Hourly Cost of Downtime

ITIC 2024 Hourly Cost of Downtime Survey Results

By Laura DiDio

Cost of Hourly Downtime Exceeds $300,000 for 90% of Firms; 41% of Enterprises Say Hourly Downtime Costs $1 Million to Over $5 Million

ITIC Position

In the 21st century Digital Age of "always on" IoT interconnected systems, AI, analytics and cloud computing, organizations have zero tolerance for downtime. This is true for all organizations – from micro SMBs with 1 to 20 users to Fortune 100 global multinational enterprises with 100,000+ workers. Outages of even a few minutes duration cause business and productivity to grind to a halt; negatively impact reliability and security and place companies at higher risk for regulatory compliance as well as civil and even criminal penalties.

ITIC's latest research indicates the cost of hourly downtime continues to spike. The average cost of a single hour of downtime now exceeds $300,000 for over 90% of mid-size and large enterprises. These costs are exclusive of litigation, civil or criminal penalties. These are the results of ITIC's 2024 Hourly Cost of Downtime Survey, an independent Web survey that polled over 1,000 firms worldwide from November 2023 through mid-March 2024.

Downtime Dangers in a Post-Pandemic World Economy

ITIC survey data finds the escalating cost of computing/network outages is attributable to several factors:

- An increase in the number of interconnected devices, systems and networks via the Cloud and the Internet of Things (IoT) ecosystems. Connectivity is a two-edged sword. It facilitates faster, more efficient transmissions and data access. But it also creates a limitless "attack surface" and exponentially increases the number of vulnerability points across the entire corporate ecosystem.

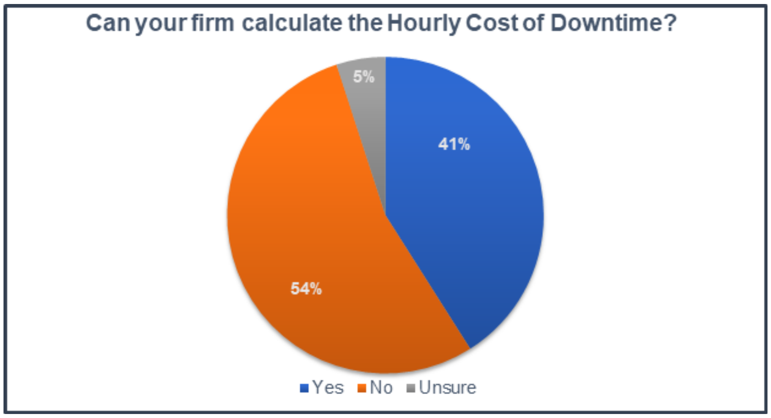
- An ongoing sharp spike in security vulnerabilities. These include targeted security and ransomware attacks by organized hackers; Email Phishing scams; CEO fraud and a wide range of malware, viruses, and rogue code. The spike in security and data breaches were further exacerbated by the COVID-19 global pandemic that forced countries to go on lockdown and businesses to mandate that employees work from home. This in turn, gave rise to a spate of opportunistic COVID-19 related security scams which continue today.

- End user carelessness. Everyone from CEOs, knowledge workers, IT and Security administrators, developers, full and part-time employees, and contract workers access corporate servers, applications, and information. Users regularly access sensitive data assets and intellectual property (IP) via a wide array of devices and networks. These include company and employee-owned (BYOD) mobile phones, tablets, laptops, and desktops as well as public networks. Unfortunately, many of these devices and networks lack adequate security. Absent up-to-date security and encryption, a lost or stolen device leaves the company's data assets as well as personal employee information and the data of corporate customers, business partners and suppliers all potentially vulnerable and exposed.

- Organizations' near-total reliance on computers and networks to conduct business. Downtime of even a few minutes interrupts productivity and daily business operations. Downtime also has a domino effect, even if no data is lost, stolen, changed, destroyed, or hacked.

ITIC anticipates that all these trends – particularly security and data breaches as well as the trend towards remote working and remote learning -- will continue unabated. The hourly cost of downtime will continue to rise. It is imperative that organizations implement the necessary measures to ensure the reliability and security of their hardware, software applications and connectivity devices across the entire network ecosystem. Security and security awareness training are necessary to maintain the uptime and availability of devices and data assets. This will ensure continuous business operations and mitigate risk.

Exhibit 1. Six-in-10 Businesses Cannot Calculate Hourly Downtime Costs



Source: ITIC 2024 Hourly Cost of Downtime Survey

Security and Human Error are Chief Culprits Causing Downtime

And continuing a trend that has manifested over the past three years, Security, Human error, followed by software flaws and bugs, are the chief issues that undermine server hardware/server operating system, application software, appliances and network reliability resulting in unplanned downtime. An 84% majority of ITIC survey respondents ranked Security as their top cause of downtime followed by 69% that cited Human error and 65% that said software flaws.

Unsurprisingly, in the 21st Century Digital Age, the reliability of the core foundation server hardware and server operating systems is more crucial than ever. The server hardware and the server OSes are the bedrock upon which the organization’s mainstream line of business (LOB) applications rest. High reliability and continuous availability to data assets is imperative for organizations’ on-premises, cloud based and Network Edge/Perimeter environments. Infrastructure — irrespective of location – is essential to the overall health of operations.

Additionally, ITIC’s latest 2024 Reliability research reveals that a variety of external factors are having more of a direct impact on system downtime and overall availability. These include overworked and understaffed IT departments; the rapid mainstream adoption of complex new technologies such as IoT, Big Data Analytics, virtualization and increasing cloud computing deployments and the continuing proliferation of BYOD and mobility technologies.

In the context of its annual Reliability and Security surveys, ITIC broadly defines human error to encompass both the technology and business mistakes organizations make with respect to their network equipment and strategies.

Human error as it relates to technology includes but is not limited to:

- Configuration, deployment, and management mistakes.
- Failure to upgrade or right size servers to accommodate more data and compute intensive workloads.
- Failure to migrate and upgrade outmoded applications that are no longer supported by the vendor.
- Failing to keep up to date on patches and security.

Human error with respect to business issues includes:

- Failure to allocate the appropriate Capital Expenditure and Operational Expenditure funds for equipment purchases and ongoing management and maintenance functions.
- Failure to devise, implement and upgrade the necessary computer and network to address issues like Cloud computing, Mobility, Remote Access, and Bring Your Own Device (BYOD).
- Failure to construct and enforce strong computer and network security policies.
- Ignorance of Total Cost of Ownership (TCO), Return on Investment (ROI).
- Failure to track hourly downtime costs.
- Failure to track and assess the impact of Service Level Agreements and regulatory compliance issues like Sarbanes-Oxley (SOX), Health Insurance Portability and Accountability Act (HIPAA).

On a positive note, the inherent reliability of server hardware and server operating system software as well as advancements in the underlying processor technology, all continue to improve year over year. But the survey results also reveal that external issues, most notably human error and security breaches, have also assumed greater significance in undermining system and network accessibility and performance.

The overall health of network operations, applications, management, and security functions all depend on the core foundation elements: server hardware, server operating systems and virtualization to deliver high availability, robust management and solid security. The reliability of the server, server OS and virtualization platforms form the foundation of the entire network infrastructure. The individual and collective reliability of these platforms has a direct, immediate, and long-lasting impact on daily operations and business results.

Security and Human Error are Chief Culprits Causing Downtime

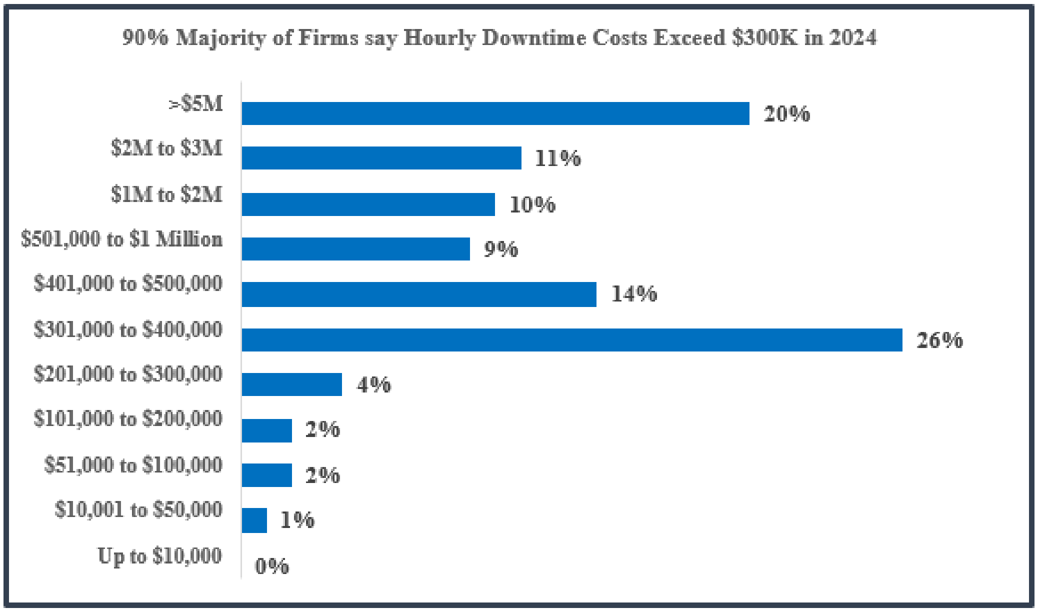
ITIC's 11th annual Hourly Cost of Downtime Survey data indicates that 97% of large enterprises with more than 1000 employees say that on average, a single hour of downtime per year costs their company over $100,000. Even more significantly: four in 10 enterprises - 41% - indicate that hourly downtime costs their firms $1 million to over $5 million (See Exhibit 1). It's important to note that these statistics represent the "average" hourly cost of downtime. In a worst-case scenario – such as a catastrophic outage that occurs during peak usage times or an event that disrupts a crucial business transaction – the monetary losses to the organization can reach and even exceed millions per minute. Among SMBs with 20 to 100 employees, 57% of companies said an hour of downtime cost their companies up to $100,000 an hour. However, SMB respondents were extremely worried about the consequences of an unplanned outage. This was particularly the case if the outage was the result of a security breach. SMBs and micro SMBs such as medical offices and clinics, for example noted that a data breach that exposed or stole patient information would be devastating to their business and put them at high risk for litigation from the patients and almost certain censure (civil and even criminal penalties) from government agencies and regulatory compliance bodies.

Additionally, in highly regulated vertical industries like Banking and Finance, Food, Energy, Government, Healthcare, Hospitality, Hotels, Manufacturing, Media and Communications, Retail, Transportation and Utilities, must also factor in the potential losses related to litigation. Businesses may also be liable for civil penalties stemming from their failure to meet Service Level Agreements (SLAs) or Compliance Regulations. Moreover, for select organizations, whose businesses are based on compute-intensive data transactions, like stock exchanges or utilities, losses may be calculated in millions of dollars per minute.

ITIC's most recent poll – conducted in conjunction with the ITIC 2023 Global Server Hardware Server OS Reliability Survey - found that a 90% majority of organizations now require a minimum of 99.99% availability. This is up from 88% in the last 2 ½ years. The so-called 99.99% or "four nines" of reliability equals 52 minutes of unplanned per server/per annum downtime for mission critical systems and applications or, 4.33 minutes of unplanned monthly outages for servers, applications, and networks.

All categories of businesses were represented in the survey respondent pool: 27% were small/midsized (SMB) firms with up to 200 users; 28% came from the small/midsized (SME) enterprise sector with 201 to 1,000 users and 45% were large enterprises with over 1,000 users.

Exhibit 1. Six-in-10 Businesses Cannot Calculate Hourly Downtime Costs



Source: ITIC 2024 Hourly Cost of Downtime Survey

These above statistics are not absolute. They are the respondents' estimates of the cost of one hour of hourly downtime due to interrupted transactions, lost/damaged data, and end user productivity losses that negatively impacted corporations' bottom line. These figures exclude the cost of litigation, fines or civil or criminal penalties associated with regulatory non-compliance violations. These statistics are also exclusive of any voluntary "good will" gestures a company elects to make of its own accord to its customers and business partners that were negatively affected by a system or network failure. Protracted legal battles and out-of-court settlements, fines and voluntary good-will gestures do take a toll on the company's revenue and cause costs to skyrocket further – even if they do help the firm retain the customer account. There are also "soft costs" that are more elusive and difficult to measure, but nonetheless negative.

These include the damage to the company's reputation which may result in untold lost business and persist for months and years after a highly publicized incident.

To reiterate: in today's Digital Age of "always on" networks and connectivity, organizations have no tolerance for downtime. It is expensive and risky. And it is just plain bad for business.

Only four (4%) percent of enterprise respondents said that downtime costs their companies less than $100,000 in a single 60-minute period and of that number an overwhelming 93% majority were micro SMBs with fewer than 10 employees. Downtime costs are similarly high for small and midsized businesses (SMBs) with 11 to 200 employees. To reiterate, these figures are exclusive of penalties, remedial action by IT administrators and any ensuing monetary awards that are the result of litigation, civil or criminal non-compliance penalties.

Do the Math: Downtime Costs Quickly Add Up

> *Downtime is expensive for all businesses – from global multinational corporations to small businesses with fewer than 20, 50 or 100 employees. Hourly losses of hundreds of thousands or millions per hour or even minutes in transaction-heavy environments are unfortunately commonplace.*

One minute of downtime for a single server in a company that calculates its hourly cost of downtime for a mission critical server or application at $100,000 is $1,667 and $16,670 per minute when downtime affects 10 servers and main line of business applications/data assets. The above chart graphically emphasizes how quickly downtime costs add up for corporate enterprises.

Small businesses are equally at risk, even if their potential downtime statistics are a fraction of large enterprises. For example, an SMB company that estimates that one hour of downtime "only" costs the firm $10,000 could still incur a cost of $167 for a single minute of per server downtime on their business-critical server. Similarly, an SMB company that assumes that one hour of downtime costs the business $25,000 could still potentially lose an estimated $417 per server/per minute. With few exceptions micro SMBs –with 1 to 20 employees – typically would not rack up hourly downtime costs of hundreds of thousands or millions in hourly losses. Small companies, however, typically lack the deep pockets, larger budgets, and reserve funds of their enterprise counterparts to absorb financial losses or potential litigation associated with downtime. Therefore, the resulting impact could be as devastating for them as it is for enterprise firms.

Hourly downtime costs of $25,000; $50,000 or $75,000 (exclusive of litigation or civil and even criminal penalties) may be serious enough to put an SMB out of business – or severely damage its reputation and cause it to lose business.

Laura DiDio is Principal Analyst at ITIC, a research and consulting firm in the Boston area.

INFORMATION TECHNOLOGY ITIC INTELLIGENCE CONSULTING

✉ ldidio@itic-corp.com

https://itic-corp.com/

@lauradidio