quark lepton

WHITEPAPER / MAY 17, 2017 / QL217575

IBM i on Power Systems Enables Enterprise Resilience for Business-Critical Systems

Sponsored by IBM

Market Situation

As the Big Data revolution changes the way businesses operate, growing emphasis is placed on robust and reliable infrastructures. High performance analytics, seamless transactions, and impenetrable security are no longer desires, but requirements for organizations that wish to thrive. While many enterprises recognize the importance of business resilience, they often do not quantify its value. Maintaining security and availability of business-critical systems is crucial for business continuity, and the effects of failing to do so may be prolonged and catastrophic.

This paper quantifies the financial impacts of downtime, and the potential risk exposure to disastrous system outages, for use of three core business information technology (IT) platforms: IBM i operating system with DB2 on Power Systems; Microsoft Windows Server with SQL Server on Intel x86 servers; and Oracle Exadata Database Machine.

For these three server platforms, the consequences of both planned and unplanned downtime on two types of enterprise applications, and the sharing of data between them, has been calculated for: 1) business-critical software, and 2) analytics and reporting, cloud and mobile connectivity, and social media applications.

The IBM i operating system—version 7.3 was released in April 2016—has a three-decade legacy and a large community of dedicated users who routinely describe IBM i as robust, secure, and reliable. More than 3,000 solutions are available for the platform. These are supported by over 2,500 independent software vendors (ISVs) and a certified network of IBM Business Partners, including leading suppliers of enterprise resource planning (ERP) systems as well as industry-specific core systems. IBM i users include some of the world's largest corporations representing a wide variety of industries, such as manufacturing, financial services, distribution, insurance, retail, and healthcare. The IBM i ecosystem extends to user groups, online communities, service providers, and consultants worldwide.

IBM i is a tightly integrated, highly securable, automated operating environment. DB2 for i, which is integrated into the IBM i operating system with automated workload balancing and advanced data management utilities, improves efficiency and streamlines operations. According to the *2017 IBM i Marketplace Survey* conducted by HelpSystems, 94.6 percent of users believe their IBM i servers have a better return on investment (ROI) than other servers.

Windows Server 2016 and SQL Server 2016, released in October and June 2016 respectively, have been deployed to support business-critical software for enterprises. These installations, however, tend to be smaller and less availability- and recovery-sensitive than IBM i equivalents, typically experiencing longer and more frequent outages. According to Information Technology Intelligence Consulting's (ITIC) *2016 Global Server Hardware, Server OS Reliability Report*, IBM Power Systems typically average 10.2 minutes of unplanned downtime per server per year, whereas x86 systems average from 10.8 to 18 minutes of unplanned downtime per server per year.

Windows Server 2016 integrates new and/or enhanced features, such as Windows Defender, management and automation tools, software defined networking, and Windows Server Containers.

Exadata X6 Database Machine, released in April 2016, has been promoted by Oracle as a dedicated, high performing, highly available engineered system for the Oracle Database. Exadata is a tested, pre-integrated architecture running specialized Oracle Database software on separate compute and storage processing hardware, equipped with all-flash or hybrid storage arrays, and InfiniBand networking.

Higher risks associated with the Exadata platform include the highly specialized database architecture, as well as the limited selection of Oracle software and standard hardware supported. Database administrators (DBAs) are required to have a specialized Exadata skillset to support the system's unique Oracle Database software execution between compute nodes and storage nodes. Because of these factors, companies migrating to an Exadata system face significant administrative challenges, regardless of whether they are migrating an existing Oracle Database or another database system.

Results for the installation comparisons are summarized as follows:

- **Costs of downtime** for all industries covered for planned and unplanned outages of less than four hours over three years averaged 8.2 times higher for use of Windows Server on x86 platforms and 3.4 times higher for use of Oracle Exadata than for use of IBM i on Power Systems. For supply chain companies, cost of downtime for use of IBM i averaged 87 and 70 percent less than Windows and Oracle, respectively. For financial services companies, costs for use of IBM i averaged 90 percent less than Windows, and 73 percent less than Oracle. (Figure 1)

  Lower IBM i costs of downtime represented average three-year business savings of $15.2 million compared to use of Windows Server, and $5.1 million compared to Oracle Exadata.

- **Risk exposure** for enterprises is an aggregate of numerous factors, including potential downtime caused by conflicts or failures in IT infrastructure and business applications. Risk exposure can also be influenced by other elements such as support responsiveness and/or effectiveness of various vendors. The potential costs of severe unplanned outages of more than four hours over three years averaged

65 and 24 times higher for the use of Windows Server and Oracle Exadata respectively than for use of IBM i. When such unplanned outages occur, core business processes can be disrupted, causing significant financial impact.

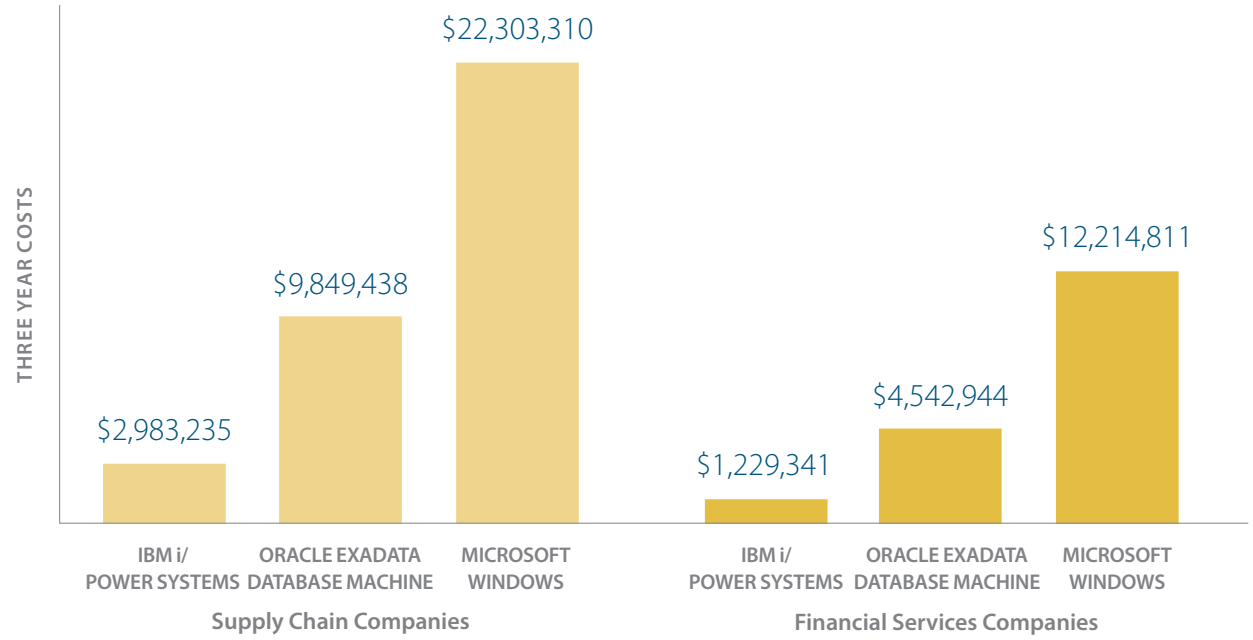
These differences result in $1.4 million in lower risk exposure for use of IBM i compared to Windows Server, and $483,000 less than for Oracle Exadata (Figure 2).

Downtime and Risk

In an interconnected world of global supply chains and instantaneous transactions, the impact of unplanned downtime has become more detrimental than ever. Although companies are experiencing shorter durations of planned and unplanned downtime, costs per minute of downtime have generally increased. According to the 2016 IHS Markit survey, *The Cost of Server, Application and Network Downtime Survey and Calculator*, downtime costs North American businesses $700 billion annually, mostly in the form of lost employee productivity. When severe unplanned outages occur, financial impacts increases in a manner that can be exponential, not linear, with time. Effects of downtime will reverberate through interconnected IT ecosystems, such as e-commerce and mobile payments.

Modern businesses are becoming more reliant on critical applications and the infrastructure that supports these applications to facilitate business. For industries that rely on advanced systems to process transactions, produce goods, and/or distribute materials, such as financial services, retail, and supply chains, a delay in or inability to process key transactions can result in significant costs.

FIGURE 1: Average Three-year Cost of Downtime for Planned and Unplanned Outages of Less Than Four Hours

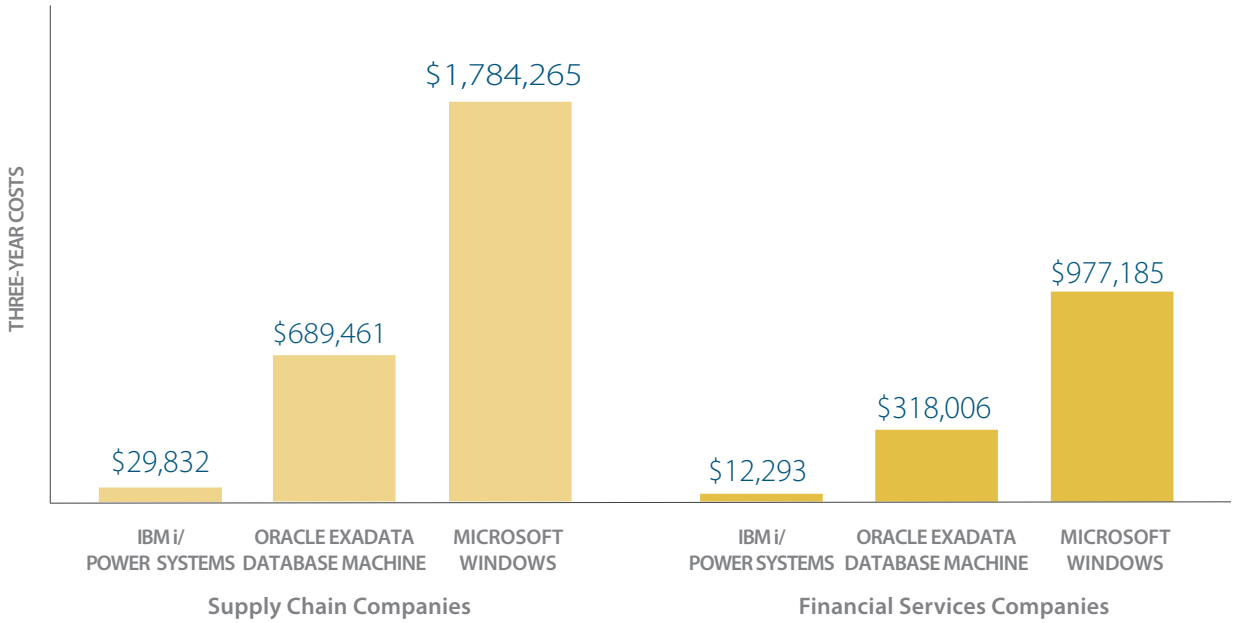


Banks and other financial services firms increasingly support customer transactions through web and mobile banking. As use of mobile banking rises, so do the expectations customers place on secure, reliable connections for managing their financial and digital life. According to the Bank of America's *2016 Trends in Consumer Mobility Report*, 54 percent of respondents actively use mobile banking, and 62 percent prefer mobile or online banking over traditional banking. These customers not only demand unrestricted, instantaneous access to their accounts, but they also expect online systems to be fully secured. Even minor downtime causing loss of access or a transaction delay can result in significant customer dissatisfaction. Security breaches compromising personal information will not only lead to customer anger, but also to significant recovery costs and possible regulatory fines.

For **large global supply chains**, downtime affects profitability in various ways. Aside from lost revenue, unplanned downtime can negatively impact employee productivity and morale, as well as cause brand damage. Loss of employee and customer confidence can affect supply chains for the long term. Ripple effects can be experienced and time zone differences can exacerbate inefficiencies. According to Allianz's *Global Claims Review 2015: Business Interruption in Focus*, "the greater interconnectivity of the global economy is manifesting itself in increasingly more complex production processes with higher economic values. The end result is more severe business interruption implications."

In the **retail industry**, downtime results in competitor advantage, and erodes customer loyalty. E-commerce customers expect 24/7 service, and negative experiences may affect their impressions long term. Retailers with a large online presence may also experience decreased *organic search* visibility when search engines lower a website's ranking due to downtime. According to Pew Research Center's *December 2016 Online Shopping and E-Commerce* survey, 80 percent of Americans shop online, and 15 percent engage in e-commerce on a weekly basis. The growth in the number of e-commerce shoppers

FIGURE 2: Average Three-year Financial Risk Exposure to Severe Unplanned Outages



relying online ratings and reviews shifts attention to vendor reliability. Downtime causing inconvenience, such as fulfillment delays, will likely be documented and may negatively affect sales.

Mobile users in 2017 are projected to account for over half of digital commerce in mature economies. In retail as in banking, mobile users are proving sensitive to slow responsiveness of online sites, not just downtime. Mobile shoppers, for example, tend to lose interest if they are unable to access a website within a second. Companies have reported that even a half second delay can result in a 10 percent difference in sales.

The **cloud technologies industry**, according to MarketsandMarkets' *Top 10 Cloud Technology Market* report of February 2017, is projected to grow its Hybrid Cloud and Cloud Storage segments at a compound annual growth rate (CAGR) of 22.5 and 25.8 percent respectively, and its Disaster Recovery and Integrated Platform as a Service segments (DRaaS and IPaaS) at 45.9 and 41.5 percent CAGR, respectively from 2016 to 2021. The strongest growth and largest segment size of this study's cloud technologies categories, DRaaS with projected 2021 revenues of $11 billion, reflects the growing use of cloud technologies to provide IT disaster recovery resources and safeguards.

However, the attractiveness and rapid growth of all cloud sectors continues to be checked by customer concerns about security risks associated with the cloud. Data center security firm, Netwrix Research Lab, reported in its *2016 Cloud Security Report* that of the 660 global companies surveyed, 448 reported they were not using cloud solutions, while 56 percent of these cited insufficient security mechanisms as the primary reason they had not yet adopted cloud solutions.

It becomes apparent that the best course of action for maintaining business continuity may be to adopt and leverage new technologies without compromising security and preventative risk measures that minimize downtime. These new technologies are coming out of a world where open source and instant access to non-proprietary innovations are today's reality, and IT leadership must learn how to balance new technologies with modernizing existing foundations. A system with a proven history of meeting customer's availability and security requirements, without sacrificing flexibility and forward compatibility, is best suited to meet these challenges.

SECURITY AND MALWARE

Security breaches remain a ubiquitous threat due to the 24/7/365 reliance our society places on access to essential information technologies. For most enterprises, especially those handling sensitive customer information or confidential data, the threat is made more dangerous by our digital culture's ever expanding channels of access and potential exposure. In an environment of complex electronic transactions involving sensitive information, it is increasingly important for organizations to implement a robust infrastructure with security policies that minimize the risks of intrusion.

Even businesses across industries known for implementing highly secure systems have experienced a growth in the number of data breaches and cyberattacks. In addition to point of sale (POS) system intrusions and web application attacks, which have made up the majority of recent years' data compromises, unchecked interoperability links within highly interconnected global systems have

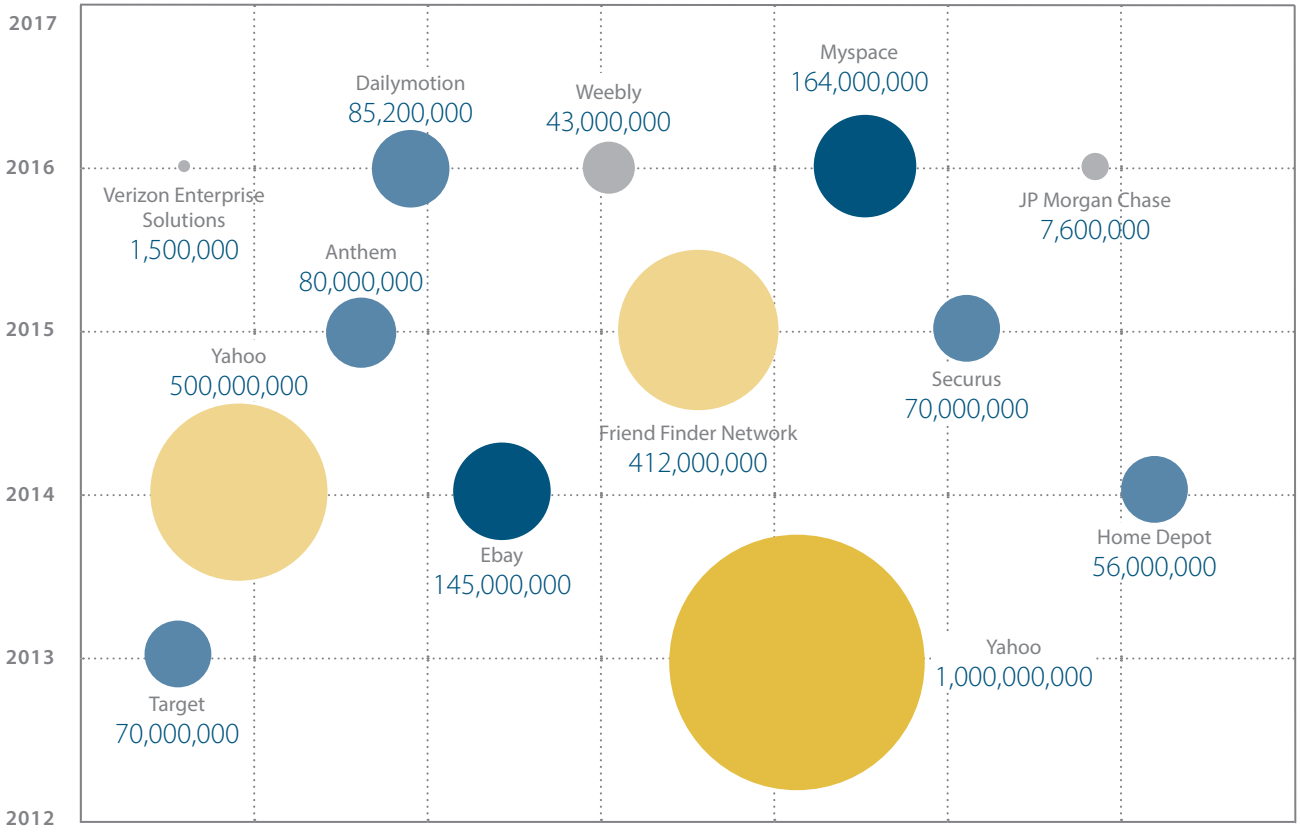
proven to be vulnerable as well. In cases such as these that involve financial services systems that span cultures, languages, and currency exchanges, the impact of security and privacy breaches in one location can result in harmful effects being triggered in systems a world away.

In 2016, the Identity Theft Resource Center (ITRC) tracked 1,093 data breaches, which exposed more than 36.6 million records. Hundreds of thousands to hundreds of millions of customer records were exposed. Not only was sensitive information revealed, but financial impacts were also substantial. Figure 3 depicts some notable breaches that have occurred in recent years.

Ponemon Institute's *2016 Cost of Data Breach* study indicates that, in the United States, the average cost per compromised record is $221, and the average total cost of a response to a data breach is $4 million. Costs can escalate dramatically according to the severity of the breach.

In September 2016, for example, Yahoo disclosed a 2014 intrusion that compromised the details of 500 million user accounts. Shortly after, in December 2016, the company disclosed another breach that occurred in 2013 compromising one billion accounts. This breach was only discovered when law enforcement became involved. The Securities and Exchange Commission (SEC) is currently investigating whether Yahoo disclosed these breaches in a timely manner. Yahoo can face significant fines if the SEC findings are unfavorable. These breach disclosures not only led to falling stock prices and customer

FIGURE 3: Number of Records Compromised in Recent Data Breaches



dissatisfaction, but negatively impacted its acquisition by Verizon as well . Yahoo is also facing numerous lawsuits as a result of these breaches.

IBM i on Power Systems has built a reputation as a highly integrated and secure system. Malware infection and security incidents are rare for IBM i users, due to object-based architecture and sophisticated tools for monitoring and logging. Organizations that configure systems for maximum security and follow best practices as recommended by IBM enjoy high levels of protection.

IBM i's unique object-based architecture provides isolation and malware resistance for business-critical systems. Objects, such as data and code, are encapsulated in a container that dictates what it can do, and who can access it. This architecture resists malware by scrutinizing containers to ensure the objects inside are not disguised as something else. This is done constantly and automatically, providing real-time protection against viruses masquerading as files. By placing strict controls on data as well as system code, the use of containers makes it extremely difficult for unauthorized instructions to execute. Intrusion detection compliments the object-based architecture by gathering information on unauthorized access attempts made over TCP/IP.

Additional IBM i security features include the authority collection, which allows administrators to capture and analyze data to better secure objects in the system. Cryptographic hardware in Power Systems adds cryptographic processing capabilities as well as encryption and digital signatures.

The security features offered by IBM i on Power Systems enable the platform to be highly securable, as demonstrated by the statistics collected by the National Institute of Standards and Technology (NIST) National Vulnerability Database (NVD). Table 1 summarizes vulnerability data reported for IBM i, Red Hat Enterprise Linux (RHEL), SUSE Linux Enterprise Server (SLES), Oracle Linux (OL), and the Windows Server operating systems.

TABLE 1: Comparative Operating System Vulnerability Data—January 2008 through March 2017

CVSS SEVERITY LEVEL	Windows Server			Red Hat Enterprise Linux Server (RHEL)		SUSE Linux Enterprise Server (SLES)		Oracle Linux (OL)		IBM i			
Version Release date	*2008 Feb '08*	*2012 Oct '12*	*2016 Oct '16*	*6 Nov '10*	*7 Apr '14*	*11 Mar '09*	*12 Oct '14*	*6 Feb '11*	*7 Jul '14*	*6.1 Apr '08*	*7.1 Apr '10*	*7.2 May '14*	*7.3 Apr '16*
Critical	2	4	1	11	9	1	2	12	10	0	0	0	0
High	725	296	66	76	50	10	34	51	65	1	1	0	0
Medium	257	117	28	53	58	24	39	26	58	0	0	0	0
Low	47	59	3	4	18	2	6	1	13	0	0	0	0
TOTAL VULNERABILITIES	1,031	476	98	144	135	37	81	90	146	1	1	0	0

DATA SOURCE: NIST Computer Security Division, National Vulnerability Database, CVSS Metrics Versions 2 & 3

Supply Chain

Supply chains are vulnerable to a unique set of risks. Nevertheless, when it comes to their disruption, most think of major interruptions caused by extreme weather and natural disasters. However, according to the Business Continuity Institute's *2016 Supply Chain Resilience Report*, unplanned IT or telecom outages were the most common cause of supply chain disruption (Figure 4). Few supply chain or risk management executives would be penalized for failing to predict an unexpected extreme weather event. But potential exposure to IT-related disruptions is a great deal easier to measure, and to mitigate.

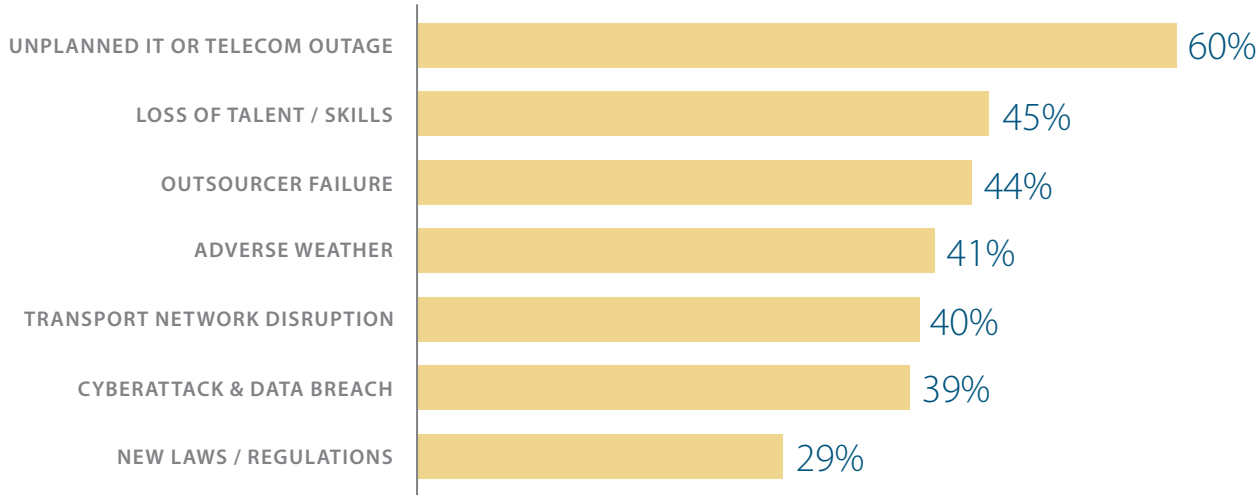
INDUSTRY TRENDS

Although modern enterprise systems integrate a broad range of traditional transactional processes, e-business has encouraged fundamental changes. Traditional ERP systems were used to internally manage a company's value chain, but today's ERP systems span markets and industries, assisting the global flow of information, labor, and goods. These systems are more interconnected than ever before, and their uninterrupted operation remains crucial.

In addition to enhancing ERP systems, to further boost competitive advantage, many businesses are integrating cloud, analytics, mobile, and social (CAMS) technologies. Businesses continue to digitize and reinvent their supply chains as digital supply networks, consolidating flow of materials, goods, labor, information, and finance.

Supply chains companies are building upon existing cost saving methods such as lean manufacturing and the application of agile principles to operations management. More companies are leveraging real-time analytics to make lightning-fast decisions for handling unexpected events. In addition, the adoption of e-commerce within supply chains is fostering the faster flow of materials and components. These strategies—contributing to the competitive advantages of successful modern supply chains—are extremely dependent on continuous uptime.

FIGURE 4: Most Common Causes of Supply Chain Disruptions—Percentage of Organizations Reporting



SOURCE: 2016 Business Continuity Institute (BCI) Supply Chain Resilience Report

ERP systems that interface with real-time analytics have become the norm. Most distributors and manufacturers that contributed to this paper, for example, had deployed mobile and/or cloud applications to support field sales and service teams. Companies had also deployed cloud solutions (e.g., for supplier interaction, workforce management, and specialized ERP functions) to supplement their principal application portfolios, and to support development and test activities.

In virtually all cases, these applications interface with business-critical software, either directly or (via data warehouses) indirectly. The result is that these systems have become the backbone of the interdependent multichannel, multimedia complexes through which companies compete.

Driven by industry trends to achieve higher efficiency, supply chains operations continue to evolve through adopting innovative technology, but this can also open business systems to new vulnerabilities. For leading supply chains with global operations and unforgiving schedules, downtime becomes more disruptive than ever. Industry trends impacting supply chains include:

- **Globalization.** Most large manufacturers, retailers, and distributors operate internationally, or employ foreign suppliers, channel partners, or both. Certain processes occurring around the clock—including procurement, logistics, and, in many cases, sales, order processing, and customer service—continue to be sensitive to downtime. The impact of disruptions tends to be greater for global supply chains operating in different time zones, as delays can cascade, affecting other processes, and extending to customers and trading partners.

- **Supply chain strategies.** Operation of just-in-time, lean, and real-time delivery models has further increased risk exposure. Modern retail customers are omni-channel shoppers, and there is higher supply chain transparency as warehouses become showrooms and inventories become visible through websites and networked applications. Compared to a traditional fulfillment model, outages are more apparent and inconvenience is highlighted. As more retail chains digitize, dissatisfied customers will inevitably lead to lost sales and turnover.

- **Cycle time decline.** Automotive parts suppliers, for example, receive continuous demand signals from their customers, causing them to recalibrate plans and forecasts, and initiate procurement, production, and logistics actions in real-time. A delay in delivering components to a plant, for example, might cause finished product deadlines to slip. This may, in turn, impact transportation schedules and warehouse operations, resulting in further delays, and causing disruption to spread. Disruptions also tend to raise error rates across most, if not all, supply chain stages.

  Additional pressures have been added by moves toward same-day and weekend delivery. In the United States, for example, Amazon.com has driven this trend, and competitors have followed. Over 40 million customers now expect free two-day shipping for their purchases. Amazon Prime Now is further pushing the fast delivery trend, offering free two-hour delivery for members in select regions.

- **New technologies.** Perhaps even more than the adoption of radio-frequency identification (RFID), the impact of additive manufacturing, commonly known as 3D-printing, may be greater. Innovative applications for this technology are rapidly being developed. Early adopters in such industries as aerospace, architecture, commercial manufacturing (i.e., automotive, consumer products, and

electronics), medicine, and life science have reported that significant savings in design times and costs are already occurring. Things that could only be imagined previously, can be made in minutes. 3D-printing has the potential to alter the supply chain by reducing manufacturing lead times to minutes rather than days or weeks, enabling new designs to have a shorter time-to-market, and allowing logistics companies to print parts on demand rather than carry inventory.

The use of robotics and automation in manufacturing and logistics will emphasize the importance of a reliable IT system. As manual labor shifts to automation, downtime will affect more aspects of the production and distribution processes.

- **Consumer data breaches.** As retailers continue to heavily integrate their POS systems with web commerce and mobile applications, the risk of compromising customer information grows. Every new application or device added to existing infrastructure introduces a potential channel for cyberattacks. When sensitive data such as credit card information is stolen, serious repercussions tend to follow.
- **Data center disruptions and outages.** Data breaches are not the only cause of disruption that may result in significant costs for companies.

  Athletic apparel retailer Finish Line, for example, experienced over $32 million in lost sales after the disastrous implementation of a new Warehouse Management System (WMS) in late 2015. The company selected a new vendor for their WMS and Distributed Order Management (DOM) system at an existing distribution center in an attempt to better satisfy omni-channel customers. The company not only suffered lost sales, but announced that it would close 150 stores over the next four years.

  Table 2 lists examples of a wide range of potential costs resulting from outages and disruptions in manufacturing companies.

REPORTING IMPLICATIONS

U.S. companies are required to identify significant risk factors to the SEC through their annual reporting publications and Form 10-K documentation. Information technology failures that can cause supply chain and other business operations disruptions are regularly reported as potential risks for many companies. Table 3 summarizes representative disclosures from three companies operating supply chains.

Companies often note the impact or potential impact of data breaches on business operations. As regulatory scrutiny increases, so does the cost of a data breach or other disruption.

While breaches such as those experienced by Yahoo tend to dominate headlines, companies in all industries face pervasive threats of hacking and malware penetration. Cyberattacks are increasingly sophisticated, and the IT infrastructures of many companies are not adequately secured against such intrusions.

Financial Services

The financial services industry is perhaps the most sensitive to security risks. The sophistication of risk-management processes and systems continues to evolve as cybersecurity remains a fundamental priority in this industry.

TABLE 2: Examples of Potential Costs of Outages—Manufacturing Companies

STRATEGIC COSTS		
• Charge against earnings	• Damaged reputation	• Legal exposure
• Financial metrics/ratios	- Financial markets	- Customers
• Share price decline	- Customers/prospects	- Third parties
• Share price volatility	- Banks	- Shareholders
• Cost of capital	- Business partners	• Compliance exposure
• Increased risk provision	- M&A candidates	- Regulatory reporting
• Reduced brand value	• Impaired credit	- Impaired inspection
• Insurance premiums	• Liquidity exposure	- Impaired traceability

CUSTOMER-RELATED COSTS		
• Lost short-term sales	• Late delivery penalties	• Customer rebates
• Lost short-term profit	• Imperfect order penalties	• Buyback pricing/concessions
• Lost future sales/profit	• Product defect penalties	• Additional customer service cost

OPERATIONAL COSTS		
• Idle capacity	• Finance processes	• Error-related costs
- Overall supply chain	- Delayed billing/receivables	- Order processing errors
- Procurement	- Inventory carrying cost	- Product defect
- Plant operations	- Cash flow cost	- Specification error
- Logistics/distribution	- Delayed close	- Manufacturing error
- Transportation	• Costs of change	- Quality failure
- Warehouses	- Procurement change	- Shipment error
- Third-party services	- Revised order processing	- Damaged product
• Personnel costs	- Special order cost	- Wrong packaging
- Idleness/underutilization	- Production schedule change	- Routing error
- Reduced productivity	- Line change cost	- Wrong delivery time
- Additional work required	- Costs of logistics change	• Other costs
- Overtime/shift premiums	- Supplier premiums	- Lost promotional expenditure
- Additional T&E costs	- Expedited transportation	- Lost marketing expenditure
	- Additional handling cost	- IT costs
	- Additional inventory cost	- Administrative costs
	- Additional checking cost	- Overhead

The growth of online and mobile banking has only increased the risks to which banks are exposed. Cyberattacks and data breaches have the potential to cause financial loss for customers, in addition to compromising sensitive information. An inability to access accounts, and delayed or lost transactions may result in late fees and penalties, frustrating customers. Theft of personal information can lead to fraudulent activity with negative impacts on customers' credit. Remedial actions may take a significant amount of time, involving numerous agencies and third parties.

Most financial institutions have developed high availability, disaster recovery, and security automation over time, but these infrastructures only help reduce risk, not eliminate it.

TABLE 3: Risk Factors Cited by Supply Chain Companies—Examples from Recent Annual Reports

MANUFACTURER	
We rely extensively on IT systems, networks & services, including Internet sites, data hosting & processing facilities & tools & other hardware, software & technical applications & platforms, some of which are managed, hosted, provided &/or used by third parties or their vendors, to assist in conducting business.	In the ordinary course of our business, we electronically maintain sensitive data, including intellectual property, our proprietary business information & that of our customers & suppliers, & some personally identifiable information of our customers & employees, in our facilities & on our networks. The secure processing, maintenance & transmission of this information is important to our operations. A breach of our security systems & procedures or those of our vendors could result in significant data losses or theft of our customers' or our employees' intellectual property, proprietary business information or personally identifiable information.
RETAILER	
Our success, in particular our ability to successfully manage inventory levels & process customer transactions, largely depends upon the efficient operation of our IT systems. A security breach of our IT systems could damage our reputation & have an adverse effect on operations & results.	We accept electronic credit & debit payment cards from customers. A number of retailers have experienced security breaches in which credit & debit card & other sensitive information has been stolen or compromised. While we have taken significant steps to prevent the occurrence of security breaches in this respect, our IT systems remain vulnerable to damage, theft or intrusion that could harm our business.
DISTRIBUTOR	
We operate a number of facilities & we coordinate company activities, including IT systems & administrative services & the like, through our headquarters operations.	Global businesses like ours are facing increasing risks of criminal, illegal & other fraudulent acts. The evolving nature of such threats…are making it increasingly difficult for us to anticipate & adequately mitigate these risks. Although management believes internal controls are adequate to timely detect unauthorized cash disbursements so as to prevent a material misstatement of the company's financial statements, these controls may not be adequate to safeguard the company's cash assets from unauthorized transfers resulting from human error. In addition, designing & implementing measures to defend against, prevent & detect these types of activities are increasingly costly & invasive into the operations of the business. The company may not be able to adequately anticipate, prevent or mitigate damage resulting from criminal & other illegal or fraudulent activities committed against it.

AVAILABILITY AND RECOVERY

The traditional business-hour window of operations no longer exists. Customer transactions and queries across all channels access business-critical software at all hours of the day, everyday. Inability to meet these expectations can lead to an erosion of customer trust and the eventual loss of customers.

The banking and financial services industry has become focused on customer lifetime value (CLV) as the appeal of a new generation of online financial services has bred competition, especially in geographic areas previously served primarily by local institutions. The high cost associated with attracting new in-bank customers (averaging $200 each) has made efforts to increase customer engagement and/or to re-engage former customers a more attractive marketing strategy to pursue. Mobile and social media business engagement requires reliable and rapid processing of current data to be effective.

In addition to providing fast, reliable service, customers also expect financial services providers to implement vigorous security measures for protecting their sensitive information. System vulnerabilities can lead to disastrous breaches, resulting in potential losses for the customers and the bank.

In November 2016, Tesco Bank experienced an attack that appeared to affect 20,000 accounts and led to a loss of over $3 million.

In December 2016, Bank of New York Mellon Corporation experienced a 19-hour technology interruption that prevented it from processing payment instructions sent to them via the Swift network. Bank clients routinely use the Swift network to communication instructions to the bank to make billions of dollars of payments. It is believed that the root of the problem was a technological issue inside a single platform hosted by the bank. The bank now has backup plans and systems in place.

In January 2017, Lloyds Bank was hit by a distributed denial of service (DDoS) attack that culminated in an extortion attempt. Although customers did not suffer financial loss, they were unable to access their accounts for several days. Time-sensitive transactions may have been delayed and late fees incurred, resulting in customer dissatisfaction.

Banking industry analysts agree that customer trust is becoming a critical competitive differentiator. The ability of banking institutions to evolve and adapt to meet customer expectations—such as secure, 24/7 availability, self-service features accessed via web and mobile, and personalized, tailored services —is the digital currency required by customers in order to earn that trust.

Centuries of conservative traditions tend to change slowly within financial institutions. Banks in particular pride themselves in maintaining heavily governed, risk avoidance strategies designed specifically to isolate, protect, and lock down assets and information. But a generation of industry newcomers that are winning over customer trust through agility and innovation have laid some impressive groundwork. Such accomplishments should, clearly, influence bank IT considerations and strategies.

SECURITY AND DATA BREACHES

Cybercrime follows the money; hence, financial services companies are the obvious and preferred targets of sophisticated external criminal threats. However, according to the *2016 Insider Threat Spotlight Report*, insider attacks are on the rise, and privileged IT users, such as administrators with access to sensitive information, pose the biggest insider threat (60 percent). This is followed by contractors and consultants (57 percent), and regular employees (51 percent). The majority of survey respondents (66 percent) indicated that they have a harder time detecting and preventing an insider attack versus an external cyberattack.

IBM i offers protection against such insider threats through its authority collection capability. IBM i is supported by most major ISVs offering core banking and electronic funds transfer (EFT) solutions. It has also been widely deployed by insurance companies and other financial businesses. According to IBM, "authority collection assists administrators in securing the objects in an application with the lowest level of authority that is required to allow the application to run successfully." By removing and/or avoiding excess authority, the chances of successful insider attacks are lowered.

Companies that have experienced breaches report that customer attrition and brand damage represent a large cost component. However, the combined total of fines, penalties, and other costs may be higher than is generally realized. Such costs may include investigations, technical fixes, customer notifications, query handling, credit monitoring, identity monitoring, and other remedial actions.

REPORTING IMPLICATIONS

Risks of disruption due to IT failures and security breaches are recognized in statutory reporting by most financial services companies.

The banking industry is undergoing rapid technological change, particularly with the rise of mobile and web banking. However, these firms cannot sacrifice the security of their existing IT infrastructure as they explore ways to successfully compete. For this industry, adopting and leveraging of new technologies requires exceptional and constant testing and monitoring.

Insurance companies, such as those providing medical or automotive insurance, deal with unpredictable events and must respond instantly to requests for customer data in emergency situations. These companies have been and remain extremely dependent on highly available, reliable systems. Any disruptions resulting in the inability of customer service staff to access policies can have dire effects. Representative comments from recent annual reports and/or Form 10-Ks are summarized in Table 4.

Platform Differentiators

Distinctive features of the IBM i operating system contribute to its strengths in simplicity, stability, and security.

- **Simplicity.** IBM i systems are automatically preconfigured, but can also be customized to firm-specific workloads.

IBM DB2 for i is fully integrated in the operating system and pre-installed on the server. Many DBA tasks are automated, such as resource allocation, index balancing, and application rebinding. In

TABLE 4: Risk Factors Cited by Financial Services Companies—Examples from Recent Annual Reports

BANK	
The financial services market is undergoing rapid technological changes, & if we are unable to stay current with those changes, we will not be able to effectively compete.	We depend upon our ability to process, record, & monitor a large number of client transactions on a continuous basis. We, our customers, & other financial institutions with which we interact, are subject to ongoing, continuous attempts to penetrate key systems by individual hackers, organized criminals, & in some cases, state-sponsored organizations. Information security risks for large financial institutions such as ours have generally increased in recent years in part because of the proliferation of new technologies. Any failure, interruption or breach in security of these systems could result in failures or disruptions in our customer relationship management, general ledger, deposit, loan & other systems, misappropriation of funds, & theft of proprietary Company or customer data… As client, public, & regulatory expectations regarding operational & information security have increased, our operational systems & infrastructure must continue to be safeguarded & monitored for potential failures, disruptions, & breakdowns…
INSURANCE	
The regulatory environment surrounding information security & privacy is increasingly demanding. We are subject to numerous U.S. federal & state laws & regulations in jurisdictions outside the U.S. governing the protection of personal & confidential information of our clients or employees, including in relation to medical records, credit card data & financial information.	While technology can streamline many business processes & ultimately reduce the cost of operations, technology initiatives present certain risks. We use computer systems, including automated underwriting platforms, to store, retrieve, evaluate & utilize customer & company data & information. Our IT & telecommunications systems, in turn, interface with & rely upon third-party information networks & systems. Our business is highly dependent on the availability, speed & reliability of these networks & systems to perform necessary business functions, such as providing new-business quotes, processing new & renewal business, making changes to existing policies, filing & paying claims, & providing customer support. If we sustain cyber-attacks or other privacy or data security incidents, that result in security breaches that disrupt our operations or result in the unintended dissemination of sensitive personal information or proprietary or confidential information, we could suffer a loss of revenue & increased costs, exposure to significant liability, reputational harm & other serious negative consequences.
IT SERVICES	
Failure to anticipate, adapt to or keep pace with new technologies in the payments industry could harm our business & impact our future growth.	The global payments industry is undergoing significant & rapid technological change, including mobile & other proximity payment & acceptance technologies, ecommerce, tokenization, crypto-currency, distributed ledger & block chain technologies, & as a result we expect new services & technologies to continue to emerge & evolve. In addition to our own initiatives & innovations, we work closely with third parties, including some potential competitors, for the development of & access to new technologies… If we or our partners fail to adapt or keep pace with new technologies in the payments space in a timely manner, it could harm our ability to compete, decrease the value of our products & services to our clients, impact our intellectual property or licensing rights, & harm our business & impact our future growth.

contrast, the engineered architecture of the Oracle Exadata Database Machine requires higher system overhead and specialized DBA skills.

IBM i's kernel incorporates single-level storage, treating all storage resources, including main memory and disks, as a single storage pool. Objects are scattered across all disks and drives as part of the storage pool, enabling high-speed, parallel retrieval of objects. The operating system automatically recognizes and integrates additional storage into the system's single storage pool without user intervention. Transparent, automated storage configuration and management promote higher productivity and allow administrators to focus on more important tasks.

Technology-independent machine interface (TIMI) acts as a virtual instruction set independent of the underlying CPU instruction set, which allows IBM i to fundamentally change the implementation of underlying hardware, firmware, and virtualization features, without requiring rewriting, changing, or even recompiling applications written by users. TIMI provides forward compatibility for applications running on IBM i, protecting existing software investments by prolonging software lifespan.

There are no Windows or Linux equivalents to single-level storage or TIMI.

- **Stability.** IBM i components are implemented in a highly synergistic manner, and engineered to interact efficiently.

  Windows and Linux environments require that users acquire, install, configure, and administer hardware and software products from multiple vendors. As a result, deployment complexity and management challenges can be magnified. In addition to higher staffing requirements, less integrated environments are also more likely to degrade performance.

  Specialized features of IBM i further minimize risks of data loss in the event of an unplanned outage. These include auxiliary storage pools (ASPs), which can be allocated to users and/or have different levels of protection. Storage pool disks can also be protected through mirroring or by using RAID-5 arrays.

  Another capability, Live Partition Mobility, allows movement of active logical partitions (LPARs) between systems without disrupting operations. Service interruptions of one or two seconds may occur due to network latency, but are rarely noticeable to users. The Save While Active feature allows backups of the system to be made without taking systems offline. IBM PowerHA SystemMirror for i enables live failover clustering.

- **Security.** The core IBM i design is built around a unique object-based kernel in which all system resources are defined and managed as objects, providing isolation and protection for data assets. The strengths of IBM i's object-based design are reinforced by tight integration of security functions with compiler, directory server, and object-based file system structures. In contrast, security in Windows- and Oracle-based environments is implemented using separate software tools and subsystems with less integration. This is evident in the vulnerability statistics provided by the National Vulnerability Database; Windows Server and various enterprise Linux distributions, such as Oracle Linux, have historically been more vulnerable than IBM i.

Systems relying on basic user access credentials do not proactively secure data assets. IBM i adds the protection of the authority collection, a major enhancement to security management unique to IBM i. This feature tracks object usage by applications and users to enable administrators to optimize security. This provides another layer of protection as more IBM i systems are opening up to the Internet, social activity, and mobile connections. Although third party and open source applications come with increased security risks, IBM i remains a highly securable system when properly configured and managed according to best practices.

Other characteristics of the IBM i set the platform apart.

- **User community.** IBM i benefits from a knowledgeable and passionate community of users that IBM encourages and helps promote. There is an extensive network of COMMON user groups, the Large User Group (LUG), iSUC Japan, the Power Academic Initiative, and various social media communities. IBM's dedication to integrating open source software is evident in their LinkedIn Group with hundreds of members.

  The IBM i development team gathers feedback and requirements from clients to prioritize their wants and needs in future Technology Refreshes (TRs) or product releases. As a platform driven by customers' business solutions, IBM i's development team focuses on compatibility and integration with not only leading business applications, but also the latest environments and tools for developers.

- **Open source and modernization.** Recent releases of IBM i included major modernization enhancements such as intuitive graphical user interfaces (GUIs), database improvements, and newer languages and frameworks.

  The IBM Rational Developer for i is an Eclipse-based platform offering a rich selection of development tools to enable higher team productivity. For Java development, IBM offers the IBM i Toolbox for Java and JTOpen, a library of Java classes that enable Java applets, servlets, and applications to access IBM i resources.

  For modern organizations, mobile and web access to core business data has become a necessity. Zend offers various products for IBM i modernization to satisfy business requirements. Zend Server for IBM i is a no charge, production-ready PHP development platform that runs natively, bringing the most popular web and mobile language to i. The enterprise-class Zend DBi introduces the popular open source MySQL and MariaDB to the IBM i ecosystem, allowing IBM i shops to leverage popular industry standard PHP applications and frameworks valued by the open source community.

  The numerous open source products currently supported on IBM i include Ruby on Rails, Node.js, Git, Orion, Python, Apache Web Server, and SugarCRM.

- **Commitment to continuity.** IBM has continued to invest in established languages such as the RPG II, COBOL, and CL, and ISV partners continue to offer a wide range of application modernization tools. In addition, a wide range of other languages such as C/C++, Java, PHP, XML, IBM Rational Enterprise Generation Language (EGL), and others may be employed.

IBM policy on IBM i technology upgrades is distinctive. As a general principle, IBM introduces new IBM i releases every two years and TRs—which may be applied in a simple, non-disruptive manner—every six months. This approach, widely requested by customers, avoids the disruptions caused by frequent version migrations.

In 2016, IBM reaffirmed its commitment to IBM i by stating that it would provide concurrent support for IBM i, AIX (the IBM version of UNIX), and Linux for Power Systems. The current IBM i roadmap indicates that enhancements are planned until 2026. Few operating systems, if any, come with a planned support life cycle of 10 years.

IBM POWER SYSTEMS

IBM has progressively enhanced the Power Systems platform since its introduction in 1990. In 2008, the System p and System i server lines were merged under the Power Systems name. Today's POWER8-based systems deliver significant advances over previous generations. Processor performance has been accelerated, up to eight threads per core are supported (compared to two on x86 servers), and memory and I/O features have been upgraded to support faster throughput.

The company has also put industry-leading capabilities in place.

- **Performance optimization.** Power Systems performance is a function not only of POWER processors, but also of close optimization at all levels of design and implementation. Key capabilities include highly effective compiler acceleration; chip symmetric multithreading (SMT); low levels of symmetric multiprocessing (SMP) overhead; and on-chip memory acceleration and compression technologies.

  Active Memory Expansion, for example, enables compression rates of up to 50 percent for data in memory; i.e., usable main memory may be up to double physical memory. In addition to lower memory costs, system throughput is improved.

  Additional performance boosts are incorporated in POWER8-based systems. Along with an upgrade in the number of cores to eight, a hardware-based transactional memory feature accelerates high-volume parallel applications, and a Coherent Accelerator Processor Interface (CAPI) enables higher-bandwidth CPU access for specialized co-processors. On-chip accelerators also provide high-speed encryption, compression, authentication code, and random number generation.

- **PowerVM virtualization.** This is one of the industry's most sophisticated virtualization architectures. PowerVM is extremely scalable and offers highly granular allocations of cores and virtual CPUs, allowing more efficient management of workloads. PowerVM Enterprise Edition supports up to 1000 VMs per server whereas Oracle VM only supports up to 128 VMs per Oracle VM server. Microsoft Hyper-V supports 384 VMs per host.

  Hardware-based LPARs isolate workloads more effectively than software-based partitioning techniques, and provide additional security functions. The micro-partitioning feature allows for the allocation of fractions of processors to LPARs, increasing server utilization efficiency.

PowerVM also allows AIX and Linux to run in partitions on the same physical system supporting the IBM i operating system. Linux support has allowed IBM i users to deploy Internet and intranet infrastructures, along with open source applications, on Power Systems that are also hosting business-critical software.

In addition, reliability, accessibility, and serviceability (RAS) features in Power Systems hardware are among the most sophisticated in the industry. Comparable features may be found in x86 servers in some cases. However, the microelectronics technology in Power Systems is more advanced, and these systems have longer track records of stable and effective operation.

IBM offers a variety of pricing options for IBM i on Power Systems. Solution Editions, which are customized for more than 160 industry-specific and cross-industry ISV offerings, offer packages of hardware, software, and services that reduce overall costs by up to 25 percent. Pre-configuration and testing for individual customer requirements also enables more rapid and cost-effective deployments.

Other programs allow users of larger Power Systems to license Power cores employed for application serving at lower costs than for database servers; and offer capacity-based pricing for PowerVM partitions and IBM i-defined workloads. In addition, Managed Service Provider (MSP) utility pricing offers special terms for service providers.

STORAGE SUPPORT

The IBM System Storage DS8000 series offers high levels of performance and availability and may be attached to IBM i systems. The DS8000 platform is commonly employed for the most business-critical mainframe- and UNIX server-based systems worldwide. In addition, IBM Storwize storage options are supported by IBM i systems, along with wide range of other IBM and third-party storage systems, including IBM FlashSystem and other vendors' all-flash arrays.

Although Windows systems can use a variety of storage systems, it often requires integration of software and hardware from different vendors, which can lead to deployment complexity. On the other end of the spectrum, Oracle Exadata users are limited to using specific Oracle hardware and software.

Easy Tier, IBM's solution for automated storage tiering, is supported by IBM i for DS8000 as well as other IBM disk arrays. Easy Tier enables full-function tiering while minimizing the complexities with which storage administrators must contend when implementing other storage tiering solutions. Additionally, IBM Spectrum Scale parallel file system offers the Transparent Cloud Tiering feature, which enables hybrid cloud storage.

Cost of Downtime

Detailed financial and operational data supplied by 62 companies employing IBM i, Microsoft Windows Server, and/or Oracle Exadata to run core enterprise systems were used to create composite companies in six industries. Average costs of downtime were estimated for each of the three platforms for a three-year period. The focus was placed on underlying hardware and software platform outages, rather than application-level downtime.

Comparisons are for six companies operating as either supply chains (a manufacturer, a retail chain, and an industrial distributor) or providing financial services (a bank, an insurance company, and a IT services company). Companies range from $30 million to $6 billion in revenues, and have between 1,000 and more than 20,000 employees. For each company, three-year costs of downtime are shown in Figure 5.

Supply chain cost calculations are based upon ERP systems, such as customer relationship management (CRM), supply chain management (SCM), product data management (PDM), product lifecycle management (PLM), supplier relationship management (SRM), electronic data interchange (EDI), and other applications, affected by hardware and operating system outages. Supply chain costs included outages experienced with mobile sales, cloud services, and social media applications. Loss of personnel productivity (executives, managers, analysts, and others) was caused by delays in current data delivery from business-critical software.

FIGURE 5: Three-year Cost of Downtime

Downtime costs were significant for financial services companies that experienced outages or delays. Cost calculations for companies in this sector factored in customer reliance on mobile and web banking, and operations involving social media marketing, customer and partner cloud resources, and data warehouse responsiveness and currency.

For each of the company profiles upon which calculations were based, calculations factored in applications that range from analytics to customer transactions.

COMPANY PROFILES

The results presented in this paper were based on the company profiles summarized in Table 5.

Profiles were constructed using survey data from companies of approximately the same size, in the same industries, with generally similar business profiles. Comparisons are between IBM i 7.3 on POWER8 systems with IBM PowerHA SystemMirror for i clusters; Microsoft Windows Server 2016 with SQL Server 2016 AlwaysOn clusters on latest-generation Intel E5 and E7 x86-based hardware; and Oracle Exadata Database Machine X6-2 and X6-8 with Real Application Clusters (RAC) and Data Guard.

Data was collected on business operations including, where appropriate, vulnerability to cascading effects; applications employed including packaged as well as custom software; workloads; availability experiences including frequency and duration of planned and unplanned outages; security and disaster recovery arrangements; and other quantifiable outcomes.

TABLE 5: Company Profiles

Supply Chain Companies					
AUTO PARTS MANUFACTURER		**RETAIL CHAIN**		**INDUSTRIAL DISTRIBUTOR**	
Sales	$2B	Sales	$5B	Sales	$3B
Employees	10,000	Employees	20,000	Employees	10,000
Distribution centers	30	Stores / Branches	3,000+	Stores / Branches	300
		Distribution centers	5	Distribution centers	10

Financial Services Companies					
BANK		**INSURANCE COMPANY**		**SERVICES COMPANY**	
Revenue	$6B	Revenue	$40M	Revenue	$1.5B
Employees	10,000	Employees	1,000	Employees	2,500
Branches	600+	Assets	300M+	Assets	$30B+
Assets	$300B+	Policyholders	500,000+		

SEVERE UNPLANNED OUTAGES

For this paper, risk exposure to severe unplanned outages of over four hours was determined for the same applications and platforms as for costs of downtime. Risk exposure for supply chain companies averaged 24 and 66 times less for use of IBM i than for Oracle Exadata and Windows Server respectively. For financial services companies, risk exposure for IBM i averaged 26 and 79 times less than for Oracle Exadata and Windows Server, respectively.

Probabilities of outages for each platform for each company were calculated based on user input as well as general industry data for the frequency and severity of outages for platforms. Projected business impacts were calculated for severe unplanned outages of over four hours for each company.

The probability of severe unplanned outages was then multiplied by projected business impact; e.g., if the probability of a six-hour outage was eight percent, and the cost of such an outage was $5 million per hour, the calculation was 0.08 x $5 million/hour x 6 hours = $2.4 million.

All values for costs of downtime as well as severe unplanned outage exposure were for the US.

SUPPLY CHAIN COMPANIES

Costs of downtime for supply chain companies were calculated as follows:

- **Automotive parts manufacturer**. Costs included lost sales; idle and underutilized capacity; handling of delivery delays; additional inventory carrying costs; costs of change for procurement, production and logistics processes; customer billing and payments delays; late delivery and imperfect order penalties; and costs of remedial actions such as rebates and discounts required to win back customer business.

  Costs were divided between inbound supply chain and production disruption, consisting of costs incurred between supplier queries and factory release; and outbound supply chain disruption, consisting of costs incurred between factory release and customer delivery.

  Categories correspond to the Source and Make and Deliver segments of the Supply Chain Operations Reference (SCOR) model developed by the Supply Chain Council. Inbound supply chain and production disruption calculations include costs of scheduling, setup, and other production changes. Costs of downtime for the company's EDI cloud were included in inbound supply chain costs.

- **Retail chain.** Costs included lost sales; supply chain disruption (including the same components as for the automotive parts manufacturer); and selling, general and administrative (SG&A) costs including reordering, restocking, and (in storefront outlets) display changes.

  Costs of downtime for mobile sales and social media marketing applications were included in lost sales.

- **Industrial distributor.** Costs of downtime include lost sales due to inventory shortages; inability to process customer queries and orders and related effects; and supply chain disruption costs, including the same components as for the automotive parts manufacturer and retail chain.

Costs of downtime for customer and partner clouds were divided between both categories, and comparable costs for mobile sales applications were included in lost sales.

Values were based on user input and published material such as financial reports and presentations.

FINANCIAL SERVICES COMPANIES

Breakdowns of costs of downtime per hour for each industry are shown in Figure 6 and were calculated as follows:

- **Bank.** Costs included customer attrition (lost customer income); lost transaction fees (including ATM/debit fees, and fees for transactions conducted online and through call centers); and other costs, (including lost interest, lost customer acquisition expenditure, as well as productivity loss by branch,

FIGURE 6: Detailed Costs of Downtime per Hour

Supply Chain Companies

AUTO PARTS MANUFACTURER	
Cost category	*Outage cost per hour*
Outbound supply chain disruption	$158,888
Inbound supply chain & production disruption	$40,773
Customer penalties & remedial costs	$56,532
TOTAL	**$256,193**

RETAIL CHAIN	
Cost category	*Outage cost per hour*
Lost sales	$229,138
Supply chain disruption	$132,008
SG&A costs	$53,188
TOTAL	**$414,335**

INDUSTRIAL DISTRIBUTOR	
Cost category	*Outage cost per hour*
Lost sales	$135,720
Supply chain disruption	$145,390
TOTAL	**$281,110**

Financial Services Companies

BANK	
Cost category	*Outage cost per hour*
Customer attrition	$116,462
Lost fee income	$148,179
Other costs	$53,077
TOTAL	**$317,718**

INSURANCE COMPANY	
Cost category	*Outage cost per hour*
Lost sales	$12,946
Other costs	$530
TOTAL	**$13,476**

SERVICES COMPANY	
Cost category	*Outage cost per hour*
Lost income	$61,135
Other costs	$33,169
TOTAL	**$94,304**

call center, and other customer-facing staff during outages. Costs of mobile banking outages were included in customer attrition and lost fee income.

- **Insurance company.** Costs included lost premium income due to customer attrition, missed sales opportunities, and payment delays; and other costs, including lost interest, lost customer acquisition expenditure, and productivity loss by customer interaction center staff.

  Costs of downtime for social media marketing and account service were included in lost income.

- **IT Services company.** Costs include lost fee income, customer attrition, and other costs including lost interest and productivity loss by customer interaction center staff.

  Costs of downtime for customer and partner clouds as well as for social media marketing and account service applications are included in lost fee income and customer attrition.

For the three companies, costs of customer attrition were calculated based on appropriate CLV values. Costs of data warehouse downtime were included in the Other category. Published materials were again employed.

Conclusions

The IT world has moved toward greater complexity and interconnectedness. Cyberattacks are more sophisticated than ever, and concern over cybersecurity is at an all time high. As businesses become more reliant on real-time business intelligence (BI) applications, mobile and web commerce, big data, automation, and other technology advancements, they also become increasingly at-risk of paying significant costs due to downtime.

IBM i employs a simple—yet securable—architecture that minimizes personnel overhead. It is the industry's most resilient platform, and its strengths in automated management, malware resistance, and backward and forward platform compatibility provide a tested foundation from which downtime challenges can be addressed.

Three-year costs of downtime averaged 8.2 times more for use of Windows Server, and 3.4 times more for use of Oracle Exadata than for use of IBM i. Lower IBM i costs of downtime result in potential three-year business savings of $15.2 million compared to the use of Windows Server, and $5.1 million compared to Oracle Exadata. Risk exposure for both supply chain and financial companies averages 24 and 66 times less for IBM i when compared to Windows Server and Oracle Exadata respectively.

IBM i design strengths contribute to overall lower costs of downtime. IBM i also supports the extension of business-critical software to cloud, mobile, analytics, and social media applications, while maintaining a focus on flexibility, cost savings, and virtualization benefits that it has sustained over decades.

Index

LIST OF FIGURES

LIST OF TABLES

LIST OF REFERENCES

Pew Research Institute's Online Shopping & E-Commerce survey found at www.pewinternet.org/2016/12/19/online-shopping-and-e-commerce/

Bank of America's 2016 Trends in Consumer Mobility Report found at newsroom.bankofamerica.com/files/press_kit/additional/2016_BAC_Trends_in_Consumer_Mobility_Report.pdf

Ponemon Institute's 2016 Cost of Data Breach found at securityintelligence.com/media/2016-cost-data-breach-study/

2017 IBM i Marketplace Survey found at static.helpsystems.com/hs/pdfs/2017-marketplace/2017-ibmi-marketplace-survey.pdf

Identity Theft Resource Center found at www.idtheftcenter.org/images/breach/ITRCBreachStatsReportSummary2016.pdf

Ponemon Institute's 2016 Cost of Data Center Outages found at datacenterfrontier.com/white-paper/cost-data-center-outages/

National Institute of Standards and Technology found at nvd.nist.gov/

Business Continuity Institute's 2016 Supply Chain Resilience Survey found at www.thebci.org/index.php/bci-supply-chain-resilience-report-2016

Insider Threat Spotlight Report found at www.crowdresearchpartners.com/wp-content/uploads/2016/09/Insider-Threat-Report-2016.pdf

NetDiligence 2016 Cyber Claims study found at netdiligence.com/portfolio/cyber-claims-study/

Quark + Lepton™

CORPORATE OFFICE
Boulder, Colorado USA

www.quarkandlepton.com