Hourly Cost of Downtime Part 2

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.

Downtime = unreliability. Unreliable devices, systems, applications and networks will be insecure. And insecure systems will be unreliable.

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.

Introduction

An overwhelming 33 million firms or 90%+ of companies currently operating in the U.S. are small businesses, according to statistics compiled by both the United States Small Business Administration’s Office of Advocacy[1] and the U.S. Chamber of Congress[2].

As of the end of 2023, the U.S. Small Business Administration said there are 33,185,550 small businesses in the U.S., which combined, account for 99.9% of all companies currently operating in the USA. And of this number, 81% or nearly 28 million are micro SMBs with no full-time employees; 16% of small businesses fall into the category of having between one and 19 employees, comprising over 5.4 million businesses. On the higher end of the SMB spectrum some 647,921 businesses have a workforce size ranging from 20 to 499 employees, according to the U.S. SBA.

Additionally, SMBs and micro-SMBs employ a total of 61.6 million people, which represents 45.9% of the entire U.S. workforce.

Although small businesses with 1 to 100 employees and even micro SMBs with 1 to 20 workers, may not rack up hourly downtime costs exceeding $100,000 or $1million (USD) like their enterprise counterparts. Nonetheless, the consequences of unplanned outages can be devastating to their business. SMBs and micro SMBs typically lack the budgets of their larger mid-sized and enterprise counterparts. And more often than not , a micro-SMB or a small satellite office for a law firm, hospital, bank/brokerage house or trucking, transportation or retail facility will not have dedicated onsite technical IT and security resources.

[1] United States Small Business Administration Office of Advocacy. https://advocacy.sba.gov/2023/03/07/frequently-asked-questions-about-small-business-2023/

[2] U.S. Chamber of Commerce. “The 2023 State of Small Business Report.” https://www.uschamber.com/small-business/state-of-small-business-now

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.** The ITIC 2024 Global Server Hardware Security Reliability Survey which polled 2,000 businesses found that 84% of respondents attributed their network outages to a security breach or vulnerability. 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 swindles which continue today.

ITIC expects that the ongoing threat of security and data breaches coupled with human error, software bugs and flaws, and incompatibilities among systems, applications and networks will continue unabated and contribute to the rise in unplanned downtime outages and costs.

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.

Calculating the Consequences of Downtime for SMBs

Let's be blunt: in a 24 x 7 interconnected world, there is never a good time for unplanned downtime.

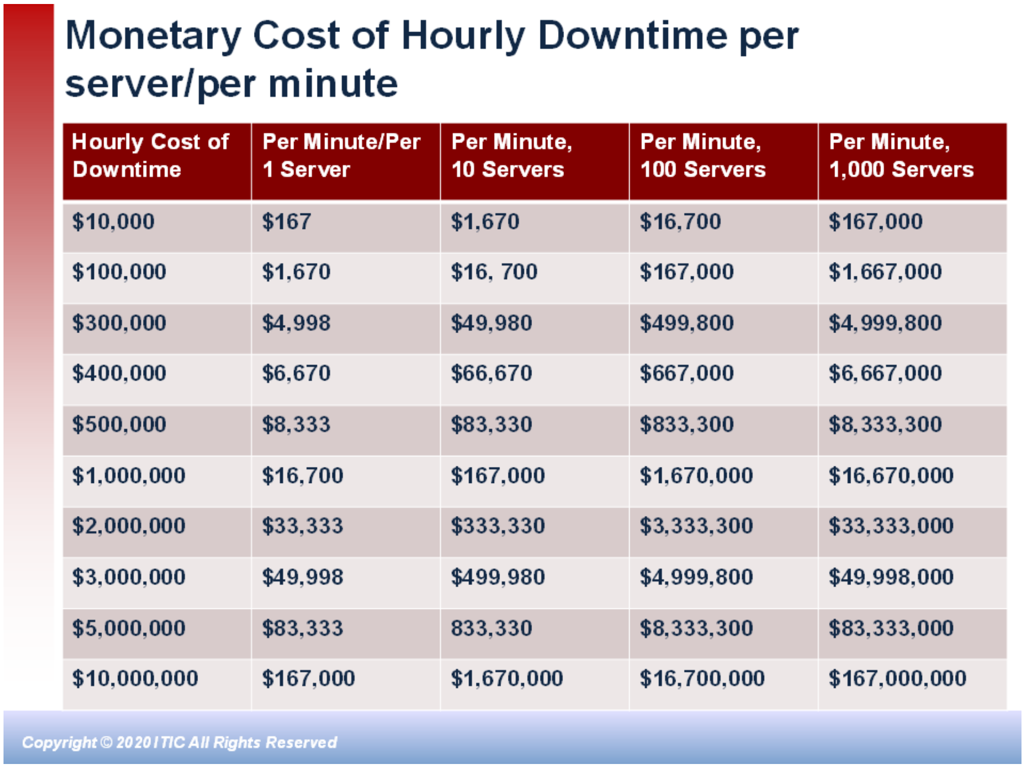
Downtime impacts revenue, employee productivity and daily business transactions and operations.

When networks, systems, devices, and applications are unavailable, business ceases. By association, the company's customers, business partners and suppliers may also be negatively impacted. An outage may also damage the organization's reputation and result in lost business.

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.

Exhibit 1 depicts the monetary costs of per server/per minute downtime involving a single server to as many as 1,000 servers in which businesses calculate hourly downtime costs from $100,000 to $10,000,000 million (USD).

Exhibit 1. Hourly Downtime Costs Per Server/per minute



Monetary Cost of Hourly Downtime per server/per minute

Hourly Cost of Downtime	Per Minute/Per 1 Server	Per Minute, 10 Servers	Per Minute, 100 Servers	Per Minute, 1,000 Servers
$10,000	$167	$1,670	$16,700	$167,000
$100,000	$1,670	$16, 700	$167,000	$1,667,000
$300,000	$4,998	$49,980	$499,800	$4,999,800
$400,000	$6,670	$66,670	$667,000	$6,667,000
$500,000	$8,333	$83,330	$833,300	$8,333,300
$1,000,000	$16,700	$167,000	$1,670,000	$16,670,000
$2,000,000	$33,333	$333,330	$3,333,300	$33,333,000
$3,000,000	$49,998	$499,980	$4,999,800	$49,998,000
$5,000,000	$83,333	833,330	$8,333,300	$83,333,000
$10,000,000	$167,000	$1,670,000	$16,700,000	$167,000,000

Copyright © 2020 ITIC All Rights Reserved

Source: ITIC 2024 Hourly Cost of Downtime Survey

As **Exhibit 1** illustrates a 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.

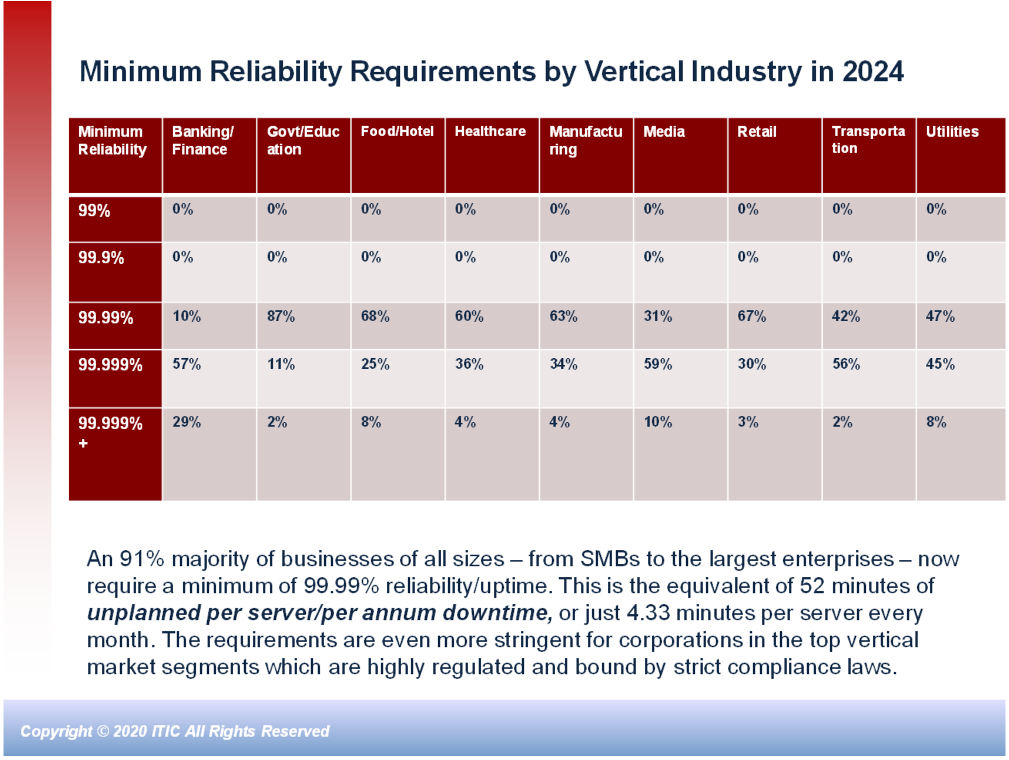
Small businesses are equally at risk, even if their potential monetary downtime losses are a fraction of large enterprises. For example, an SMB company that estimates that one hour of downtime “only” costs the firm $10,000 could still incur a cost of $167 for a single minute of per server downtime on 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 a 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 the SMB out of business – or severely damage its reputation and cause it to lose business.
In 2024 and beyond, corporations have a near total reliance on their personal and employer-owned interconnected networks

and applications to conduct business. Corporate revenue and productivity are inextricably linked to the reliability and availability of the corporate network and its data assets.

The minimum reliability/uptime requirements for the top vertical market segments encompassing SMBs, SMEs and large enterprises in the top vertical industries are even more stringent and demanding than the corporate averages in over 40 other verticals as Exhibit 2 below illustrates.

Exhibit 2. Minimum Reliability Requirements by Vertical Industry



Minimum Reliability Requirements by Vertical Industry in 2024

Minimum Reliability	Banking/ Finance	Govt/Education	Food/Hotel	Healthcare	Manufacturing	Media	Retail	Transportation	Utilities
99%	0%	0%	0%	0%	0%	0%	0%	0%	0%
99.9%	0%	0%	0%	0%	0%	0%	0%	0%	0%
99.99%	10%	87%	68%	60%	63%	31%	67%	42%	47%
99.999%	57%	11%	25%	36%	34%	59%	30%	56%	45%
99.999%+	29%	2%	8%	4%	4%	10%	3%	2%	8%

An 91% majority of businesses of all sizes – from SMBs to the largest enterprises – now require a minimum of 99.99% reliability/uptime. This is the equivalent of 52 minutes of ***unplanned per server/per annum downtime,*** or just 4.33 minutes per server every month. The requirements are even more stringent for corporations in the top vertical market segments which are highly regulated and bound by strict compliance laws.

Copyright © 2020 ITIC All Rights Reserved

Source: ITIC 2024 Hourly Cost of Downtime Survey

The above industries are highly regulated and incorporate strict compliance laws. But even without regulatory oversight the top vertical market segments are highly visible. Their business operations demand near flawless levels of **uninterrupted, continuous operation.**

These statistics reinforce what everyone knows: infrastructure, security, data access and data privacy and adherence to regulatory compliance are all imperative.

Server hardware, server OS and application reliability all have direct and far-reaching consequences on the corporate bottom line and ongoing business operations. Unreliable and unavailable server hardware, server operating systems and applications will irreparably damage companies' reputation.

In certain extreme cases, business, and monetary losses because of unreliable servers can cause an enterprise to miss its quarterly or annual revenue forecasts or even go out of business as a direct consequence of sustained losses and litigation brought on by the outage.

Minimum Reliability Requirements Increase Year over Year

Time ***is*** money. Time also equates to productivity and the efficiency and continuity of ongoing, ***uninterrupted*** daily operations. If any of these activities are compromised by outages for any reason – technical or operational failure that renders the systems and the data unavailable. This negatively impacts the corporate enterprise. The longer the outage lasts, the higher the likelihood of having a domino effect on the corporation's customers, business partners and suppliers. This in turn will raise Total Cost of Ownership (TCO) and undermine the return on investment (ROI).

High reliability and high availability are necessary to manage the corporation's level of risk and exposure to liability and potential litigation resulting from unplanned downtime and potential non-compliance with regulatory issues. This is evidenced by corporations' reliability requirements which have increased every year for the past 11 years that ITIC has polled organizations on these metrics.

Consider the following: in 2008, the first year that ITIC surveyed enterprises on their Reliability requirements, 27% of businesses said they needed just 99% uptime; four-in-10 corporations – 40% - required 99.9% availability. In that same 2008 survey, only 23% of firms indicated they required a minimum of "four nines" or 99.99% uptime for their servers, operating systems, virtualized and cloud environments, while a seven percent (7%) minority demanded the highest levels of "five nines" – 99.999% or greater availability.

A decade ago, in ITIC's 2014 Hourly Cost of Downtime poll, 49% of businesses required 99.99% or greater reliability/uptime, four nines - 99.99%+ and greater reliability are mission-critical are now the minimum standard for reliability. In ITIC's latest 2024 survey ***– none – 0%- of survey respondents*** indicated their organizations could live with just "two nines" – 99% uptime or 88 hours of annual unplanned per server downtime!

"Four nines" or 99.99% uptime and availability is the average minimum requirement for 88% of organizations. As of April 2024, 39% of ITIC survey respondents in companies of all sizes and across all vertical industries said their businesses now strive for "five nines" or 99.999% system, device, application and network uptime and availability. This equates to 5.26 minutes of per server/per annum unplanned downtime.

Increasingly many organizations have even more stringent reliability needs. Requirements of "five and six nines" – 99.999% and 99.9999% - reliability and availability are becoming much more commonplace among all classes of businesses. The reasons are clear: corporations have no tolerance for downtime. They, their end users, business partners, customers, and suppliers all demand uninterrupted access to data and applications to conduct business 24 x7 irrespective of geographic location.

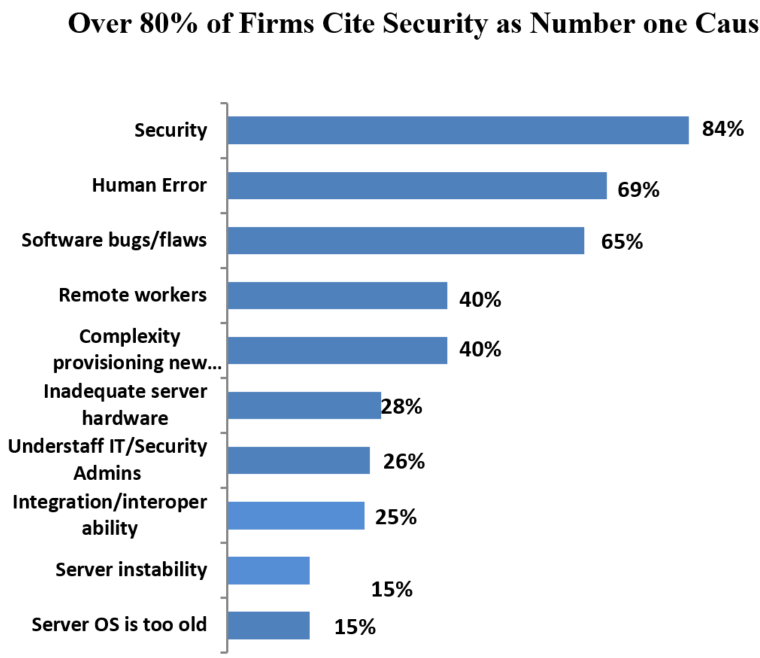
Security Attacks: End Users are Biggest Culprits in Downtime

ITIC's latest survey results found that security issues and end user carelessness were among the top causes of unplanned system and network downtime in 2024. Hacking is big business. The hackers themselves are more organized and data breaches and malware are more targeted, sophisticated, and pernicious.

- **Security attacks –** including targeted attacks by organized hackers, Ransomware attacks, Phishing and Email scams and CEO fraud hacks – now rank as the top cause of downtime, according to 84% of ITIC survey respondents **(See Exhibit 3).**

- **Human Error –** is also increasingly contributing to corporate downtime and is among the top three causes of company outages along with software flaws/bugs, according to 69% of ITIC survey respondents. End user carelessness encompasses everything from company employees being careless with and losing their own and company owned BYOD devices like laptops, tablets, and mobile phones. Many users fail to properly secure their devices and when they are lost or stolen, the intellectual property (IP) and sensitive data is easily accessible to prying eyes and thieves. End user carelessness also manifests itself in other ways: naïve users click on bad links and fall prey to Phishing scams, CEO fraud and leave themselves and their company wide open to security hacks.

Exhibit 3. Security, User Error and Software Bugs are Top Causes of Downtime



Over 80% of Firms Cite Security as Number one Cause of Downtime

Source: ITIC 2024 Hourly Cost of Downtime Survey

The percentage of enterprises unable to calculate the hourly cost of downtime consistently outpaced those that had the ability to estimate downtime costs over the last 10 years. Of the 39% that responded “Yes” only 42% - can make detailed downtime estimates. Only 22% of organizations, or approximately one in five, can accurately assess the hourly cost of downtime and its impact on productivity, daily operations/transactions, and the business’ bottom line.

Consequences of Downtime

To reiterate: there is never an opportune time for an unplanned network, system, service failure or security hack. The hourly costs associated with downtime paint a grim picture. But they do not tell the whole story of just how devastating downtime can be to the business’ bottom line, productivity, and reputation.

The ITIC survey data revealed that although monetary losses topped users’ list of downtime concerns, it was one of several factors worrying organizations. The top five business consequences that concerned users are (in order):

- Transaction/sales losses.
- Lost/damaged data.
- Customer dissatisfaction.
- Restarting/return to full operation.
- Regulatory compliance exposure.

Consider these scenarios:

- **Healthcare:** A system failure during an operation could jeopardize human lives. Additionally, targeted hacks by organized groups of professional “black hat” hackers increasingly seek out confidential patient data like Social Security numbers, birth records and prescription drug information. Healthcare is one of the most highly regulated vertical industries and the U.S. and other countries’ government agencies worldwide are aggressively penalizing physicians, clinics, hospitals and healthcare organizations that fail to live up to regulatory compliance standards with respect to privacy and security. And small doctors’ offices, clinics and labs may be even more vulnerable since they usually do not have dedicated onsite and security staff.

- **Banking and Finance:** Unplanned outages during peak transaction time periods could cause business to halt. Banks and stock exchanges could potentially be unable to complete transactions such as processing deposits and withdrawals and customers might not be able to access funds in ATM machines. Brokerage firms and stock exchanges routinely process millions and even billions of transactions daily. The exchanges could lose millions of dollars if transactions or trading were interrupted for just minutes during normal business hours. Financial institutions and exchanges are also among the most heavily regulated industries. Any security breaches will be the subject of intense scrutiny and investigation.

- **Government Agencies:** A system failure within the Social Security Administration (SSA) that occurs when the agency is processing checks could result in delayed payments, lost productivity and require administrators to spend hours or days in remedial action.

- **Manufacturing:** The manufacturing vertical is one of the top verticals targeted by hackers, surpassing the healthcare industry. According to the US National Center for Manufacturing Sciences (NCMS), 39% of all cyber-attacks in 2016 were against the manufacturing industry. Since January of 2017 and continuing to the present, March 2024, attacks against manufacturing firms are up 38% thanks to technologies like Machine Learning (ML), Artificial Intelligence (AI) and IoT. Manufacturers are often viewed as “soft targets” or easy entry points of entry into other types of enterprises and even government agencies. Efficiency and uninterrupted productivity are staples and stocks in trade in the manufacturing arena. Any slips are well documented and usually well publicized. The manufacturing shop floor has a near total reliance on robotics and machines and automated networks to get the job done. There are thousands of potential entry points – or potential vulnerability points into the network. The implementation of industrial control systems (ICS), centralized command centers that control and connect processes and machines, and the Internet of Things (IoT) external device integration like cameras and robotics, add multiple points of process failure and access points with possible wormholes allowing hackers to infiltrate larger networks.

- **Retail:** Retailers and sales force personnel trying to close end-of-quarter results would be hard pressed if an outage occurred, which rendered them unable to access or delay access to order entries, the ability to log sales and issue invoices. This could have a domino effect on suppliers, customers, and shareholders.

- **Travel, Transportation and Logistics (TT&L):** An outage at the Federal Aviation Administration’s (FAA) air traffic control systems could cause chaos: air traffic controllers would find it difficult to track flights and flight paths, raising the risk of massive delays and in a worst-case scenario, airborne and even runway collisions. A June 2019 report released by the U.S. General Accounting Office (GAO)[3] confirmed that 34 airline IT outages occurred over a three-year span encompassing the years 2015 through 2018. According to the GAO “about 85% of these led to flight delays or cancellations. In 2023 and 2024, the aviation industry has been hit hard by flight cancellations and delays due to faulty aircraft components before and during flights. This always results in a domino effect that impacts other businesses. Additionally, the U.S. Department of Transportation’s 2023 Annual Transportation Statistics Annual Report[4] noted the entire U.S. transportation system vulnerable to cyber and electronic disruptions. Aviation systems are dependent on electronic and digital navigation aids, communication systems, command and control technologies, and public information systems. Outages and cybersecurity issues also plague other transportation sectors like the trucking and auto industry. Cyber incidents pose a variety of threats to transportation systems. Cyber vulnerabilities have been documented in multimodal operational systems, control centers, signaling and telecommunications networks, draw bridge operations, transit and rail operations, pipelines, and other existing and emerging technologies. State and local governments face growing threats from hackers and cybercriminals, including those who use ransomware software that hijacks computer systems, encrypts data, and locks machines, holding them hostage until victims pay a ransom or restore the data on their own. A 2021 Report by SOTI, a global management firm headquartered in Ontario, Canada found that in the trucking industry "…When trucks are on the road, T&L companies make money. When they're not, they're losing money due to the cost of downtime which averages $448 to $760 USD per vehicle per day."

[3] June 2019 Commercial Aviation, Information on Airline IT Outages - U.S. General Accounting Office (GAO), https://www.gao.gov/assets/gao-19-514.pdf

[4] U.S. Department of Transportation, "Transportation Statistics Annual Report 2023," Pg. 1 -39, https://www.bts.gov/sites/bts.dot.gov/files/2023-12/TSAR-2023_123023.pdf

Conclusions

Hourly downtime costs and risks will continue to rise. Downtime of any duration is expensive and disruptive. When a mission critical application, server or network is unavailable for even a few minutes, business risks increase commensurately, including:

- Lost productivity.
- Lost, damaged, destroyed, changed or stolen data.
- Damage to the company's reputation potentially can result in lost business.
- Potential for litigation by business partners, customers, and suppliers.
- Regulatory compliance exposure.
- Potential for civil, criminal liabilities, penalties and even jail time for company executives.
- Potential for unsustainable losses which can result in companies going out of business.

To minimize downtime and increase availability corporations must ensure that robust reliability is an inherent feature in all servers, network connectivity devices, applications, and mobile devices. A crucial component of this strategy is to deploy the appropriate device and network security and monitoring tools. Every 21st Century network environment needs robust security on all its core infrastructure devices and systems (e.g., servers, firewalls, routers, etc.) and continuous, comprehensive end-to-end monitoring for complex, distributed applications in physical, virtual and cloud environments.

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

ITIC

✉ ldidio@itic-corp.com

https://itic-corp.com/

@lauradidio