

The Resilience Premium of Digital Business: A Gartner Trend Insight Report

Published: 24 May 2018 **ID:** G00348528

Analyst(s): Mark Thomas Jagers, Roberta Witty

Committing to resilience will equip your digital business with the mindset, resources and planning to recover from inevitable disruptions. Security and risk management leaders must deliver by building a culture of systemic resilience through viewing resilience as a premium and not as a cost.

Opportunities and Challenges

- Customer trust in an organization can be irreparably damaged by digital disruptions.
- Cyberattacks and system failures negatively impact revenue, productivity, brand reputation and reliability of digital business systems, which is especially detrimental to digital business initiatives, where the 24/7 operation of services is a mandatory element of success.
- Organizations have neglected the design of software systems for reliability and recoverability in favor of dependence on underlying technologies.
- Leaders create new opportunities by identifying cultural attitudes that impede work and talent from forming competencies for resilience.

What You Need to Know

People are the root of resilience, as an organization's success forms in its ability to handle adversity while maintaining adequate performance levels, and to resume to a "new normal" state of operations. Systemic resilience is critical, and leaders should ensure that systems can adjust functioning in anticipation of, during, or following internal and external events in order to sustain an acceptable level of required operations under both expected and unexpected conditions. Resilient infrastructure sustains perturbations, yet leaders should aim to maintain a level of adaptive capacity within the infrastructure to restore its structure and capabilities to the same or new levels of operational requirements.

Insight From the Analyst

Resilience in Digital Business Is Not Simply an Expense, but a Premium That Can Yield Dividends



Mark Thomas Jaggers, Research Director



Roberta Witty, Research VP

Although this is a world of inevitable disruption, resilience is often viewed as an expense. Business leaders account for it as a cost center — money to cover response recovery and restoration expenses if disaster strikes. Organizations perform limited resilience functions, sometimes only when regulations require. Such actions are deeply flawed.

Leaders who seek to guide digital business initiatives should reorient their view of resilience. Resilience must be held as a premium — as incentive, objective and capability; to attain resilience is to elevate a business's value. Leaders should view resilience through a lens of profits generated. It should be an ongoing concern of the workforce, as resilient organizations can turn potential disasters into beneficial situations.

As clients expand their digital business engagement, we've committed to researching what resilience means to organizations today. The Oxford Dictionary definition is blunt: resilience is "the capacity to recover quickly from difficulties; toughness." We wanted to go further as we recognized different layers of organizational resilience.

The most influential agents of resilience are people. Leaders can now be proponents of resilient practices and investments. A resilient culture helps reinforce the organization's abilities to maintain its commitments to customers or citizens. Staff of differing backgrounds and work styles can use their collective strengths to carry the business through an outage.

Also important are resilient infrastructure and processes that quickly restore structure and capabilities while adapting to operational requirements. By exploring each layer of resilience, we describe the practices and resources that organizations can use for resilient digital business engagement.

Executive Overview

Definition

Success rests on the ongoing resilience of business operations across the entire organization, supplier and service delivery ecosystem. Disruptions are uncontrollable, unpredictable, inevitable

and full of consequences. They range from large-scale events to smaller-scale, but increasingly frequent, errors and malfunctions. Any of these incidents can halt your operations. Speculation rushes like a flood tide across social media and cable television, misleading both the public and staff about the true risks facing the organization. This inevitability can be survived, however. Organizational resilience is a priority of the growing need to provide 24/7 services to support digital business and customer-facing services. It is a commitment that requires planning, transparency, flexibility, creativity and, above all, a preservation of business goals.

We have defined organizational resilience in numerous contexts. Cultural resilience represents the capability of a group to handle adversity while maintaining adequate performance levels, and then to resume to a new normal state of operations. A system is resilient if it can adjust its functioning prior to, during or following internal and external events — be they changes, disturbances or opportunities — and thereby sustain required operations under both expected and unexpected conditions. Resilient infrastructure withstands incidents not without performance impacts, but nonetheless can be quickly restored in terms of structure and capabilities while adapting to operational requirements. A cyber resilient organization ensures that rapidly restored software and technology infrastructure/services are reliable, safe and accessible, despite hostile or adverse disruptions of all types to those ecosystems. It is important to express that resilience is not only being "robust" — a term often used in technology discussions. Robust resources are susceptible to various stresses, especially unknown stresses. Resilience contends with the complexity and unpredictability that digital business represents, allowing the organization to return to stability without slowing down its operations. Speed remains a valuable characteristic of resilient digital businesses.

For organizational resilience, we offer a definition that establishes how leaders and employees should aspire to respond to outages:

Organizational resilience is the ability of an organization to resist, absorb, recover and adapt to business disruption in an ever changing and increasingly complex environment to enable it to deliver its objectives, and rebound and prosper (a slightly modified version of the ISO 22316:2017 definition).

The internal and external drivers of organizational resilience are shown in Figure 1.

Figure 1. Organizational Resilience Drivers



Source: Gartner (May 2018)

Research Highlights

Organizational Resilience Overview

Organizational risks range from natural disasters to man-made disruptions, equipment failure (IT, Internet of Things, operational technology, physical) and operational errors. These risks are occurring at an increasing frequency and turning into business disruptions that impact the viability of the organization. The World Economic Forum's annual global risk reports have tracked five types of organizational risks — economic, environmental, geopolitical, societal and technological — for over 10 years. The diversity and ubiquity of these risks bring about an evolution in organizations that intend to thrive in such conditions. It is now obvious that the characteristics of a resilient

organization are impossible to implement in a business environment focused on short-term benefits only.

When trying to increase the resilience of systems and technologies, many organizations find that they've optimized their abilities to handle some failures, and increased the likelihood of a new and different type of failure occurring ... When there's an unexpected failure, the teams responsible for day-to-day operations are unable to handle the events, because it exceeds their understanding of the system.

Leaders must anticipate disruptions and prepare the organization to return to stability in a short time. The complexity of digital business makes preparations especially difficult. A resilient digital organization requires orchestration across business and technology domains. The following research defines and provides an overview of organizational resilience, the delivery model, how it affects application architecture and the potential downside risks.

Related Research

"Organizational Resilience Defined: It's More Than the Latest Trend": Organizational resilience is a strategic imperative and an organizational capability. Security and risk managers must work with the whole organization to deliberately design, implement and maintain resilience characteristics to ensure that digital business initiatives become sustainable operations.

"The Organizational Resilience Program Delivery Model": A well-defined and implemented delivery model is required to ensure a strong organizational resilience program. This delivery model includes four components: program management, management discipline scope, risk identification and management, and governance and accountability framework.

"Delivering Resilience and Recoverability for Distributed Transactions Poses a Whole New Challenge": For over 40 years, traditional database engines have given transactional systems phenomenal resilience. But as digital business software embraces heterogeneous distributed transactions and microservices, application leaders need new means of ensuring data and process integrity.

"There's a Downside Risk to Resilience": By trying to increase system resilience, infrastructure and operations (I&O) leaders who are planning and enabling infrastructure delivery can increase costs

with little or no benefit, and worsen the potential impact of failures. Organizations should focus on best practices to align potential impacts with the costs of improvement, reduce the potential damage propagated during cascade failures and understand the harm-versus-reward potential.

Guide People to Maintain Resilient Mindsets and Prioritize the Organization's Ability to Endure

People are the most active element of an organization's resilience capability. They contribute to problem identification and planning, they anticipate challenges, and their collaboration strengthens the organization's responsiveness by magnitudes. The willingness of each contributor — every contractor, staffer and executive — to prepare the organization to uphold its performance, no matter the disruption, must be in place. The very culture of the enterprise should hold organizational resilience as both an operational ideal and a fundamental trait.

It is clear that digital businesses require the involvement of people to recognize situations and take corrective action to achieve true system resilience.

Individual resilience — and group resilience — in a digital business context involves the capability to return to operational stability. As leaders display a new appreciation for resilience needs in digital business initiatives, successful executives and managers must advocate for resilient practices in each department's functionality. Training, empowerment and accountability to resilience efforts must be prime aspects of each employee's experience. Associates and partner staff who appreciate their contributions to the enterprise's resilience will be actors in the response to a disruption.

Our research expresses the significance of resilience as a human skill, a professional outlook, a cultural value and a role objective.

Related Research

"Organizational Resilience: Create the Teams That Plan and Respond Best": The ability to recover swiftly and gracefully from adverse events requires teams that can anticipate and then respond. CIOs should create teams that capitalize on the team members' strengths, while ensuring that there is enough diversity to bring the creativity and innovation needed.

"Focus on Your People and Culture to Achieve Resilient Digital Infrastructure Delivery": In planning and delivering resilient digital infrastructure, people are as important as infrastructure and processes. I&O leaders must create a culture that prioritizes resilience over remediation by emphasizing continuous process improvement to maximize continuity of delivery and minimize downtime.

"Build Resilience in Your Workforce Through Succession Planning and Management": Faced with ever-more competitive talent markets and aging workforces, CIOs must respond to disruptions and manage workforce-related risks to sustain performance. This research guides CIOs to establish succession planning and management, and build workforce resilience for the digital business future.

"Reimagine Apprenticeships to Develop Talent to Scale Digital Business": Digital business exacerbates the need for critical skills and competencies. A reimaged form of apprenticeships can groom existing employees, but CIOs will need to build a program tailored to information and technology needs that unleashes the abilities of all employees of the organization.

"Boost Resilience and Deliver Digital Dexterity With Cyber Ranges": Security and risk management leaders responsible for cybersecurity should consider the different use cases for a cyber range. Our analysts explain how organizations can foster new skills and competencies to increase organizational resilience and manage the new risks of digital business.

"Don't Let Your Culture Derail Your Diversity Efforts": A culture of homogeneity will quash diversity and inclusion programs. This research provides insights so application leaders can both spot the cultural defenses obstructing inclusive ways of working and identify actions they can take to let diverse talent bloom.

"The #DigitalSociety Requires a Digital Social Contract": Being part of the digital society is a given. As a result, in addition to a customer value proposition, digital businesses must have a societal value proposition. A social contract is the set of common, explicitly or implicitly understood principles that describe how we feel our society should work. The basic idea of the social contract is that, by living in a society, we have made exchanges that benefit us individually or as a whole. This research helps leaders understand how to uphold this negotiation.

Use Process to Create Primary Business Functions That Are Resilient and Prepare the Organization to Respond to Disruptions

Business leaders and IT professionals must create resilient practices in a dynamic environment. Process represents one of the best methods to meet the "always on, from anywhere" expectations of customers and the workforce.

Organizational resilience is not synonymous with IT disaster recovery (IT DR) nor BCM. And organizational resilience cannot emerge from one department and not

another. It must become standard operating procedure and be built into day-to-day operations.

As digital businesses turn to vendors as deliverers of services — from primary business functions that require resiliency or resilient technologies — the relationships between organizations and service providers grow more crucial, and increasingly complex. Technology alone will not protect the providers and the enterprise, whether from their own carelessness or malicious actors. Due diligence is an important effort; organizations should always be assessing a vendor's contribution to the partnership's overall resilience.

Process is key to a resilient infrastructure, which sustains perturbations without foreseen performance impacts. With well-designed processes in place, the enterprise quickly restores its structure and capabilities while adapting to the same or new levels of operational requirements.

Given that the lines between personal and business technology are blurring, enterprises should also consider extending protections to vendor employees at home. This research explores the process requirements of a sound resilience program.

Related Research

"Maverick* Research: Building Corporate Resilience and Restoring Faith in Facts in the Fake News Era": Fake news and misinformation expose enterprises to much more than reputational damage. Here, we highlight the risks they face and provide practical steps that CIOs can take to protect their companies. (Maverick research exposes unconventional thinking and advice.)

"Ensure Digital Business Resilience Through Better Risk Management Planning": Enhancing your business through digital transformation needs a different approach to risk planning. Security and risk management leaders must consider impacts to organizational responsibilities and external relationships, and reflect potential impact of new participants, new technologies and process changes to digital business resiliency.

"Infrastructure Resilience Debt: Pay Now or Pay Later, but Manage Your Debt": Just as financial debt borrows from the future to fund the present, infrastructure resilience debt borrows from tomorrow to deliver results today. In the context of digital business, infrastructure resilience debt comes with demanding and changing dynamics that I&O leaders must understand and plan for at the design stage and throughout their ongoing support for the infrastructure.

"Improve Operational Resilience Through a More Collaborative Incident Response Process": Organizations and business users benefit when security and risk management leaders coordinate an approach to managing incident response and resolution. Harmonized incident response facilitates collaboration, utilizes shared systems and reduces response times to improve operational resiliency.

"Ensuring Workforce Resilience Through Travel Risk Management Best Practices": Travelers face constant disruption through device losses, theft, loss of communications and seizure at borders. Gartner promotes resilience best practices to help end users keep the business process running, no matter what happens.

"Design Resilience Into Your Supply Chain With Scenario Planning to Weather the Unexpected": Gartner's supply chain research shows the security of connected facilities and assets, and that of digital products, was perceived as the top challenge for digital business. Scenario planning helps build this resilience by negotiating a path between the false certainty of a single possible outcome and paralysis by analysis. Our research describes how to secure the best outcome for now while preparing good alternate options to rely upon depending on how the situation unfolds.

Deploy Technology That Minimizes Disruptions or Continues to Support Business Initiatives Despite Disturbances

Increased interdependence among people, things and enterprises creates new opportunities and risks for organizations venturing into this new digital business delivery model. While the digital business ecosystem is new, the technologies involved with information and communications are more familiar to IT departments. However, the growing need to provide 24/7 technology services to support digital business and customer-facing services is placing additional pressure on the IT department. From a technology perspective, organizations must practice resilience in depth, allocating for different capabilities at independent layers of the technology infrastructure stack, from applications to network.

Failures anywhere in the ecosystem can have a cascading and detrimental effect on the performance of the entire workflow, preventing subsequent tasks from occurring.

Infrastructure resilience competes with other aims of IT leaders, who seek efficiency and usability in their resources. For instance, leaders are often actively working to simplify and homogenize their suppliers and their operation processes. This intent is seemingly at cross purposes with resilience; while this makes environments easier to manage and more cost-effective, homogeneity might make disruption more likely through cyberattack. Infrastructure grows more fragile as commonality grows among the overall IT system cohort.

As the following research suggests, however, several options allow for enhanced awareness of technology performance and responsiveness during and after an incident.

Related Research

"Resilient IT Infrastructure Delivery: Find Weaknesses in Service Delivery": I&O leaders must deliver resilient digital infrastructure. However, blind spots are inevitable due to the depth, breadth and scale of the systems they're responsible for. This research identifies top recommendations for finding and mitigating resiliency blind spots.

"Delivering Resilient Digital Infrastructure: Don't Let Technology or Systems Become Liabilities": Resilient IT infrastructure requires not only the right technology, but also the correct implementation of that technology. From the outset, I&O leaders must plan their overall processes and systems around multiple methods of delivering services to achieve sustainable, cost-effective resilience.

"How to Reduce Network Downtime in the Era of Digital Business": Network outages negatively impact revenue, productivity and brand reputation, and are increasingly impactful as organizations implement digital business initiatives. Our analysts identify how I&O leaders responsible for networking can reduce the number and duration of network outages.

"Reimagining Security and IT Resilience for a Cloud-Native DevSecOps World": Resilient organizations require resilient infrastructure, including security infrastructure. Security and risk management leaders should use the shift to rapid cloud-native application and development architectures as a catalyst to rethink legacy security infrastructure and processes — with a result of improved security and resilience.

"A Guidance Framework for Architecting Highly Available Cloud-Native Applications": Application architects must design the availability of service capabilities into their production cloud applications. Cloud service providers give you a jump-start to meeting SLAs but do not guarantee application uptime. Follow this guide to architect high availability into your cloud applications.

"Resilient and Robust Availability Solutions for Database Management Systems": I&O leaders can choose robust or resilient approaches for DBMS availability. Resilient approaches are typically less costly, but a combined approach may offer maximum availability. Organizations need to make cost-effective technical decisions for implementing an availability solution.

"Prepare for the Inevitable: Resilience Enabled by 3D Printing": CIOs understand the need for IT resilience. However, their IT organizations will also be intimately involved with manufacturing's recovery from a continuity event. Our research assesses how 3D printing enables manufacturing's resilience while raising critical IT support issues.

"Will Hybrid Cloud Infrastructure Offerings Improve or Impair Enterprise Resilience?": Many major vendors are starting to roll out hybrid cloud infrastructure platforms. Nascent products are varying drastically in their implementations and objectives. In this research, we will evaluate the impact of hybrid cloud platforms on resilience capabilities within the enterprise.

"Satellite Communications Strengthen Operational Resiliency Planning": Near-global availability of broadband satellite service now makes it an essential element in infrastructure resilience. Satellite data and voice links can supplement or rapidly replace unavailable terrestrial network services, helping I&O leaders mitigate risks of disruption to digital business.

"How to Plan for Resiliency in the Cloud": Public cloud computing offers high reliability and resiliency, but this can't be taken for granted. Security and risk management leaders need to understand the features and administrative mechanisms specific to each of their strategically significant cloud services to ensure appropriate utilization.

Take Action to Increase Organizational Resilience

It is not enough to merely consider the risks facing an organization and layers of resilience that may serve it through a crisis. A leader must commit to action. Implementation of organizational resilience practices and policies is an expansive endeavor that requires various skills. Diplomacy, strategic thinking, negotiation and communication are just some of the areas in which leaders must show competence. Writing security incident response plans is a different process from acquiring SaaS resources, yet the leader must understand how to execute each activity to make the organization more resilient.

The digital society cannot be designed; it emerges as the result of all the digital interactions between people, organizations and things. Parts of those interactions are triggered by you. You are part of the digitalization of society, thus are responsible for making a positive contribution.

When using our research, leaders should recognize the two sources of force putting pressure on the organization to be resilient: internal and external. Internal forces are those that are moving the organization to transform and deliver successful digital business initiatives. External forces are ever present, and changing and pushing in on the organization. Resilience programs need to address both internal and external forces across all five layers of the organizations, such that mitigation controls are implemented to reduce the risks while allowing the organization to move forward on its growth trajectory.

This research covers several functions that will become essential pieces of the effort to make a business resilient.

Related Research

"Build Your Security Incident Crisis Communication Playbook": It is bad enough to have to deal with the confusion of a security incident. The situation quickly becomes complicated by the potential internal and public relations difficulty pouring out of the security incident. As a result, internal confusion can reign as employees and partners act on incorrect or partial information. Our analysts

describe the key practices that allow leaders to communicate to employees and consumers the causes and responses of a disruption.

"Provider Selection Criteria for Outsourcing Agile Application Development to Avoid Imminent Failure": Three areas of preparation are crucial to avoiding imminent failure of software performance: assessing internal competencies, defining governance and selecting the right supplier. Failing to complete such preparation before sourcing agile services will impact how you measure progress, control product quality and address provider support. This research guides sourcing and vendor management leaders to manage these risks, contain total cost of ownership and deploy software on schedule.

"Evolving IT Resilience Service Levels Into the Public Cloud": IT resilience service-level management is a nascent discipline. Evolving its coverage scope into the public cloud can be even more of a challenge. The cloud transition experience of a global entertainment company provides I&O leaders with insight regarding a practical set of first steps.

"Toolkit: Agile SaaS Acquisition Using Gartner's Triage Methodology": The Gartner triage method enables SaaS acquisition with agility and speed, while managing risk. This resource demonstrates how sourcing and vendor management leaders focused on technology procurement can expedite business capability by utilizing the triage method for review and negotiation of SaaS agreements.

"5 Ways of Dealing With Dualities in the #DigitalSociety": Digital innovation and transformation on the societal level work different than on the business level. Society is based on dualities. CIOs developing innovative business models need to dream big and adopt five next practices, such as embracing diversity and taking responsibility for externalities.

"Prepare for the Inevitable With an Effective Security Incident Response Plan": A serious security incident is a question of "when," not "if." This reality makes developing effective response plans a critical concern for any CISO. Security and risk management leaders should include both technical and nontechnical resources in incident response preparations.

Related Priorities

Table 1. Related Priorities

Priority	Focus
Risk Management Program	Risk management programs mitigate the impact of uncertainty on business performance. Gartner recommends an integrated risk management (IRM) approach to build and sustain successful risk management.
Building and Sustaining Dependable Infrastructure	Building and sustaining dependable infrastructure focuses on what is needed to support mission-critical infrastructure, applications and operations.
Information Security Management Program	Information security management is the discipline of designing, implementing and maturing security practices to protect critical business processes and IT assets across the enterprise.
Managing Vendor Performance and Risks	Gartner research on managing vendor performance and risk reveals the best practices for assessing, monitoring, and managing vendor performance, risks and relationships in pursuit of business goals.
Security Compliance and Audit Management	This initiative covers the planning and execution of security-related compliance activities and improving the digital risk coverage of the internal audit program.

Source: Gartner

Gartner Analysts Supporting This Trend



[Christie Struckman](#)



[Earl Perkins](#)



[Traverse Clayton](#)

Related Resources

Webinars

["Recover From Digital Business Disruption With Resilience"](#)

Gartner Recommended Reading

Some documents may not be available as part of your current Gartner subscription.

"Advance Your Application Performance Monitoring Strategy to Support Microservices"

"Driving Digital Business Transformation for Industry Leadership: An IT Perspective"

"Calculating the Total Cost of Your Digital Strategy"

"How to Assess Your Application to Adopt Cloud-Native Architecture"

"Methods to Achieve High Availability for Traditional Applications on Microsoft Azure"

"Hype Cycle for Business Continuity Management and IT Resilience, 2017"

GARTNER HEADQUARTERS

Corporate Headquarters

56 Top Gallant Road
Stamford, CT 06902-7700
USA
+1 203 964 0096

Regional Headquarters

AUSTRALIA
BRAZIL
JAPAN
UNITED KINGDOM

For a complete list of worldwide locations,
visit <http://www.gartner.com/technology/about.jsp>

© 2018 Gartner, Inc. and/or its affiliates. All rights reserved. Gartner is a registered trademark of Gartner, Inc. or its affiliates. This publication may not be reproduced or distributed in any form without Gartner's prior written permission. If you are authorized to access this publication, your use of it is subject to the [Gartner Usage Policy](#) posted on gartner.com. The information contained in this publication has been obtained from sources believed to be reliable. Gartner disclaims all warranties as to the accuracy, completeness or adequacy of such information and shall have no liability for errors, omissions or inadequacies in such information. This publication consists of the opinions of Gartner's research organization and should not be construed as statements of fact. The opinions expressed herein are subject to change without notice. Although Gartner research may include a discussion of related legal issues, Gartner does not provide legal advice or services and its research should not be construed or used as such. Gartner is a public company, and its shareholders may include firms and funds that have financial interests in entities covered in Gartner research. Gartner's Board of Directors may include senior managers of these firms or funds. Gartner research is produced independently by its research organization without input or influence from these firms, funds or their managers. For further information on the independence and integrity of Gartner research, see "[Guiding Principles on Independence and Objectivity](#)."