freeing them up to concentrate on their daily workloads. Protected Harbor stands tall in the face of cyberattacks, human error, technical failure and compliance issues. [www.protectedharbor.com](http://www.protectedharbor.com)

