INFORMATION TECHNOLOGY
INTELLIGENCE CONSULTING

Information Technology Intelligence Consulting

ITIC

ITIC 2021 Global Server Hardware, Server OS Security Report

June 2021

Table of Contents

Executive Summary

For the third straight year, corporate enterprises ranked mission critical servers from IBM, Lenovo, Huawei and Hewlett-Packard Enterprise (in that order) as the most secure platforms which experienced the least amount of successful data breaches and proved the toughest for hackers to crack.

Those are the results of the latest ITIC Global Server Hardware Security survey which compared the security features and functions of 15 different server platforms. ITIC's independent Web-based survey polled over 1,100 businesses worldwide across 28 different vertical market sectors from January 2021 through mid-June 2021.

IBM, Lenovo, Huawei, HPE and Cisco maintained their top positions as the most reliable and secure server platforms despite a significant 42% spike in security hacks and data breaches during the COVID-19 global pandemic over the last 18 months.

The top servers led by the IBM Z; IBM POWER; the Lenovo ThinkSystem and the Huawei KunLun (in that order), all scored their respective best security and reliability/uptime performances ever during the COVID-19 era and notably achieved the best security results among all 15 mainstream server hardware platforms in every security category in ITIC's latest poll, including:

- The fewest number of successful security hacks/data breaches.
- The least amount of overall unplanned server downtime for ***any*** reason and the least amount of unplanned server downtime as the result of a security incident.
- The fastest Mean Time to Detection (MTTD) from the onset of the attack until the company isolated and shut it down.
- The fastest Mean Time to Remediation (MTTR) to restore servers, applications and networks to full operation.
- The least amount of lost, stolen, destroyed, damaged or changed data as a direct consequence of a security data breach (e.g. Ransomware, phishing scam or CEO fraud).
- The least amount of monetary losses due to a successful security hack.
- The highest confidence in the embedded security of the server hardware to deliver alerts/warnings and repel security attacks and data breaches.

Business critical systems from Hewlett-Packard Enterprise (HPE) and Cisco also delivered a high level of security and rounded out the top five most secure server distributions. On the other end of the spectrum, unbranded White box servers again proved the most porous, registering the highest totals of successful security penetrations.

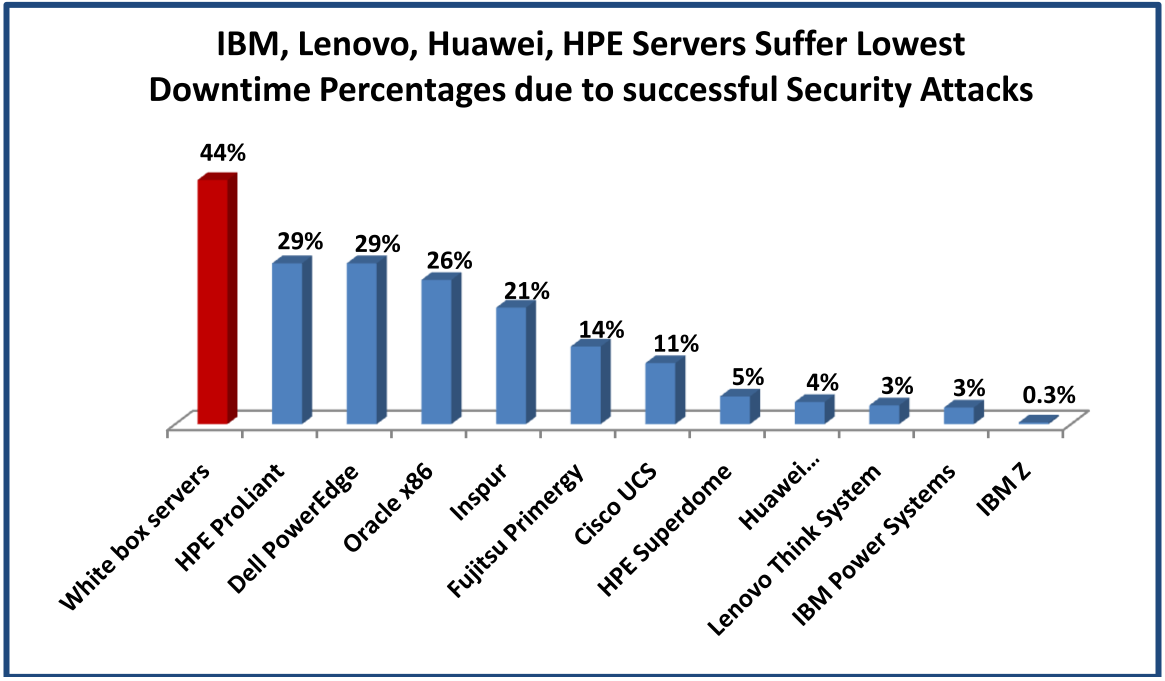
ITIC's most recent Global Security poll similarly found that IBM, Lenovo, Huawei and HPE mission critical servers experienced the lowest percentages of downtime due to successful security hacks and data breaches (**See Exhibit 1).**

The IBM Z mainframe outpaced all other server distributions and is in a class of its own as it achieved its most robust security and reliability ratings to date in the latest ITIC study.

Only a minuscule – 0.3% - of IBM Z high end servers, suffered a successful data breach. Among other mainstream hardware platforms, just three percent (3%) of IBM Power Systems and Lenovo ThinkSystem users reported their systems were successfully hacked, while fewer than four percent (4%) of Huawei KunLun and five percent (5%) HPE Integrity Superdome server customers reported a successful security breach from January 2021 through mid-June 2021.

Just over one-in-ten or 11% of Cisco UCS servers were successfully hacked. Cisco's hardware performed extremely well, particularly when one considers that many of the UCS servers are deployed in remote locations and at the network edge, which frequently are the first line of defense and take the brunt of hack attacks. Unbranded White box servers were the most vulnerable to security penetrations; 44% of ITIC survey respondents reported those systems were successfully hacked.

Exhibit 1. IBM, Lenovo Servers Most Secure, Toughest to Crack



Source: ITIC 2021 Global Server Hardware, Server OS Security Survey

Overall, ITIC's survey findings indicate that there is a clear and widening gap in server hardware security and reliability among the top performing platforms and the most insecure offerings. The global pandemic sparked a wave of COVID-19 related data breaches, Ransomware, Phishing, Business Email Compromise (BEC), CEO fraud and attacks that continue unabated.

ITIC's most recent survey results indicate that reliability and security are inextricably intertwined and even symbiotic. Security and data breaches immediately undermine compromise server, application and network uptime and availability. Security hacks and data breaches are expensive and dangerous. They compromise businesses' intellectual property (IP) as well as that of business partners, customers and suppliers. A successful security hack can also expose employees' personal data.

It is no coincidence that the top five most reliable server platforms: the IBM Z, the IBM Power Systems, Lenovo ThinkSystem, Huawei KunLun and Fusion Servers, the HPE Superdome Integrity and Cisco UCS (in that order) also boast the most formidable security.

Introduction

The global pandemic sparked a wave of COVID-19 related data breaches, Ransomware, Phishing, Business Email Compromise (BEC), CEO fraud and attacks that continue unabated – across every vertical sector targeting myriad corporate and consumer devices and software.

No one and nothing is immune. This makes inherent, robust infrastructure security imperative.

ITIC's latest poll found that overall, 73% of survey respondents fear their organizations will fall victim to a targeted attack by professional hackers over the next 12 to 18 months. This timetable coincides with the widespread trend of K-through-12 schools, colleges and universities, students and teachers that have done remote learning that are now preparing to head back to the classroom. Likewise, many corporate enterprises and government agencies are now transitioning to a hybrid teleworking from home model as a health safety measure.

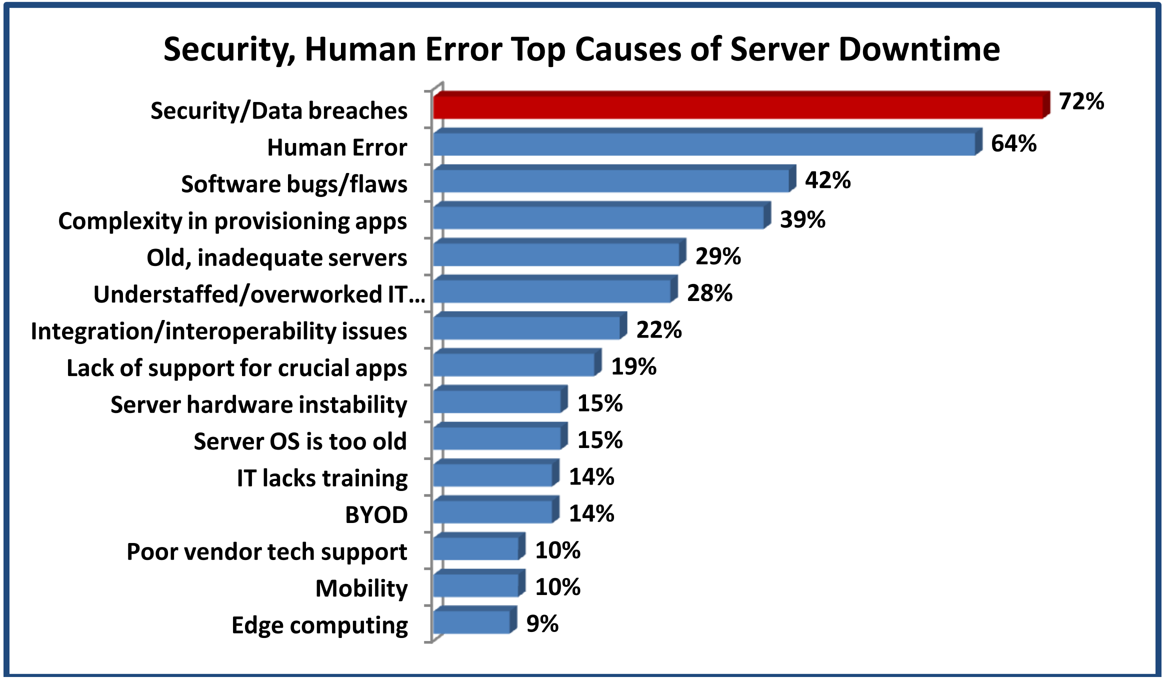
ITIC's latest security survey findings are bolstered by various U.S. Federal government agencies which have issued multiple cybersecurity risk alerts since the beginning of 2020. The Federal Bureau of Investigation (FBI); the Department of Homeland Security Cybersecurity and Infrastructure Security Agency (CISA) and the Securities and Exchange Commission's (SEC) Office of Compliance Inspections and Examinations (OCIE).

The COVID-19-related cybersecurity threats include: scams targeting state unemployment insurance benefits and Federal stimulus checks; healthcare; bank; elder; crypto currency and government fraud schemes, according to FBI alerts published in May and June. The FBI notes, it has also seen instances of "…criminals engaging in online predatory behavior targeting children who are continuing their education from home during the pandemic."

The strong security results posted by IBM, Lenovo, Huawei, HPE and Cisco (in that order) are especially noteworthy since they occurred during the height of the COVID-19 global pandemic. Some 40% of ITIC survey respondents reported their servers, operating systems and critical business applications suffered successful security hacks since the outset of COVID-19 in early 2020. This is an increase of nine percentage points from 31% in just the last six months and a hike of 21 percentage points based on the 19% of organizations that said their servers were successful hacked in ITIC's 2020 Global Server Hardware, Server OS Reliability survey.

Security is a technology and business issue that impacts all enterprises. Some 72% of respondents cited security and data breaches as the greatest threat to server, application, data center, network edge and cloud ecosystem reliability **(See Exhibit 2)**. The hacks are more targeted, pervasive and pernicious. They are designed to inflict maximum damage and losses on their enterprise and consumer victims.

Exhibit 2. Security, Human Error, Software Bugs Top Causes of Downtime



Source: ITIC 2021 Global Server Hardware, Server OS Security Survey

The Threat Landscape: Security Vulnerabilities and Data Breaches Are Biggest, Most Expensive Reliability Threat

Data breaches are big business and a primary business for the burgeoning professional hacking community. A successful hack is expensive on many levels. In 2020, the cost of a data breach averaged $3.86 million, according to the 2020 Cost of a Data Breach Study jointly conducted by IBM and the Ponemon Institute[1]. This represents a 10% increase since 2015. Actual costs will vary according to the duration and severity of the hacks. Ransomware attacks continue to surge.

[1] "2020 Cost of a Data Breach Study," IBM and the Ponemon Institute. URL: https://www.ibm.com/security/data-breach

And they are very costly. The May 7, 2020 ransomware attack by the DarkSide hackers shut down the Colonial Pipeline Co. for six days[2]. The Colonial Pipeline supplies 45% of gas and diesel fuel to the U.S. East Coast from New Jersey to Florida. It shut down deliveries and caused gas shortages in several states including Florida, North Carolina, and Virginia. It only ended when Colonial Pipeline, chief executive Joseph Blount agreed to pay the hackers a $4.4 million ransom. Blount told The Wall Street Journal that he authorized the ransom payment of $4.4 million because executives were unsure how badly the cyberattack had breached its systems, and consequently, how long it would take to bring the pipeline back.

The Colonial Pipeline Ransomware attack is just one of many. It underscores the vulnerabilities, risks and the high cost associated with successful security attacks. The Colonial Pipeline Ransomware hack further reinforces the need to have a top notch, robust security infrastructure in place. Server hardware is the foundational element of every corporate network and ecosystem.

A DTEX Systems Report found that "only 30% of organizations were prepared to secure a complete shift to remote work." The DTEX Systems study also found that almost 75% of organizations are concerned about the security risks introduced by users working from home and 73% of businesses admitted they have partial or no visibility into user activity if their VPN is disabled by remote workers. Another alarming finding is that teleworkers use their work laptops for personal use; with 25% of respondents acknowledging this increases the risk of drive-by-downloads, with 15% saying their firms are more susceptible to Phishing attacks.

ITIC's most recent study indicates that the Hourly Cost of Downtime continues to climb. It now exceeds $300,000 for 89% of SME and large enterprises. Overall, 42% of mid-sized and large enterprise survey respondents reported that, on average a single hour of downtime, costs their firms over one million ($1 million). In a worst case scenario a data breach that occurs during peak usage hours and interrupts crucial business operations can cost businesses millions per minute. Any organization that suffers a protracted outage of hours or days as the result of targeted Ransomware attack will almost certainly incur many millions in damages.

Besides the obvious monetary losses due to productivity and disrupted operations, businesses must factor in amount of manpower hours and the number of IT and security administrators

[2] "Colonial Pipeline CEO Tells Why He Paid Hackers a $4.4 Million Ransom," The Wall Street Journal, May 19, 2021. URL: https://www.wsj.com/articles/colonial-pipeline-ceo-tells-why-he-paid-hackers-a-4-4-million-ransom-11621435636

involved in remediation efforts and full return to operation. Companies must also determine whether or not any data or intellectual property (IP) was lost, stolen, damaged, destroyed or changed. Organizations must also add in the cost of any litigation as well as potential civil or criminal fines/penalties associated with security incidents and data breaches. Some costs, like damage to an organization's reputation are incalculable and may result in lost business.

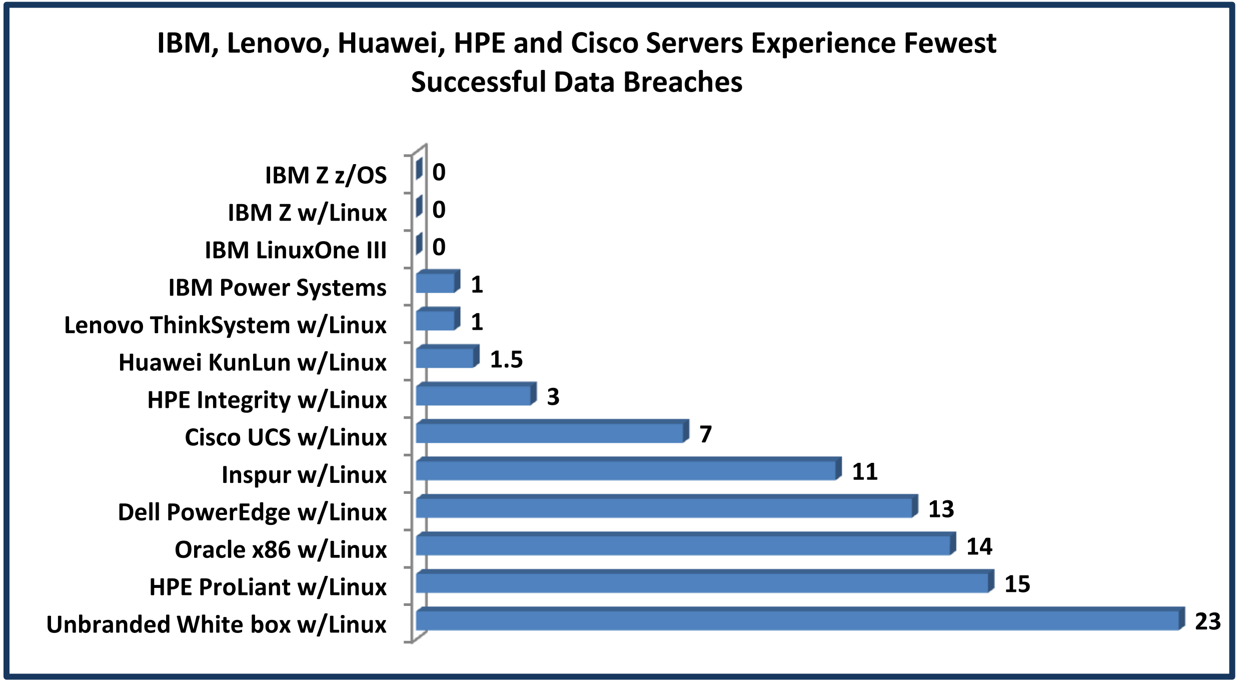
Hackers pick and choose their targets with great precision and are quick to take advantage of every opportunity. The COVID-19 pandemic is a prime example. Hackers immediately set their sights on teleworkers and remote learning students taking online and Zoom classes. They zeroed in on so-called "soft targets." Local and state municipalities; small and mid-sized school districts, hospitals, health care clinics, doctors' offices and branch bank offices that may lack full-time onsite security and IT administrators and may not have installed the latest security.

Server Vendors: IBM, Lenovo, Huawei and HPE Step Up Security

It's no surprise that vendors like IBM, Lenovo, Huawei, HPE, which perennially achieve top server reliability ratings are also among the most secure hardware platforms. These vendors and more recently Cisco, have made server security – and in Lenovo's case server, PC and laptop security – a top priority and have invested heavily in bolstering the inherent security of their product offerings over the last several years. So, when the COVD-19 pandemic hit, they already had strong, embedded security and this stood them in good stead.

As **Exhibit 3** indicates, the most secure server hardware platforms experienced the fewest successful security breaches. The IBM Z running the z/OS and Red Hat Enterprise Linux (RHEL) and IBM LinuxONE III respondents all said those platforms had no successful security hacks over the 16 months. They were followed by the IBM Power Systems and Linux ThinkSystem servers with one each; Huawei KunLun which averaged two hacks; the HPE Integrity with three successful penetrations and Cisco's UCS servers with seven data breaches. The unbranded White box servers were the most porous, averaging 20 successful data breaches in the past 16 months.

Exhibit 3. IBM, Lenovo, Huawei, HPE and Cisco Servers Experience Fewest Successful Hacks



Source: ITIC 2021 Global Server Hardware, Server OS Security Survey

Data & Analysis: Vendor Security Results

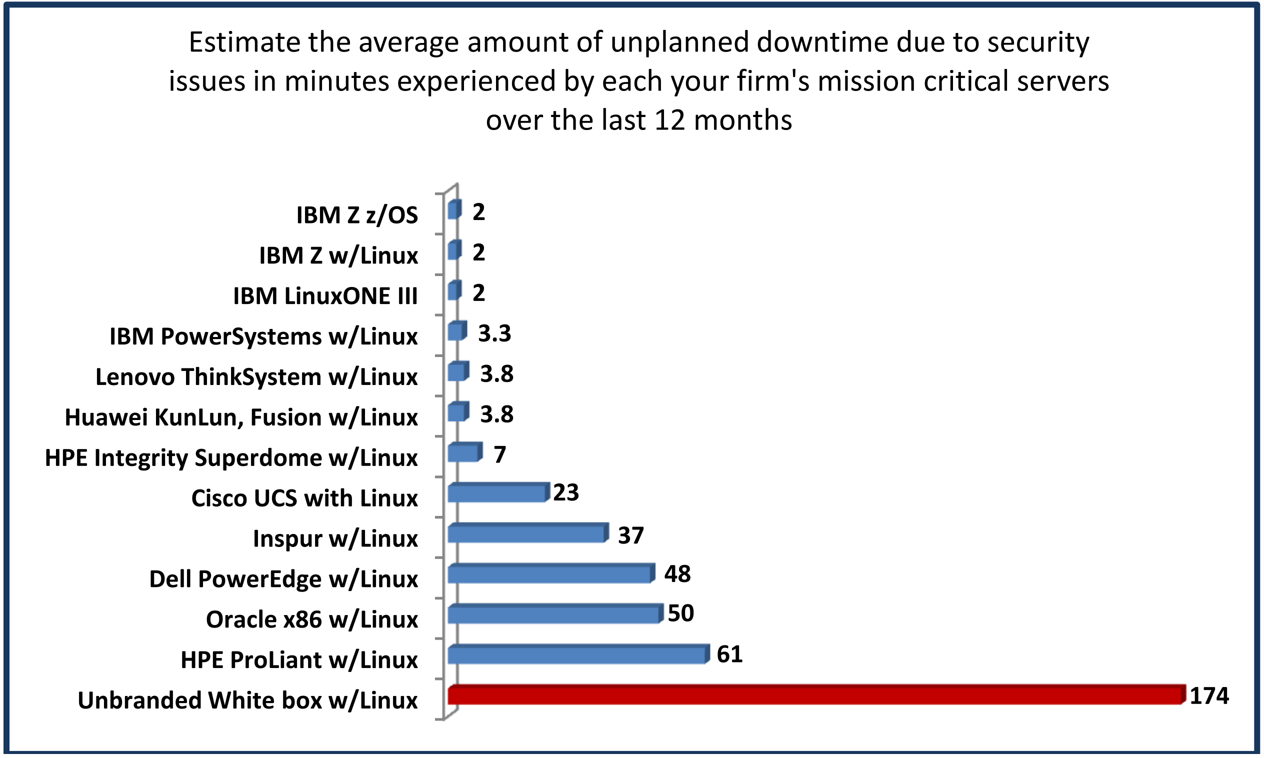
To reiterate, ITIC's 2021 Global Server Hardware Security survey found that the IBM Z, IBM Power Systems, Lenovo ThinkSystem and Huawei KunLun and Fusion servers (in that order) achieved the best results in every security category including:

- The fewest number of **successful** security hacks/data breaches.
- The least amount of overall unplanned server downtime for ***any*** reason and the least amount of unplanned server downtime as the result of a security incident.
- The fastest Mean Time to Detection (MTTD) from the onset of the attack until the company isolated and shut it down.
- The fastest Mean Time to Remediation (MTTR) to restore servers, applications and networks to full operation.
- The least amount of lost, stolen, destroyed, damaged or changed data as a direct consequence of a security data breach (e.g. Ransomware, phishing scam or CEO fraud).
- The least amount of monetary losses due to a successful security hack.
- The highest confidence in the embedded security of the server hardware to deliver alerts/warnings and repel security attacks and data breaches.

As **Exhibit 4** illustrates, the IBM Z, the IBM Power Systems, the Lenovo ThinkSystem and Huawei KunLun mission critical servers experienced the least amount of unplanned downtime as the direct result of successful security incidents and data breaches.

The IBM Z and IBM LinuxONE III overall averaged just 2 minutes each of per server unplanned downtime due to security issues. They were followed closely by IBM's POWER8 and POWER9 servers which experienced just over 3 minutes of per server unplanned outages as the result of a security issue; the Lenovo ThinkSystem hardware and Huawei KunLun and Fusion servers each experienced an average of 3.8 minutes of per server unplanned downtime associated with security incidents. Once again, unbranded White box servers, many of which run unlicensed versions of server operating systems and software applications, racked up 174 minutes or close to three hours each of downtime directly attributable to security-related issues. That makes the most secure IBM Z servers up to 87x more secure and reliable than the least secure White box hardware, while the IBM POWER8 and POWER9 offerings are up to 58x more secure than unbranded White box servers.

Exhibit 4. IBM, Lenovo and Huawei Deliver Best in Class Server Security



Source: ITIC 2021 Global Server Hardware, Server OS Security Survey

Mean Time to Detection is a Critical Barometer

Security hacks and data breaches are a fact of doing business in the digital age. At some point, every organization and its critical main line of business servers, server operating systems and applications will be the victims of an attempted or successful data breach of some type.

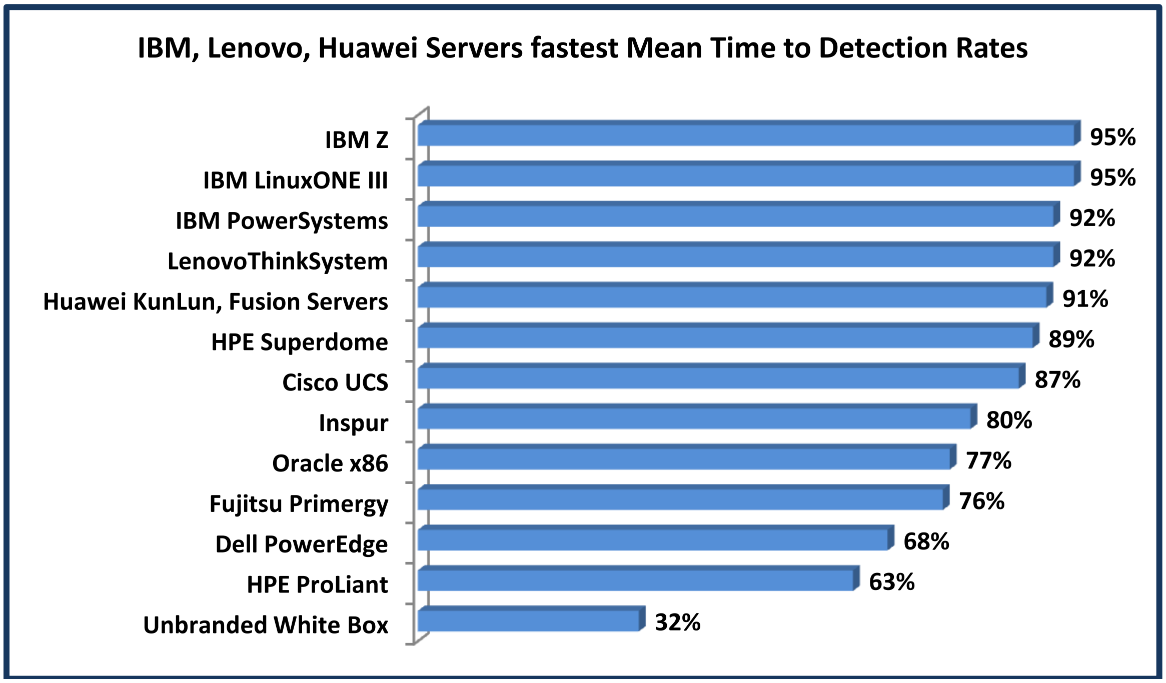
Organizations must rely on strong embedded server and infrastructure security that recognizes the danger, sends alerts and alarms and that possess the ability to isolate the threats. Strong preparedness on the part of the corporation and having a well trained staff of security professionals and IT administrators are of paramount importance.

The more quickly the company's servers and software can detect a security issue and respond to it, the greater the chances of isolating and thwarting the attack ***before*** it can infiltrate the network ecosystem, interrupt data transactions and daily operations and access sensitive data and IP.

Exhibit 5 shows that once again, the IBM Z, IBM Power Systems, Lenovo ThinkSystem, Huawei KunLun and Fusion Servers, HPE Superdome and Cisco UCS Servers (in that order) excelled in thwarting hacks. These servers had the best Mean Time to Detection (MTTD) percentages among all server platforms.

An overwhelming 95% of IBM Z, IBM LinuxOne III survey respondents indicated their servers were able to detect an attempted security breach "Immediately or within the first 10 minutes" of the hack and shut it down. They were followed in order by the IBM Power Systems, Lenovo ThinkSystem and Huawei KunLun distributions; 92% of each of those platform users said they were able to recognize and repel a security breach "Immediately or within the first 10 minutes." The faster the critical core infrastructure servers, operating systems and mission critical applications can repel a hack, the better the chances the business will experience little to no downtime or fall victim to stolen, changed, damage or compromised data and IP theft.

Exhibit 5. Over 90% of IBM, Lenovo and Huawei Servers Detect Security Attacks Immediately or within the First 10 Minutes



Source: ITIC 2021 Global Server Hardware, Server OS Security Survey

Server Vendor Security Results

IBM Security Survey Highlights

- **IBM Z** servers continue to achieve top grades for overall reliability, accessibility, performance, and security among all server platforms. The IBM Z family – the "Z" stands for zero downtime - consistently outperforms **all** competitors in every reliability category and delivers the lowest total cost of ownership (TCO) and fastest return on investment (ROI). The z13, z14 and z15 Systems servers scored the best reliability/uptime, application availability ratings and security across the board in terms of actual minutes of unplanned per server/per annum downtime. The IBM z mainframe and the IBM LinuxONE distributions both exhibit true fault tolerance experiencing just 0.60 - less than one minute of ***unplanned*** per server, per annum annual downtime due to server flaws, compared to the 0.74 seconds the Z and LinuxONE platforms averaged in ITIC's 2019 Global Server Reliability poll. While the reduction of 0.14 seconds of YoY per server downtime sounds negligible, in fact it cuts downtime by nearly 19% and lowers the TCO of the IBM Z and LinuxONE by $230 – from $1,232 per server/per minute in 2019 to $1,002 per server/per minute in the latest ITIC 2021 Global Server Hardware Security study. Overall, the IBM Z registers just 4.32 seconds of near imperceptible monthly downtime. Equally important, given the ongoing surge in security hacks and data breaches, is the IBM Z server's superlative security. The Z continues to register the lowest percentage - less than one percent - of successful data breaches from January through mid-June 2021. Additionally, IBM Z and LinuxONE III survey respondents also reported the quickest Mean Time to Detection (MTTD) with 95% of ITIC enterprise respondents stating their security and IT administrators were able to detect and shut down hacks on these platforms. Singularly and collectively, these results underscore the success of the Z and LinuxONE III offerings. The platforms have also been bolstered by IBM's 2019 acquisition of Red Hat; this has resulted in a significant uptick of Linux workloads on the Z and LinuxONE platforms. IBM executives publicly stated the company has seen a 55% increase in Linux MIPS. They also noted that 92 of IBM's top 100 Z clients run Linux workloads. Overall, the Z platform averages 100 to 200 new deployments annually, according to IBM.

- **IBM's LinuxONE III** is based on the IBM Z platform. It specifically addresses hybrid cloud environments and utilizes the Z's pervasive encryption. The LinuxONE III platform and the IBM z15 also incorporate the IBM Hyper Protect Data Controller, which delivers transparent, end-to-end, data-level protection and privacy. The IBM Hyper Protect Data Controller enables corporations to encrypt data, grant and revoke access to it, and maintain control of it – even as it moves off the system of record**.** The result: IBM LinuxONE III shared the highest security and reliability rankings in ITIC's 2021 poll with 95% of LinuxONE III enterprises detecting and shutting down data breaches "Immediately or within the first 10 minutes" of the attack.
- **IBM Power Systems** a 92% majority of IBM Power Systems customers reported their IT and security administrators were able to detect and thwart attacks "Immediately or within the first 10 minutes" of a breach. IBM's POWER9 scale-out systems have been out three years and the next generation Power10 servers are slated to ship in fall 2021. IBM continually refreshes and updates the line – placing particular emphasis on performance, support for mission critical workloads, support for advanced analytics, in-memory databases and embedded security. All of the Power Systems models are cloud ready. IBM Power Systems have security built in at all layers in the stack – processor, systems, firmware, OS and Hypervisor. With accelerated encryption built into the chip, data is protected in motion and at rest. IBM claims that its PowerVM hypervisor has no reported security vulnerabilities. POWER9 servers are also cloud-ready and include built-in PowerVM virtualization capabilities. The POWER9 scale-out servers are designed for integration into organizations' cloud and AI strategies. This provides the high performance and RAS capabilities required to support mission-critical workloads like IBM's Db2 and Oracle databases as well as SAP HANA. The Power10 is designed for energy efficiency and performance in a 7nm form factor. IBM estimated this will yield improvements of up to 3x greater processor energy efficiency, workload capacity, and container density than the POWER9. In addition, the upcoming Power10 servers will also incorporate a slew of advanced capabilities including: support for Multi-Petabyte Memory Clusters which will expand cloud capacity to support memory-intensive workloads. The Power10 will also feature hardware-enabled security capabilities like transparent memory encryption for end-to-end security. The IBM Power10 processor is

engineered to achieve significantly faster encryption performance with quadruple the number of AES encryption engines per core compared to the IBM POWER9 for today's most demanding standards and anticipated future cryptographic standards like quantum-safe cryptography and fully homomorphic encryption. It also brings new enhancements to container security.

Lenovo Security Survey Highlights

- **Lenovo ThinkSystem** servers achieved the best MTTD rates among all Intel x86-based servers with 92% of survey respondents stating their IT and security administrators detected and shut down attempted hacks and data breaches immediately or within the first 10 minutes of the penetration. This is no accident. In the seven years since Lenovo purchased IBM's x86-based server business and the decade since it acquired IBM's line of PCs and notebooks, Lenovo has made security a top priority. Consequently, Lenovo servers and desktops have gone from strength to strength as the company continually enhances and fortifies the performance, reliability and security of the servers and its desktop PCs and laptops. Lenovo's technical service and support is also first-rate. Lenovo's ThinkSystem servers showed continued reliability improvements – averaging their best uptime to date: 1.51 minutes of per server downtime due to hardware issues. Like IBM, Lenovo has constructed and executed an excellent and effective tactical and strategic security strategy. In 2018, Lenovo unveiled the ThinkShield end-to-end security technology for its PCs and laptops. The advanced ThinkShield technology has stood Lenovo PCs and servers in good stead over the past three years as security attacks surged. During the COVID-19 global pandemic as many organizations shifted to a remote workforce for workers and students alike, IT and security administrators have been hard pressed to keep pace with data breaches. Lenovo's ThinkShield security solution provides crucial support. ThinkShield for example, figures prominently in the ThinkSystem SE350. This model is Lenovo's first purpose-built edge server, targeted at the network edge to deliver optimal bandwidth, bolster security, and reduce downtime. The ThinkSystem SE350 is a small-footprint server. It measures 1.75 inches high, 8.1 inches wide and 14.9 inches deep and can be mounted on a wall, stacked on a shelf or installed in a rack. ThinkSystem SE350 is also designed for high-performance server. It's based on Intel's Xeon-D processor comes equipped with 256GB of RAM and 16TB of internal solid-state storage. ThinkSystem SE350 has enhanced physical security features like a locking bezel, intrusion detection, tamper detection, and encrypted storage. It boasts zero-touch deployment software. Lenovo's overarching strategy melds innovation with reliable, flexible, and secure data center systems. This is a savvy move that also has far reaching ramifications for Lenovo's servers, networks and ultimately its corporate customers. Human error is by far the biggest cause of server downtime. End users are traditionally among the weakest link in the overarching security chain – particularly during the COVID-19 global pandemic which saw a significant percentage of end users teleworking and students engaged in remote learning. It makes sense for Lenovo to lock down the desktop as well as the servers. Lenovo enforces rigorous security standards, policies and procedures at its manufacturing facilities and global supply chain. Lenovo's Quality Engineers retain the right to audit the company's Trusted Suppliers at any time, giving the company even further control and insight into the security of its devices' components. ThinkShield also delivers design level security. This includes secure BIOS and firmware, as well as privacy screens and laptop camera shutters into its devices to help minimize "visual hacking" when mobile users are in public places. ThinkShield is designed to protect users' identities and credentials, offering FIDO-certified authenticators and integration with Intel Authenticate (offering up to 7 authentication factors). ThinkShield also features BIOS-based Smart USB protection, which functions by configuring USB ports to only respond to keyboards and pointing devices. Lenovo also emphasizes that its open server, storage, networking and system management platforms seamlessly integrate with existing and legacy environments. In first person interviews with ITIC analysts, Lenovo customers cited the ease of deployment and ease of integration and backwards compatibility as contributing to the underlying reliability and stability of the ThinkSystem platform. Lenovo users also lauded the vendor's after-market service and support. Lenovo's system design supports mission-critical databases, enterprise applications, big data analytics, and cloud and virtualized environments. Both these systems incorporate numerous fault-tolerant and high-availability features into a high-density, rack-optimized lid-less package that minimizes the space needed to support "massive network computing operations" and simplify servicing, as the system never needs to be removed from the rack. In August 2020, Lenovo debuted several new models of its ThinkSystem single-socket servers based on Advanced Micro Devices AMD EPYC 702 series processors. The new additions to Lenovo's server portfolio are designed specifically to handle customers' evolving, data-intensive workloads such as video security, software-defined storage and network intelligence. They also support virtualized and network edge environments – where security is paramount. The result is a solution that packs power along with efficiency for customers who place a premium on balancing throughput and security with easy scalability. Lenovo claims the two new ThinkSystem servers "provide the performance of a dual-socket server at the cost of a single-socket" and have the potential to lower customers' software licensing costs by up to 73% and cut TCO by up to 46%.

Cisco UCS Security Survey Highlights

- **Cisco's Unified Computing System (UCS)** continues to score well and it maintained the 2.3 minutes of per server downtime that it first achieved in ITIC's 2020 Global Server Hardware, Server OS Mid-Year Update Survey. From January through mid-June 2021, Cisco's servers held steady at 2.3 minutes of per server downtime. This is no mean feat considering that many Cisco UCS servers are positioned at the network edge which is on the front line of security attacks. Despite this, 87% of Cisco UCS survey respondents said they were able to detect, isolate and shut down security hacks immediately or within the first 10 minutes. Cisco UCS survey respondents also reported that the servers experienced seven (7) successful security hacks each over the last 18 months. In response to the increase in data breaches, Cisco began publishing the Cisco UCS Hardening Guide. The document is available for free download. It contains detailed information to help users secure Cisco UCS platform devices to improve network security. Structured around the three planes by which the functions of a network device are categorized, this document provides an overview of each Cisco UCS Software feature and references related documentation. Additionally, Cisco introduced a number of management and performance upgrades aimed at improving TCO and accelerating installation and deployment. Cisco claims its UCS will allow an 86% reduction in cabling, and allow provisioning in a matter of minutes (rather than days or weeks), while reducing capital expenses by more than 40%. Manufacturers assure users of 100% compatibility between and among components. And load balancing is a non-issue.

HPE Security Survey Highlights

- **HPE's Superdome** line of servers (including the Integrity and Flex models) also exhibit high reliability of five and six nines for a 92% majority of its customers. And 89% of HPE survey respondents said their firms discovered and shut down security breaches "Immediately or within the first 10 minutes." The ITIC survey data shows that HPE Superdome servers each experienced three (3) successful security hacks within the last 18 months. This puts the HPE hardware platforms in the top five most secure systems. The Superdome portfolio also benefits from the inherently strong stability of the HPE hardware. HPE has made security, feature/performance innovation and after-market technical service and support, its top priorities. All of this is critical in the increasingly insecure, complex and interconnected Digital Age. HPE is well entrenched in corporate enterprises from SMBs to the largest multinational businesses. The HPE Superdome Flex Server features RAS capabilities and end-to-end security to protect vital workloads. The HPE Superdome Flex Server, for example delivers scalability of up to 32 sockets. This is 2.3x the scalability of prior generation servers. It also features an In-memory design and memory capacity of 768GB - 48 TB in a single platform. HPE Superdome Flex Server has a modular design that scales flexibly from 4- to 32-sockets in 4-socket increments. HPE also says the Superdome Flex server has a more cost efficient entry point for mission-critical workloads at 4 sockets, it delivers up to 45% lower acquisition cost compared to previous models. HPE also emphasizes reliability claiming that the Superdome Flex Server embedded RAS capabilities deliver five nines - 99.999% - of single-system availability. HPE also asserts that the Superdome Flex server reduces human error via its predictive fault handling Error Analysis Engine. Security and human error are two issues that are closely linked and undermine security and reliability. This engine predicts hardware faults and initiates self-repair with no need for human intervention or "operator assistance." It contains errors at the firmware level, including memory errors, before any interruption can occur at the Operating System layer with HPE's "Firmware First" approach. HPE also provides continuity for Linux workloads with its HPE Serviceguard for Linux (SGLX) high availability and disaster recovery clustering solution. This enables businesses to safeguard their servers running Linux against a multitude of infrastructure and application faults across physical or virtual environments over any distance.

Huawei Security Survey Highlights

- Over the last five years Huawei, headquartered in Shenzhen, China has emerged as one of the top five server hardware vendors worldwide with its high end KunLun mission critical server and its general purpose FusionServer x 86-based servers. Based on ITIC's 2021 Global Server Hardware, Server OS Reliability Survey and the ITIC 2021 Global Server Hardware Security Survey, the Huawei KunLun and Fusion Servers are also among the top three most reliable and secure hardware platforms. A 91% majority of Huawei survey respondents noted their IT and security administrators detected and shut down attempted breaches "Immediately or in under 10 minutes." Huawei survey respondents indicated that the KunLun and Fusion servers each experienced 1.5 hacks during the last 18 months. Since 2015, Huawei fortified the advances features, inherent security and overall performance of its servers. To successfully compete with rivals including Cisco, Fujitsu, HPE, IBM, Inspur, Lenovo and others, Huawei's server family includes general purpose rack and blade servers to mission critical hardware to address high performance computing (HPC). Huawei has also imbued its servers with advanced capabilities to support emerging compute intensive applications like AI, Big Data Analytics, Deep Learning and Machine Learning. Huawei is emphasizing security via best practices documents on "How to Build a Proactive Defense System?" via its HiSec solution which enables more intelligent threat detection, threat response, security operations and maintenance. Huawei says HiSec improves the threat prevention capabilities of enterprise networks and the telecom infrastructure, thus increasing security O&M efficiency and reducing O&M costs. In addition, Huawei offers a number of new security offerings for its various server solutions in the data center, the cloud and the network.

Conclusions

Security is the number one issue that negatively undermines the reliability and availability of server hardware, server operating systems and business critical applications. All organizations should make security a priority and work closely with their vendors to mitigate security risks to an acceptable level.

Every added second and minute of server downtime and application unavailability negatively impacts business operations, employee productivity and revenue.

ITIC's 2021 Global Server Hardware and Server OS Reliability Survey findings indicate that the IBM Z mainframe, IBM Power Systems, followed closely by Lenovo ThinkSystem, Huawei

KunLun and HPE Integrity Superdome servers continue to solidify and improve their status as the most reliable server hardware offerings. The IBM Z enterprise platform stands alone in delivering fault tolerant reliability of six and seven nines – 99.9999% and 99.99999% reliability for upwards of 93% of its enterprise users. Excluding super computers and high availability (HA) hardware no server platforms come close to achieving the Z's level of reliability, availability and near-flawless uptime and security.

Nine-in-10 survey respondents affirmed that the IBM Power Systems and Lenovo ThinkSystem solutions both registered five and even the vaunted six nines - 99.999% and 99.9999% - of reliability and availability. The IBM Power Systems and Lenovo ThinkSystem platforms are up to 30x more reliable and as much as 36x more cost effective and economical than the worst performing unbranded White box servers.

In another notable achievement, IBM and Lenovo captured first or second place rankings in every reliability and availability category or, they tied for first or second place in every uptime, security or manageability metric in the survey.

Reliability is fluid, not static. No server, no component part – hard drive, memory or CPU; operating system; application, device or connectivity mechanism is immune from inherent problems or failures.

Servers are the bedrock upon which the entire network infrastructure and extended network ecosystem rests. When servers fail, data access is denied. Business stops. Productivity ceases. Revenue suffers. Some 88% of all corporations now require a minimum 99.99% reliability for their firms' server hardware, operating systems and main line-of-business applications to ensure productivity and deliver uninterrupted data access. High reliability and availability also safeguards the corporation's daily operations, data assets and intellectual property (IP), employees' personnel information, business processes and revenue stream.

In 2021 and beyond security, human error and end users constitute the biggest threats that can undermine the reliability and availability of servers, operating systems and applications.

No one knows how long the COVID-19 global pandemic will last. And even when the pandemic is ruled officially over, its negative effects and impact will likely persist for years – especially with regards to security and data breach threats.

This is the new normal: organized hackers are here to stay. They will continue to use this pandemic to exploit vulnerabilities. Hackers will continue to seize every opportunity to exfiltrate corporate and employee data assets for profit.

Server reliability, uninterrupted data and application access and security are always imperative – but especially so in the COVID-19 era of teleworking and remote learning. Every added second and minute of server downtime and application unavailability negatively impacts business operations, employee productivity and revenue.

A significant portion of enterprise servers and applications now reside in virtualized cloud environments and at the network edge. Since the pandemic began over 18 months ago, many businesses transitioned their employees to teleworking; schools and universities also adopted remote learning. This places greater pressure on organizations and over-extended IT and security administrators to ensure uptime and availability of all data assets.

Security is extremely crucial. Vendors must continue to fortify embedded server security; quickly supply fixes and patches when flaws are found and work with customers to provide prescriptive guidance. Corporate enterprises must also assume responsibility to ensure the reliability and security of the entire server and network infrastructure and key business applications in datacenters and the cloud. It's critical that companies implement and enforce strong security policies and procedures for **all employees,** particularly teleworkers and students. Reliability and security are core foundational elements of the network infrastructure. Both are necessary to ensure uninterrupted daily operations, secure data access and to protecting the revenue stream.

ITIC's 2021 Global Server Hardware, Server OS Security Survey emphasizes the need for **all** organizations, irrespective of size and vertical industry to proactively and continually strive to identify and thwart the growing array of increasingly sophisticated and targeted cyber attacks.

That means implementing all appropriate security measures. Enacting and enforcing strong computer security policies and procedures for **all company employees** – from C-suite executives down to company contract workers and interns is imperative. Businesses must allocate adequate budgets for purchasing security products and devote the necessary time and appropriate internal and external third party resources to provide end users and IT administrators and security professionals with the security tools and security training.

There is no such thing as 100% foolproof security. However, multi-layer security defenses, bolstered by vulnerability testing and security awareness training can thwart the number of data breaches and Ransomware hacks and mitigate risk to an acceptable level.

Mission critical systems from Cisco, HPE and Huawei also performed extremely well and did not experience any declines in reliability in the past 18 months since the onset of the COVID-19 global pandemic. The Cisco, HPE and Huawei servers have achieved near reliability parity with IBM and Lenovo based on the inherent robustness of the core hardware.

Cisco's UCS servers maintained the reliability gains in ITIC's latest 2021 Global Server Hardware, Server OS Reliability Survey Mid-Year Update. Since 2019 Cisco UCS server shops reported downtime had declined from just over four (4.1) minutes in ITIC's previous reliability survey to just over two (2.3) minutes per server/per annum due to hardware flaws. This is critical. A significant portion of Cisco's UCS servers are deployed at the network edge - long considered to be among the most vulnerable points of the ecosystem.

No vendor can rest on its laurels. Competition in the worldwide global server hardware market is intense. It is, and will remain a buyer's market. While many companies, particularly SMBs, make their purchasing decisions based on price, a significant portion of enterprises choose to purchase more robust hardware, equipped with embedded security, advanced management, AI and big data analytics functionality.

The survey data shows that corporate enterprises place an extremely high value on after-market vendor technical service and support. Corporations require vendors to act quickly if and when problems arise. Vendors should provide customers with realistic recommendations and prescriptive guidance for system configurations and product lifecycles to achieve and maintain optimal performance and availability.

As always, ITIC maintains that vendors also bear the responsibility to deliver patches, fixes and updates in a timely manner and to inform customers to the best of their ability regarding any known incompatibility issues that may potentially impact performance. Vendors should also be honest with customers and notify them of problems or delays in delivering replacement parts.

Recommendations

No server platform, server OS or business application will provide foolproof security. However, IBM, Lenovo, Huawei, HPE and Cisco which are among the most reliable server platforms also provide the greatest levels of inherent security. This enables customers to achieve the greatest economies of scale and safeguard their sensitive IP and data assets. Security is a 50/50 proposition. While vendors must deliver robust security, corporations are responsible for maintaining the reliability of their server and overarching network infrastructure. ITIC strongly advise businesses to:

- **Take Inventory.** Know what's on your network. This means cataloguing ***all*** servers, crucial main line-of-business applications; network devices (firewalls, routers) across the entire network ecosystem including the datacenter, remote offices, public, private and hybrid clouds, IoT devices and the network edge.
- **Right size server hardware**. Server hardware must be robust enough to accommodate current workloads as well as anticipated increased workloads and larger applications.

- **Regularly replace, retrofit and refresh server hardware.** This means keeping up-to-date with the necessary patches, updates and security fixes ***as needed*** to maintain system health and achieve peak system performance.
- **Update Software.** Whenever possible, never stay more than two revisions behind on server operating systems and key server-based applications.
- **Implement strong security policies and procedures.** It is imperative that companies of all sizes and across all vertical market segments construct corporate wide security policies and procedures. Disseminate them via hard copy and Email to all employees. The computer security policies should be an integral part of the overall corporate guidelines and should contain specific provisions and penalties for first, second and third offenses. Companies are also advised to have all employees attend mandatory computer security training, similar to sexual harassment training.
- **Closely Monitor Service Level Agreements (SLAs).** Pay close attention to SLA contracts to ensure that your firm's hardware, software vendors and cloud vendors meet or exceed the terms of SLAs to deliver agreed upon reliability levels.
- **Conduct security vulnerability testing.** Given the continuing spike in all types of security hacks and data breaches e.g., Ransomware, Phishing attacks and CEO Fraud to name a few, all corporate enterprises should conduct vulnerability testing at least once a year and as-needed. ITIC recommends that corporations work with independent third party experts.
- **Construct a Governance and Remediation plan.** Have a remediation and governance plan in place in the event your firm is successfully hacked. Designate a hierarchy of who's in charge in the event of a data breach or network outage. The Governance and Remediation plan should also assign and designate specific tasks for specific groups and individuals. Make sure the plan also includes the pertinent contact information for all vendors and third party service providers.
- **Train and certify Security and IT Administrators.** Ensure that Security and IT professionals receive adequate training and have the necessary security certifications.
- **Train End users.** Ensure that end users as well as contract workers and temporary employees receive adequate security awareness training on the latest Email and Phishing scams and Ransomware threats.

Methodology

ITIC's *2021 Global Server Hardware Security Reliability Survey*, polled C-level executives and IT managers at over one thousand corporations worldwide from January 2021 through mid-June 2021. The independent Web-based survey included multiple choice questions and one Essay question. To maintain objectivity, ITIC accepted no vendor sponsorship. No survey participants received any remuneration. ITIC analysts also conducted two dozen first person customer interviews to obtain valuable anecdotal data and gain deeper insights and contextual knowledge of the impact and implications of security vulnerabilities and data breaches on the reliability of the corporate server and network infrastructure. Respondents included C-suite executives, IT and security administrators and end users. ITIC employed authentication and tracking mechanisms to prevent tampering and to prohibit multiple responses by the same parties.

Survey Demographics

ITIC polled 1,100 companies of all sizes and across 28 vertical markets for the survey. Corporations of all sizes were well represented. Respondents came from companies ranging from small and medium businesses (SMBs) with fewer than 50 workers, to multinational enterprises with over 100,000 employees.

All market sectors were equally represented: SMBs with one-to-100 employees accounted for 24% of the respondents. Small and medium enterprises (SMEs) with 101-to-1,000 workers represented 28% of the participants. The remaining 43% of respondents came from large enterprises with 1,001 to over 100,000 employees. Survey respondents hailed from 49 different vertical markets. Approximately 61% of respondents hailed from North America; 39% were international customers who hailed from 22 countries throughout Europe, Asia, Australia, New Zealand, Central/South America and Africa.

Appendices

This section provides links to the various ITIC statistics and surveys cited in this Report.

ITIC Website and links to survey data and blog posts:

https://itic-corp.com/blog/2019/11/ibm-lenovo-hpe-and-huawei-servers-maintain-top-reliability-rankings-cisco-makes-big-gains-ibm-lenovo-hardware-up-to-24x-more-reliable-28x-more-economical-vs-least-reliable-white-box-servers/

https://itic-corp.com/blog/2019/11/1678/

https://itic-corp.com/blog/2019/08/itic-poll-human-error-and-security-are-top-issues-negatively-impacting-reliability/

https://itic-corp.com/blog/2019/08/itic-2019-server-reliability-mid-year-update-ibm-z-ibm-power-lenovo-system-x-hpe-integrity-superdome-huawei-kunlun-deliver-highest-uptime/

http://itic-corp.com/blog/2017/07/ibm-z14-mainframe-advances-security-reliability-processing-power/

http://itic-corp.com/blog/2017/06/ibm-lenovo-servers-deliver-top-reliability-cisco-ucs-hpe-integrity-gain/