NATIONAL CENTER FOR
THE MIDDLE MARKET

A SPECIAL REPORT BY THE NATIONAL CENTER FOR THE MIDDLE MARKET

Risk & Resilience in the Middle Market

How companies prepare for and respond to major business disruptions.

IN COLLABORATION WITH

The Ohio State University
Fisher College of Business

SunTrust

Grant Thornton

Cisco

About This Report

As recent events in Florida, Texas, and California clearly demonstrate, companies of all types and sizes can fall victim to natural disaster. Beyond major events like hurricanes and wildfires, operational disruptions can also include problems with suppliers or distributors, port closures, or facility shutdowns. Risks also come in the form of strategic disruption (which includes political risk, the impact of megatrends or new technology, or industry consolidation), and digital disruptions (such as cyber breaches or system downtime).

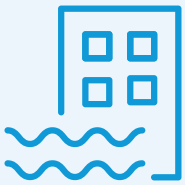
As part of the 4Q'17 Middle Market Indicator survey administered to more than 1,000 C-level executives in December 2017, the National Center for the Middle Market set out to better understand the prevalence and impact of different types of business disruptions among middle market companies and to create a comprehensive picture of the major risks companies face and their resilience to withstand those disruptions. The survey was completed in the aftermath of Hurricanes Harvey and Irma and the northern California wildfires, and we oversampled in these areas to gain perspective from middle market business leaders recovering from recent natural disasters. At the same time, we asked about other categories of risk—strategic, digital, and other operational risk—to understand the impact of disruption on business, how prepared companies are to weather the various types of storms they encounter, and how quickly they recover from different challenges.

» ***This report presents key findings along with a framework and additional resources companies can leverage to bolster their risk management capabilities.***

3 types of business disruptions can affect middle market companies

STRATEGIC DISRUPTION

Events such as industry consolidation, disruptive technology, the impact of global megatrends, changing regulations or economic conditions, and changes in ownership that undermine an organization's strategy and significantly change the competitive dynamics of an industry or market segment.



OPERATIONAL DISRUPTION

Events such as natural disasters, port closures, strikes, and facility shut-downs that can hinder operations by affecting a company's own facilities or the suppliers and distributors on which it relies.

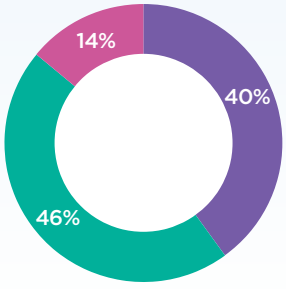
DIGITAL DISRUPTION

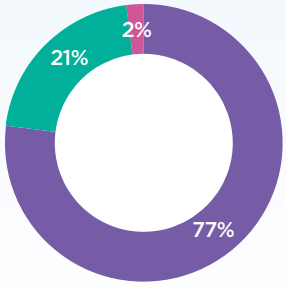
Cyber breaches, data integrity issues, system downtime, or compatibility issues that put company and customer information at risk or affect a company's ability to deliver services and conduct business.

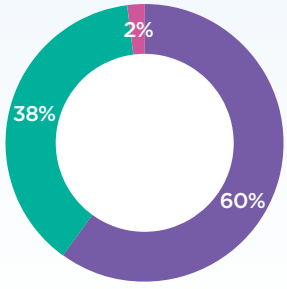
Business disruptions are common and their impact is substantial

Over the past two years, half of middle market businesses experienced some type of business disruption—strategic, operational, or digital. Strategic disruptions are the most prevalent. They also pack the biggest punch and are the hardest from which to recover.

	STRATEGIC DISRUPTION	OPERATIONAL DISRUPTION	DIGITAL DISRUPTION
PREVELANCE	27% OF COMPANIES	21% OF COMPANIES	17% OF COMPANIES
IMPACT	14.2% OF ANNUAL REVENUE	8.8% OF ANNUAL REVENUE	11.7% OF ANNUAL REVENUE
RECOVERY	40% RECOVER COMPLETELY*	77% RECOVER COMPLETELY*	60% RECOVER COMPLETELY*





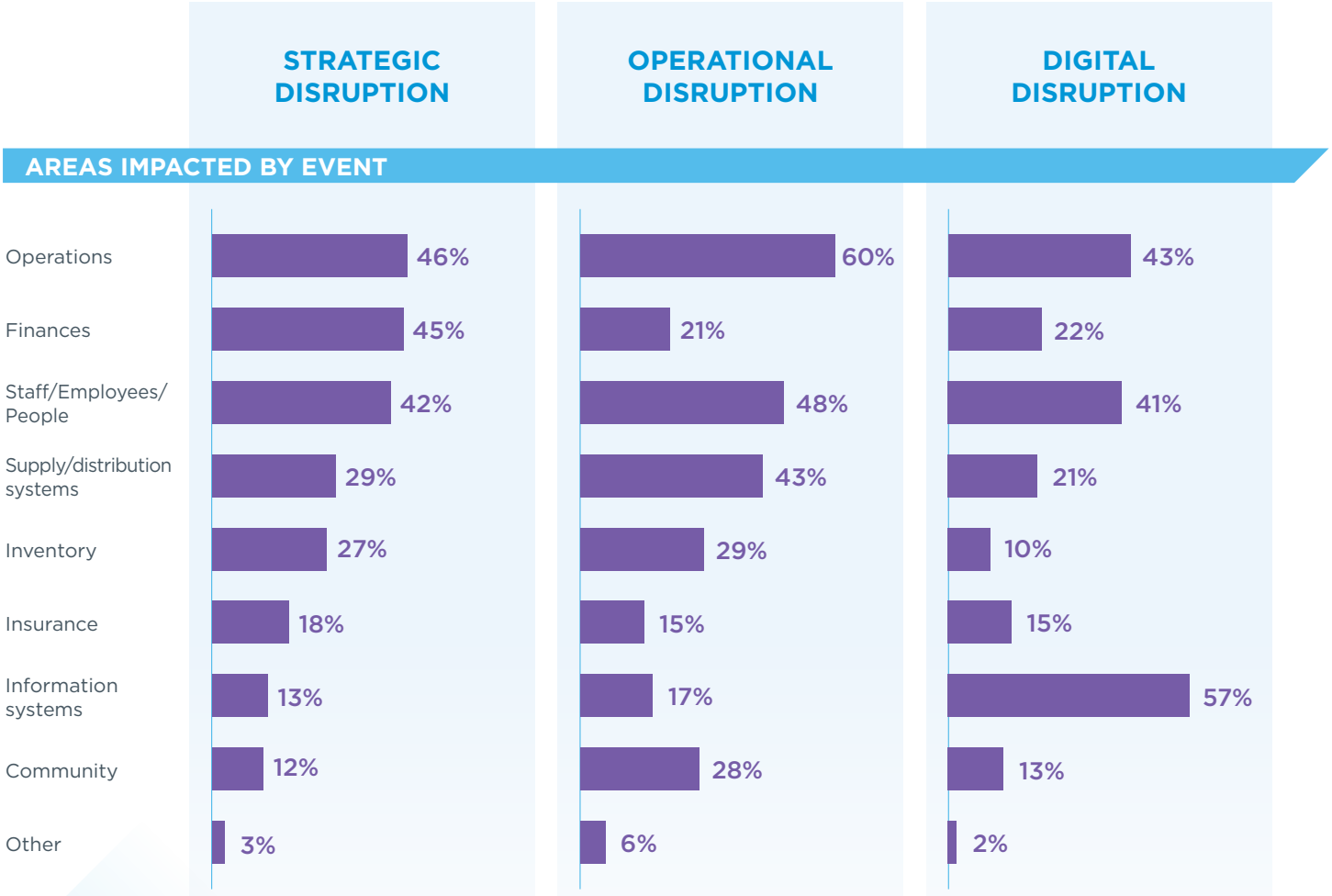


*As of survey date

Recovered completely | Recovered partially | Not recovered at all

Operations and people bear the brunt of business disruptions

Disruptions of all types have a significant impact on operations and people. Not surprisingly, technology disruptions disproportionately affect information systems. Strategic disruptions take by far the greatest toll on finances. Operational disruptions are most likely to reach beyond a business' four walls to neighboring businesses and the community at large—or, perhaps, to begin outside the company (a hurricane, a supply chain break) and come in to affect a company.



Strategic disruptions do the most damage

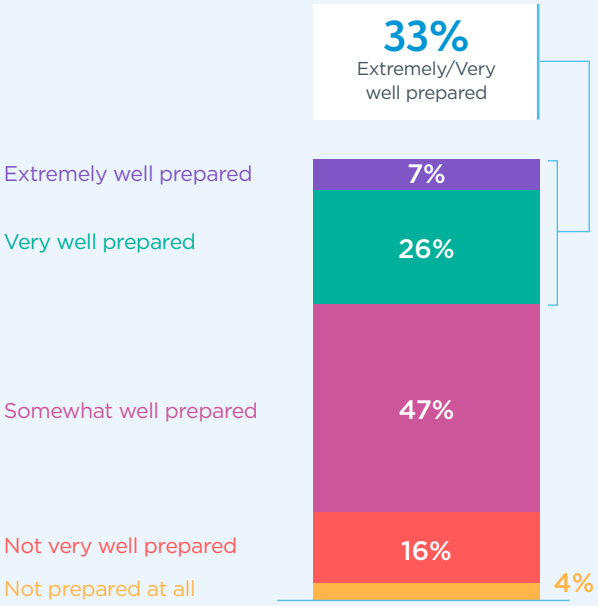
Strategic disruption is the most prevalent risk companies encounter; over a quarter of companies have been affected in the past two years. At the same time, executives are least prepared for these types of events, perhaps because they often have little to no control over the factors that contribute to them. Strategic disruption can undermine the basis on which a business is built, permanently altering the nature or structure of competition within an industry. This makes recovery challenging at best, and impossible on occasion. Executives say it can take months or even years to contend with strategic disruption. The majority of companies only recover partially, with 14% of affected businesses indicating that they have not recovered at all from a recent event.

- *» Most prevalent*
- *» Hardest to prevent*
- *» Biggest impact*
- *» Most difficult recovery*

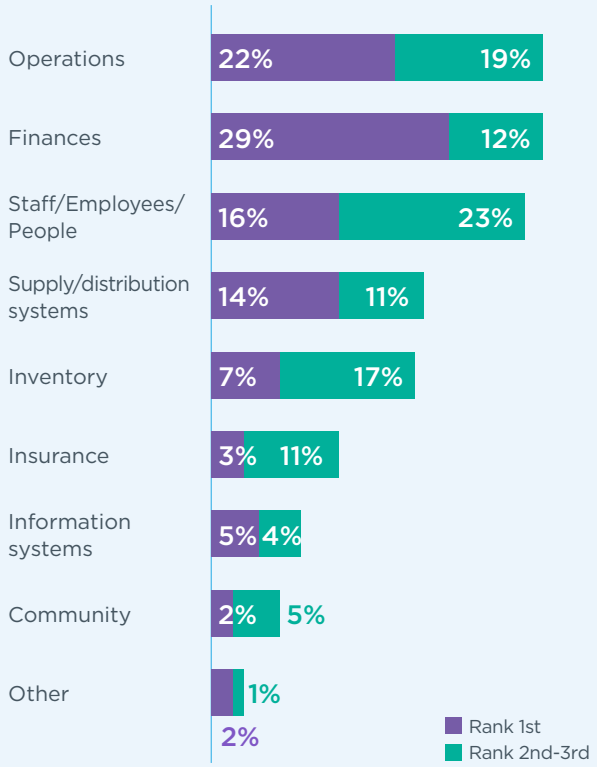
EXAMPLES OF PAST AND FUTURE STRATEGIC DISRUPTION:

- Significant changes in industry competitive dynamics, such as the effect of Amazon and others on brick-and-mortar retail
- The impact of demographic changes—such as Baby Boomer retirements and Millennials maturing—on the talent pool
- A change in company capital structure and ownership due to retirement or sale
- Major changes in regulations, international trade agreements, or macroeconomic conditions

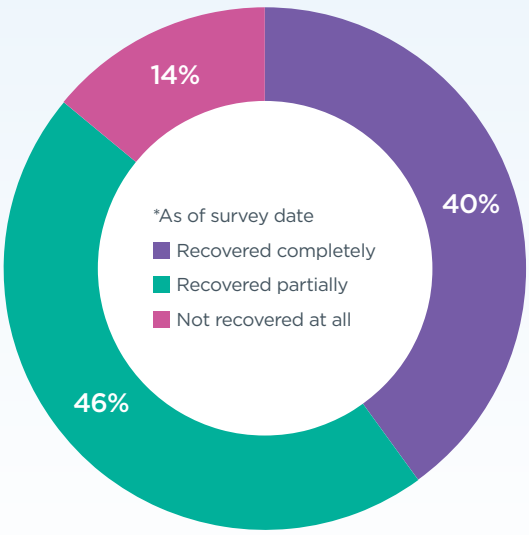
PREPAREDNESS



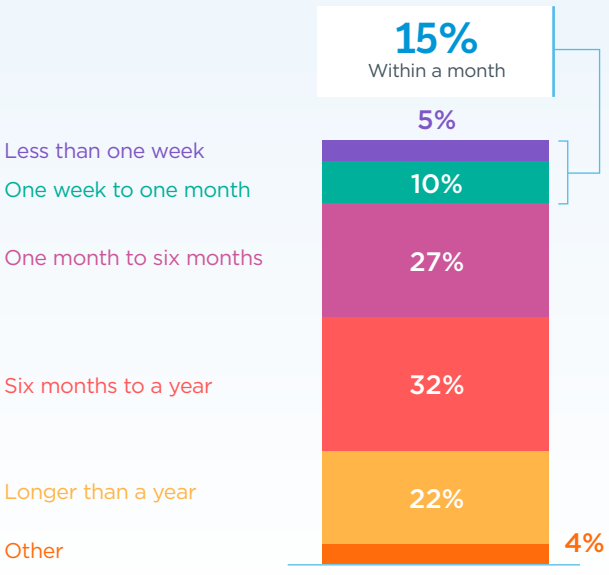
AREAS IMPACTED



DEGREE OF RECOVERY*

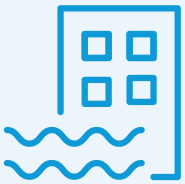


RECOVERY TIME



Operational disruptions are inconvenient—but usually manageable

One in five middle market companies has experienced an operational disruption in the past two years. Executives and companies are better prepared to handle these types of events than other kinds of disruptions, perhaps because there is a large body of knowledge about keeping processes under control and building redundancy into factories and supply chains. (Wholesalers, who stand in the middle of supply chains, report more impact from operational disruption than executives in other industries.) In some cases, companies can establish contingency plans or take actions to minimize damage in advance of an event, such as a storm. These efforts notwithstanding, operational disruptions have broad impact and are particularly likely to affect a company's employees. About half of companies say they recovered from their most recent operational disruption in a month or less, and 77% of businesses say they have fully recovered within two years.



» *Most prepared*

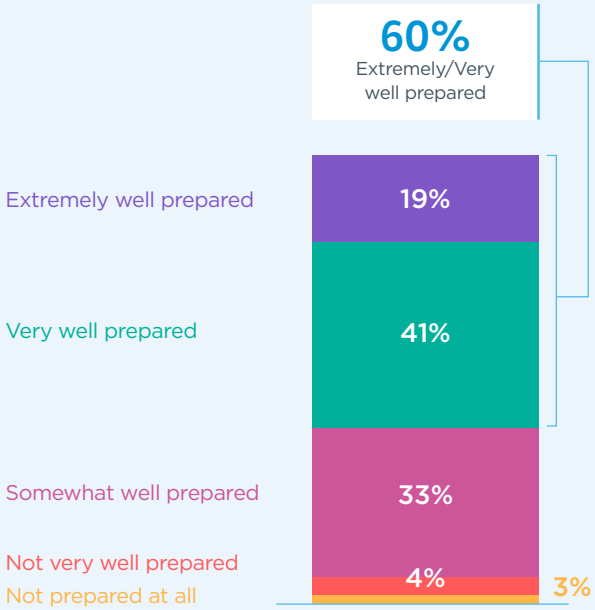
» *Most likely to recover from completely*

» *Impact is greatest on operations and people*

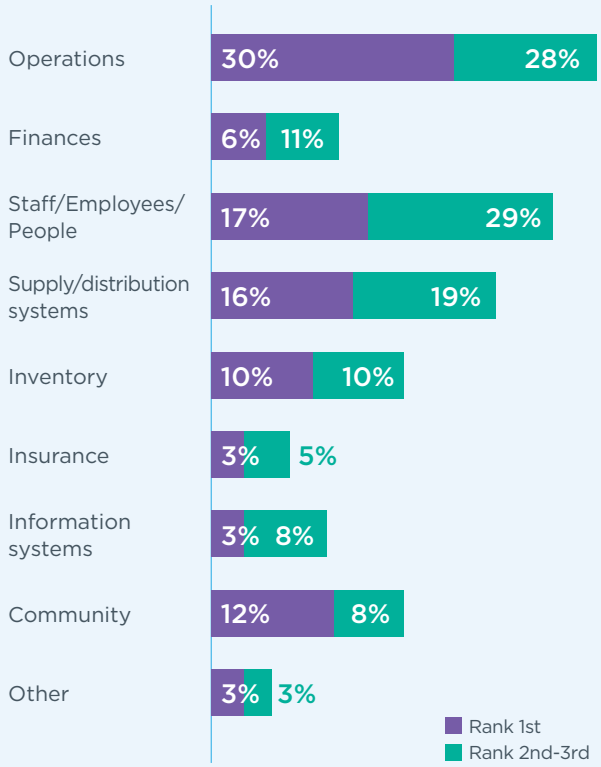
EXAMPLES OF OPERATIONAL DISRUPTION:

- Hurricanes, earthquakes, fires and other disasters
- Strikes or other labor actions
- Product recalls due to quality, safety, or health problems
- Supply chain breakdowns

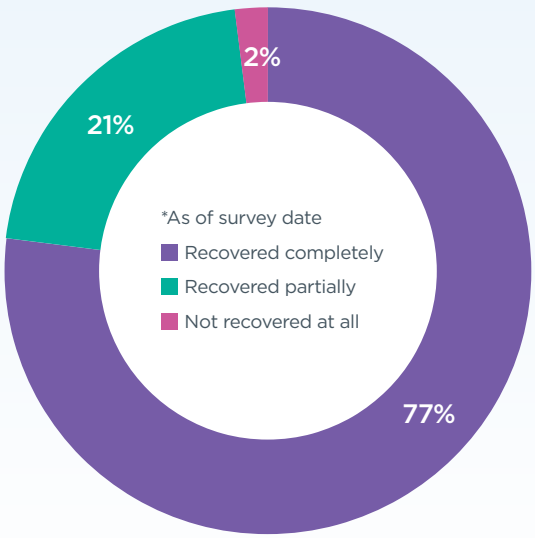
PREPAREDNESS



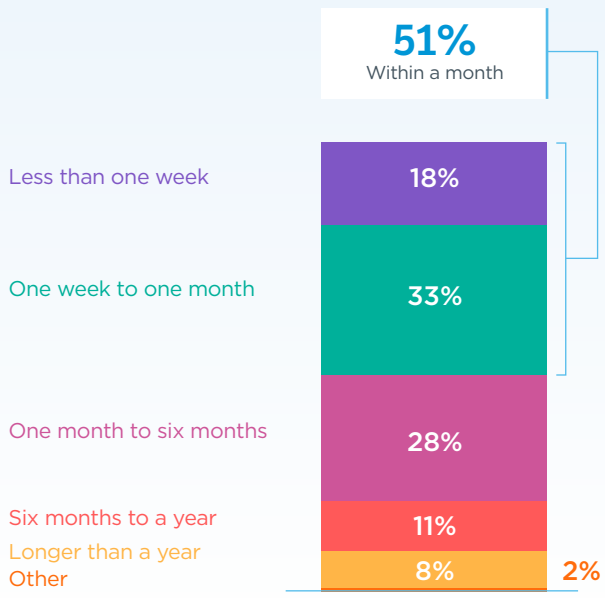
AREAS IMPACTED



DEGREE OF RECOVERY*



RECOVERY TIME



Digital disruptions demand immediate attention and quick resolution

Digital disruptions come in two basic forms: breakdowns in servers or systems caused by hardware or software failure; and cybersecurity attacks. Executives say digital disruptions are less common than strategic or operational problems. Digital disruption is almost certainly underreported, since evidence shows that, on average, it takes 200 days before a company realizes that its systems have been compromised due to an attack. Nevertheless, when a middle market company has been hit by malware or an intrusion, or when a server goes down, the event ignites a fire drill mentality, and people across the organization respond immediately. While just over half (54%) of businesses say they are very well prepared for digital disruptions, most companies recover completely and in short order: Two-thirds of firms say recovery takes a month or less; about three in 10 companies have the problem resolved within a week.

» *Least prevalent*

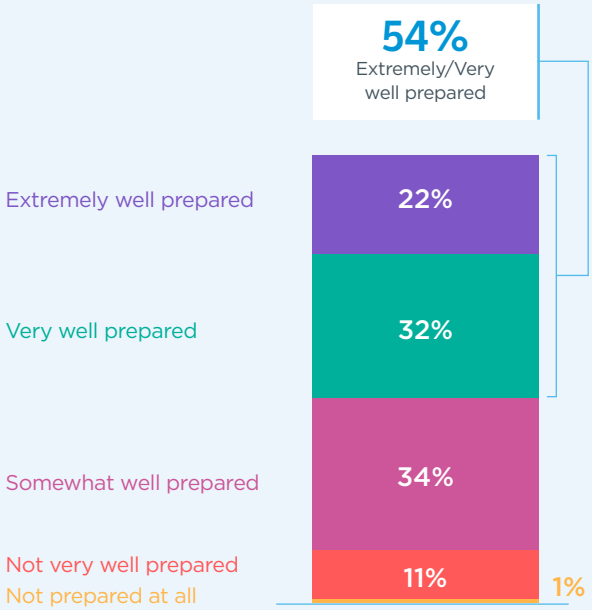
» *Quickest recovery*

» *Greatest impact on information systems*

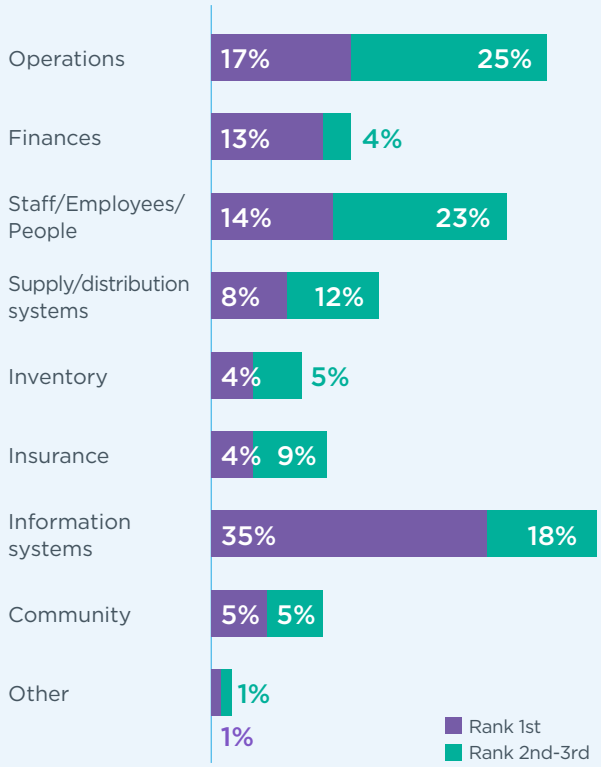
EXAMPLES OF DIGITAL DISRUPTIONS:

- Data breaches affecting a company, its employees, its customers, or its suppliers
- Widespread malware attacks such as 2017's "WannaCry"
- IT system failures like those that grounded hundreds of United, Delta, and British Airways flights in 2016 and 2017

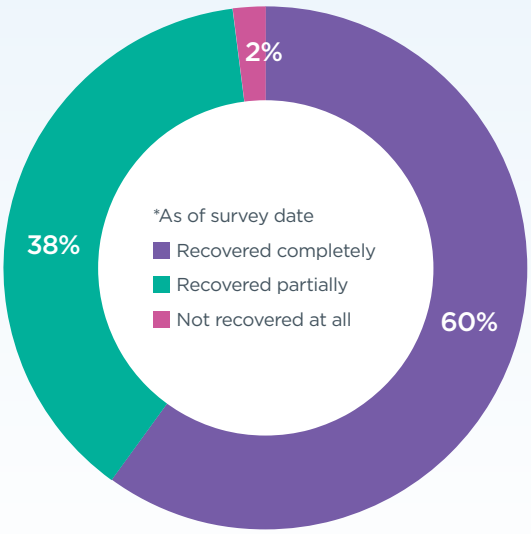
PREPAREDNESS



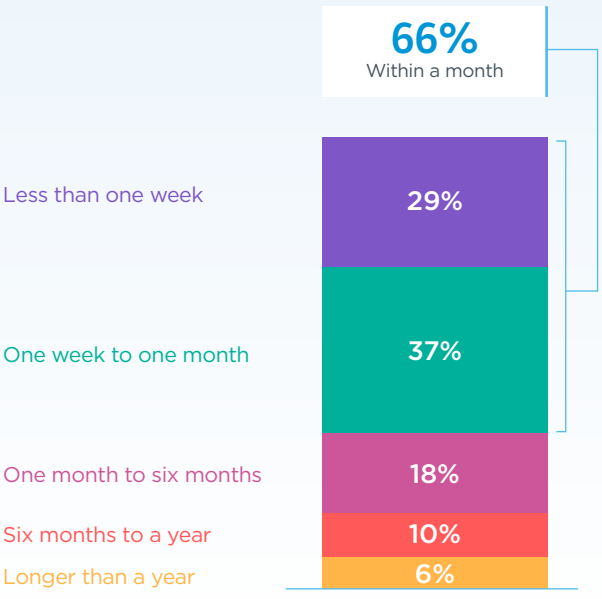
AREAS IMPACTED



DEGREE OF RECOVERY*



RECOVERY TIME



Disruptions have affected different regions in different ways

In the fall of 2017, major hurricanes hit Florida and Houston, Texas, while wildfires ravaged northern California. (Fires also affected southern California later in the year, but those events took place after the completion of our survey.) In the wake of these disasters, we asked middle market companies in all three areas to weigh in on their experiences.

TEXAS

Following Hurricane Harvey, Texas companies reported the most significant disruptions to operations and inventory. The impact on communities and people was relatively small, perhaps because the storm was localized. Albeit, Houston is a big location, but Harvey did not affect Dallas, west Texas, or other areas of the state. Industry mix plays a role as well: The petrochemical industries that cluster in south Texas are not labor-intensive, and the facilities are typically large complexes set off by themselves.

FLORIDA

While Florida businesses are no strangers to natural disasters and consider themselves more well-prepared for operational disruptions than their peers in other regions, Irma hit hard for companies in the state. This may be partially due to the sheer magnitude of the storm; it affected nearly the entire state from the Keys to Jacksonville. In addition, the industry mix is different in the Sunshine State where the economy is closely tied to tourism and transportation. It's not surprising that Florida companies experienced a greater impact on the community as the result of operational disruptions than businesses in other states and have recovered more slowly than those in Texas and California.

CALIFORNIA

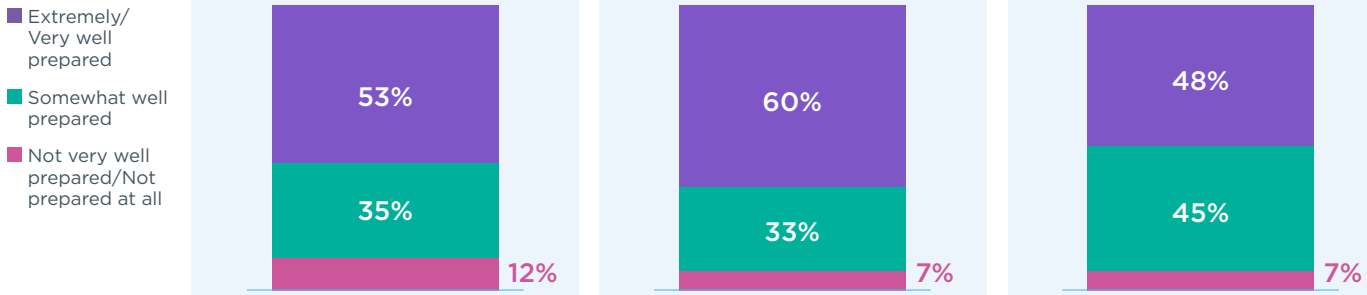
Northern California's wildfires mostly occurred outside metropolitan areas where major industries cluster; their impact on middle market businesses is hard to separate from other data. Overall, California businesses report suffering the most significant financial ramifications from cyber and data disruptions (nearly twice the impact on annual revenue than companies in other states), perhaps because of industry mix or because they are more aware of attacks that have occurred. California companies are also the least likely to recover completely from technology disruptions or breaches.

TEXAS

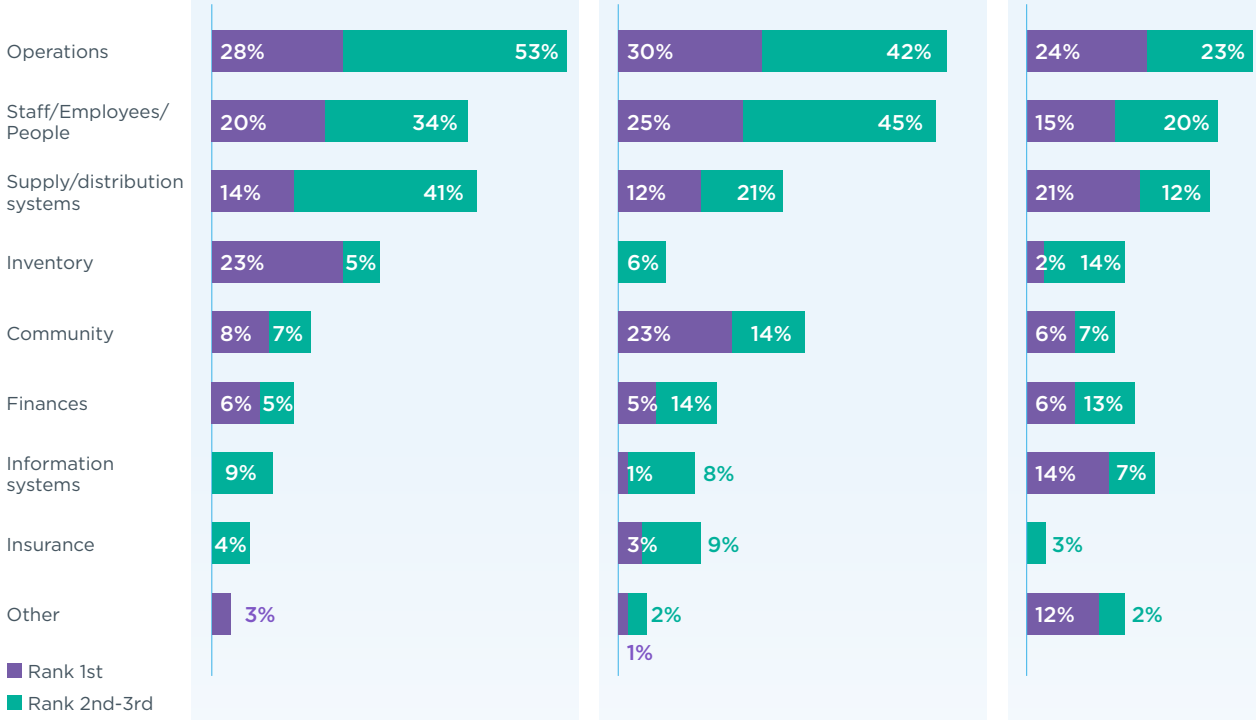
FLORIDA

CALIFORNIA

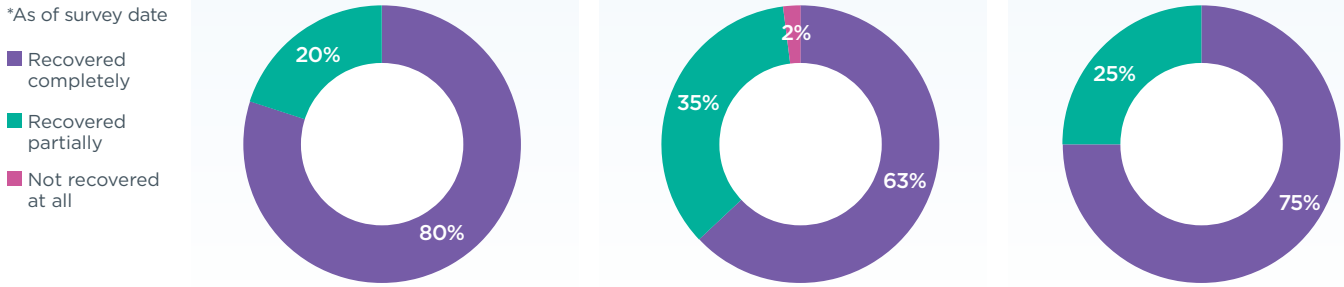
LEVEL OF PREPAREDNESS FOR OPERATIONAL DISRUPTION



BIGGEST IMPACT ON BUSINESS FROM OPERATIONAL DISRUPTION

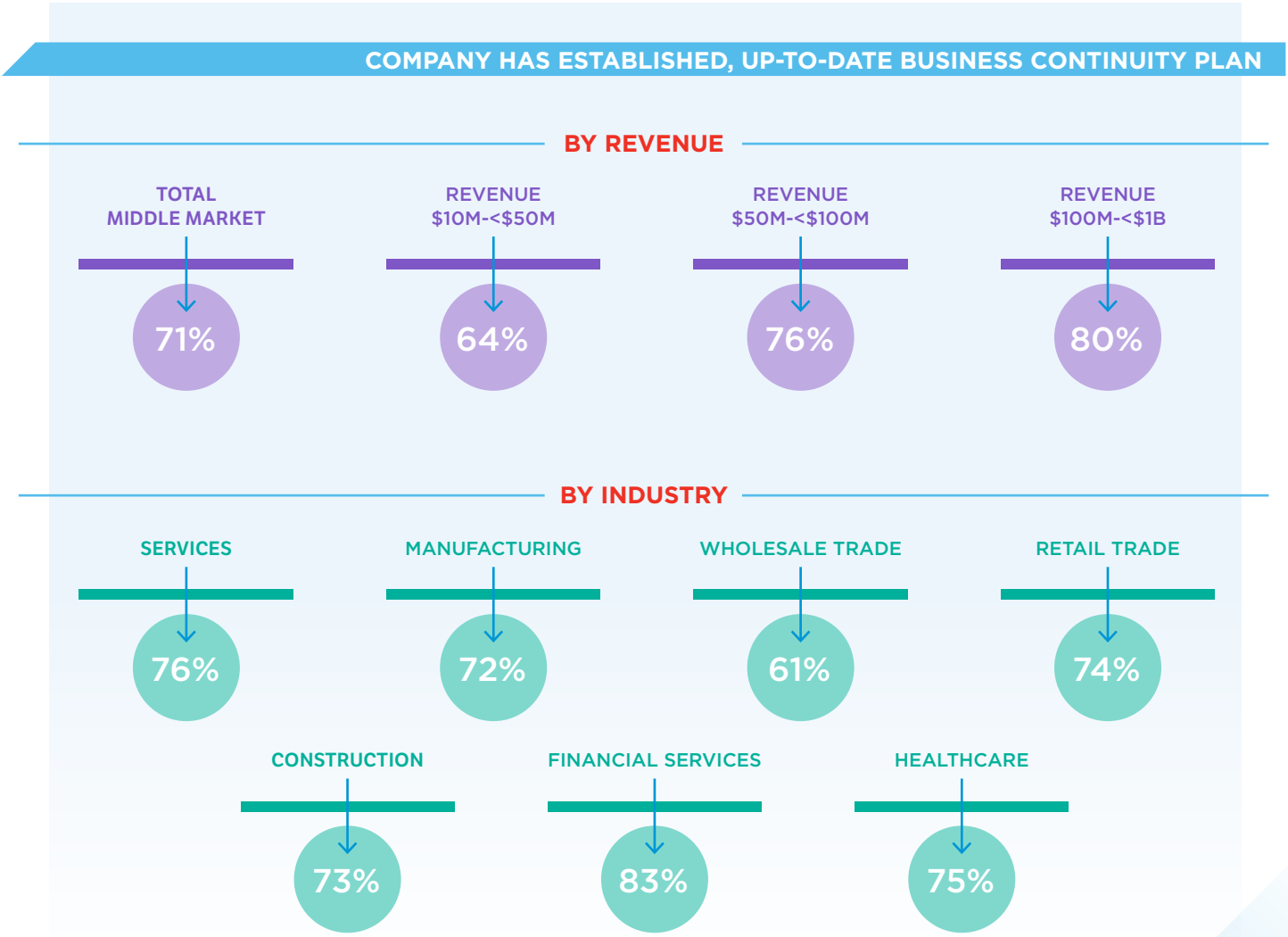


RECOVERY FROM OPERATIONAL DISRUPTIONS*



Larger businesses and financial services companies are most likely to have solid business continuity plans

A majority of companies do have a business continuity plan in place. These plans are most likely to include back-up power sources followed by alternate locations or facilities, especially among larger firms. A majority of manufacturers have alternate suppliers set up. While it is heartening to see that seven out of 10 middle market companies have business continuity plans in place, it is worth noting that they are less than comprehensive. Fewer than half of companies have contingency plans to make sure capital is available (such as an established line of credit); likewise, fewer than half have contingency plans for human capital, such as staff training.



Creating financial resilience

By Manuel M. Perdomo
Head of International Risk, SunTrust Banks, Inc.

In times of disruption, there is no greater importance than to have ample liquidity, for it provides the flexibility for actions that lead to recovery. While there is no substitute for preparations, access to cash on hand and to funding sources (lines of credit) are required to bridge back to normal.

It is understood that well run businesses have continuity plans, insurance, redundant facilities and information systems. They typically articulate these plans readily and even practice them with their workforce. Liquidity needs to be part of that plan.

Natural disasters have a unique effect upon human capital. The stress that is created by anticipation (in case of a hurricane) or by the sudden shock (earthquake, flash flood, etc.) and the aftermath brings out different reactions. Cash on hand for example can be used to support a stressed workforce and allow them to return to work sooner.

Designing and deploying robust information systems

By Joseph Muniz
Security Architect, Cisco

Cyber defense, at a high level, is addressing risk and resilience. Risks are malicious parties exploiting vulnerabilities before you remediate the weakness or enable proper defense to prevent exploitation. Resilience is avoiding a loss of available resources.

Reducing risk should include a layered defense strategy that uses different detection tactics. Tactics should be viewed as Before, During, and After an attack based on the cyber kill chain concept. “Before" means technologies that block communication to malicious sources, preventing any attempt to launch an attack. “During" focuses on detecting attack behavior, while “After" looks for attacks that have successfully breached a system. This approach should apply to all areas of physical, virtual, and cloud technologies.

Resilience is accomplished using high availability concepts such as redundant hardware and networking. Also, denial of service technologies should be considered to avoid targeted attacks designed to interrupt service. Ultimately, digital threats change and grow rapidly, which means that executives must ensure that risk and resilience efforts remain robust and up to date.

Understanding enterprise risk

By Adam Schrock
Managing Director, Grant Thornton

Risks are prevalent throughout your organization, and leaders inherently manage these risks within normal day-to-day business operations. Enterprise Risk Management (ERM) is a process that helps organizations move beyond coping with risks as they arise to a stage where they can proactively identify risks that could negatively impact business objectives. ERM will also help executive teams determine when to take risks in order to take advantage of an upside that can improve your performance or increase revenues.

In simple terms, ERM provides a top-down, holistic view of risks in order to effectively identify and manage threats to financial and strategic objectives. ERM seeks to move beyond the quantification of near-term potential losses to envision longer-term financial, strategic, operational, and people risks.

In today's world, effective ERM processes can benefit your organization in a number of ways. ERM will effectively balance risk and growth opportunities, such as digital strategies, technology innovation, and big data analytics. Striking the right balance allows your organization to transform into a risk-aware culture that protects the business, improves performance, and creates stakeholder value.

A framework for managing risk

Middle market companies can better prepare their business for all manner of business disruptions by developing a comprehensive plan to identify potential risks and prepare to cope with disruptions when they occur. This framework includes 1.) reconnaissance, or doing your homework to improve your ability to foresee and understand the risks you may face; 2.) building resiliency and redundancy into your business from a financial, human, and operational perspective; and 3.) establishing recovery plans so you know how to respond when something does go wrong.

	SHARPENING RECONNAISSANCE	IMPROVING RESILIENCE	PREPARING FOR RECOVERY
STRATEGIC	☐ Annual board-level assessment of known, known-unknown, and unknown-unknown threats: Industry changes, potentially disruptive technology, impact of megatrends, impact of outside factors (e.g., government)	☐ Review financial cushions, lines of credit and other sources of capital, preparedness, and relationships ☐ Review and strengthen key-person relationships and succession plans ☐ Review key customer/supplier relationships and contracts ☐ Create strategic options via R&D, M&A readiness	☐ Develop "fight or flight" plans to respond to most likely strategic risks ☐ Ensure long-term investor support ☐ Develop capability to create/execute restructuring plans
OPERATIONAL	☐ Annual board-level assessment of vulnerabilities to all operations from natural events, disruption in supply or distribution, etc. ☐ Include possible disruptions from and to communities in which you do business	☐ Review insurance ☐ Review banking relationships ☐ Build redundancy into key operations and supply chains	☐ Maintain an up-to-date business continuity plan ☐ Have plans in place for employees, business partners, and community ☐ Run fire drills
DIGITAL	☐ Annual board-level risk assessment and review of cybersecurity strategy and planning ☐ Real-time threat monitoring	☐ Ensure backups of all data either with own or cloud resources ☐ Fully train all employees ☐ Establish protocols for communication with vendors/customers/authorities ☐ Review and update legal risks ☐ Review and update insurance	☐ Have a disaster recovery plan ☐ Pre-identify internal and external resources needed for recovery ☐ Run fire drills

Resources

To learn more about potential business disruptions and how your organization can prepare, tap into the following resources from the Center and its sponsors.

STRATEGIC

Disruption Demystified and **Disruption Defanged** by Geoffrey Moore: How middle market companies can identify and cope with disruptive business models and technologies *http://middlemarketcenter.org/expert-perspectives/geoffrey-moore-strategy-guide-middle-market-company*

Growth Champions: Five investments top-performing middle market companies make to sustain growth over time *http://middlemarketcenter.org/middle-market-academic-research-summaries/framework-for-success-by-growth-champions*

Mastering Talent Planning: Frameworks for developing stronger, more engaged workforce, greater bench strength, succession planning, etc. *http://middlemarketcenter.org/research-reports/best-practices-middle-market-talent-planning*

Digitizing the Customer Experience: Are We There Yet? How middle market companies are integrating digital tools into customer touchpoints *http://www.middlemarketcenter.org/Media/Documents/how-middle-market-firms-integrate-customer-experience-digitization-in-their-business_NCMM_Digital_CX_Report_FINAL_web.pdf*

OPERATIONAL

The Operations Playbook: A framework for building more resilience into operations *http://middlemarketcenter.org/research-reports/the-operations-playbook-a-systematic-approach-for-achieving-and-maintaining-operations-excellence*

Working Capital Management: Techniques to free up resources and reduce dependence on outside capital *http://middlemarketcenter.org/research-reports/importance-of-working-capital-management*

The Perfect Link: How middle market companies manage supply chains up and down stream *http://middlemarketcenter.org/research-reports/middle-market-supply-chain-link-practices*

Supply Chain Resiliency Assessment *http://middlemarketcenter.org/supply-chain-resiliency-assessment*

Preparing for Supply Chain Disruption and "100-year events" by Prof. John Gray *http://u.osu.edu/riskinstitute/2014/07/09/preparing-for-supply-chain-disruption-and-100-year-events/*

DIGITAL

How Digital Are You?: Survey of the degree to which middle market companies have digitized business operations and planning *http://middlemarketcenter.org/research-reports/middle-market-digitization-trends*

Cybersecurity Resource Center: A curated collection of resources to keep up to date with recent trends in digital security *http://cybersecuritycenter.middlemarketcenter.org/*

Cybersecurity Audit: 39 questions that will help you gauge your cybersecurity preparedness *http://www.middlemarketcenter.org/Media/Self-Assessment/Cybersecurity-SelfAssessment.pdf*

The Risk Institute: Integrated Risk Management: 2017 survey revealing risk management best practices from among more than 500 companies of all sizes *https://fisher.osu.edu/sites/default/files/fcb_2017risksurveyfull_final_spreads.pdf*

About The U.S. Middle Market

The U.S. middle market comprises nearly 200,000 companies that employ 44.5 million people and generate more than $10 trillion in combined revenue annually. The middle market is defined by companies with annual revenues between $10 million and $1 billion. In addition to their geographic and industry diversity, these companies are both publicly and privately held and include family-owned businesses, sole proprietorships, and private equity-owned companies. While the middle market represents approximately 3% of all U.S. companies, it accounts for a third of U.S. private-sector GDP and jobs. The U.S. middle market is the segment that drives U.S. growth and competitiveness.

NATIONAL CENTER FOR
THE MIDDLE MARKET

The National Center for the Middle Market is the leading source of knowledge, leadership, and innovative research focused on the U.S. Middle Market economy. The Center provides critical data, analysis, insights, and perspectives to help accelerate growth, increase competitiveness, and create jobs for companies, policymakers, and other key stakeholders in this sector. Stay connected to the Center by contacting middlemarketcenter@fisher.osu.edu.

THE OHIO STATE UNIVERSITY
FISHER COLLEGE OF BUSINESS

From business as usual to business unusual, Fisher College of Business prepares students to go beyond and make an immediate impact in their careers through top-ranked programs, distinguished faculty and a vast network of partnerships that reaches from the surrounding business community to multinationals, nonprofits and startups across the globe. Our students are uniquely prepared and highly sought, leveraging Fisher's rigorous, experiential learning environment with the resources of Ohio State, a premiere research university with 500,000 proud Buckeye alumni.

SUNTRUST

SunTrust Banks, Inc. (NYSE: STI) is a purpose-driven company dedicated to Lighting the Way to Financial Well-Being for the people, businesses, and communities it serves. Headquartered in Atlanta, the Company has two business segments: Consumer and Wholesale. Its flagship subsidiary, SunTrust Bank, operates an extensive branch and ATM network throughout the high-growth Southeast and Mid-Atlantic states, along with 24-hour digital access. Certain business lines serve consumer, commercial, corporate, and institutional clients nationally. As of December 31, 2017, SunTrust had total assets of $206 billion and total deposits of $161 billion. The Company provides deposit, credit, trust, investment, mortgage, asset management, securities brokerage, and capital market services. SunTrust leads onUp, a national movement inspiring Americans to build financial confidence. SunTrust's Internet address is suntrust.com.

Grant Thornton

Founded in Chicago in 1924, Grant Thornton LLP (Grant Thornton) is the U.S. member firm of Grant Thornton International Ltd, one of the world's leading organizations of independent audit, tax and advisory firms. In the United States, Grant Thornton has revenue in excess of $1.3 billion and operates 57 offices with more than 500 partners and 6,000 employees. Grant Thornton works with a broad range of dynamic publicly and privately held companies, government agencies, financial institutions, and civic and religious organizations. "Grant Thornton" refers to Grant Thornton LLP, the U.S. member firm of Grant Thornton International Ltd (GTIL). GTIL and the member firms are not a worldwide partnership. Please see grantthornton.com for further details.

CISCO

Cisco is the worldwide leader in IT that helps companies seize the opportunities of tomorrow by proving that amazing things can happen when you connect the previously unconnected. At Cisco customers come first and an integral part of our DNA is creating long-lasting customer partnerships and working with them to identify their needs and provide solutions that support their success. Learn more at cisco.com.