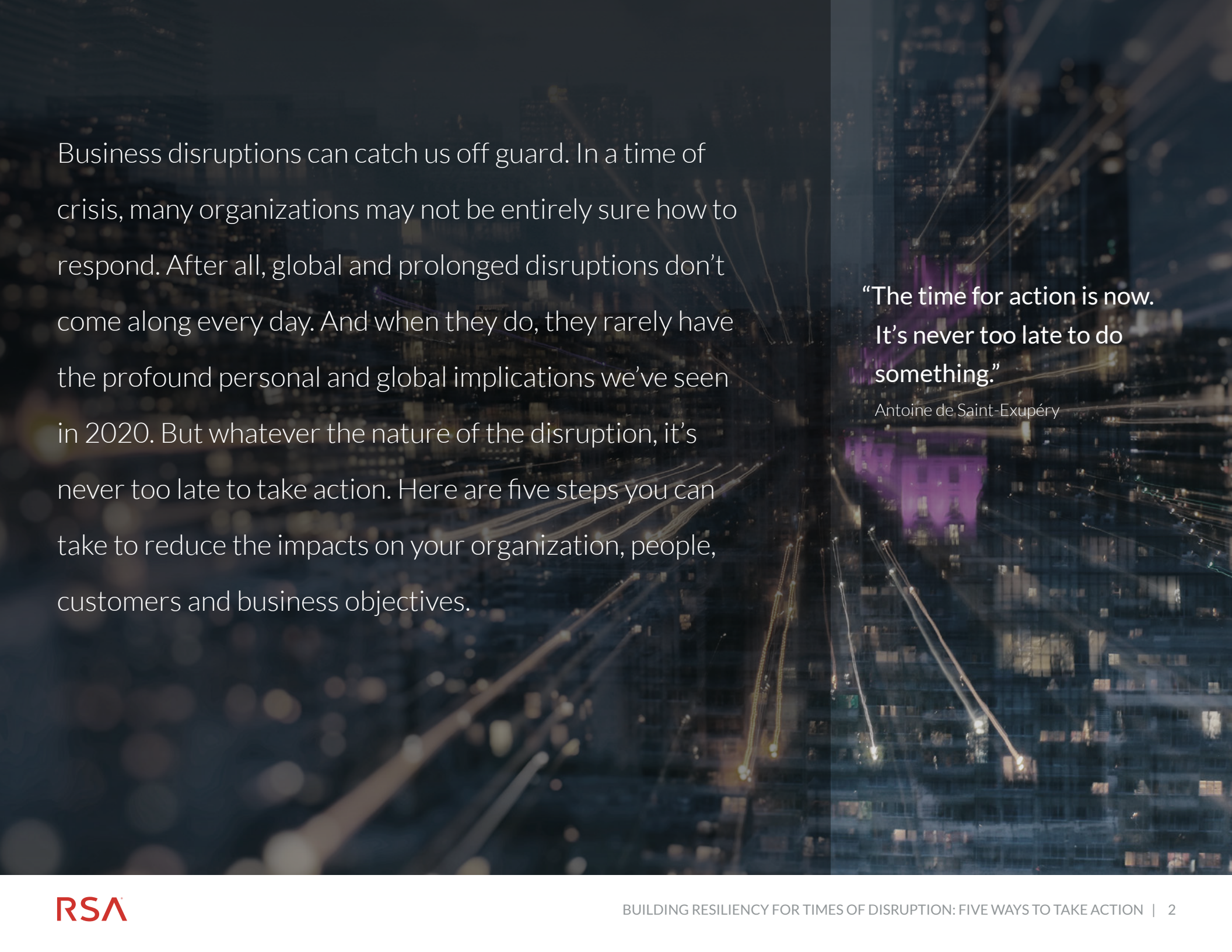


RSA

A lighthouse stands on a rocky cliff, with waves crashing against its base. The entire scene is overlaid with a red tint. The lighthouse is on the left side of the image, and the waves are on the right. The sky is dark, and the overall mood is dramatic and resilient.

# BUILDING RESILIENCY FOR TIMES OF DISRUPTION

Five Ways to Take Action



Business disruptions can catch us off guard. In a time of crisis, many organizations may not be entirely sure how to respond. After all, global and prolonged disruptions don't come along every day. And when they do, they rarely have the profound personal and global implications we've seen in 2020. But whatever the nature of the disruption, it's never too late to take action. Here are five steps you can take to reduce the impacts on your organization, people, customers and business objectives.

**“The time for action is now.  
It's never too late to do  
something.”**

Antoine de Saint-Exupéry

# STEP 1: IMPLEMENT RESPONSE AND RECOVERY PLANS

Now, more than ever, is the time to have [response and recovery plans](#) that enable your organization to react, adapt and recover from disruption. Response and recovery plans should be designed to:



Protect your people and enable them to do their jobs and support recovery of the business

---



Maintain (and recover, if needed) critical functions and supporting systems, locations and data

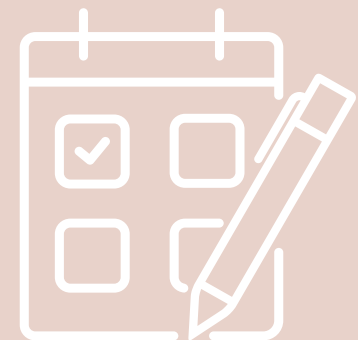
---



Ensure critical third parties are providing the level of service your organization needs, or make alternative plans if possible

## Case in Point: CDC Resources for Pandemic Planning

If you don't have response and recovery plans for large-scale disruptions such as a pandemic, take a look at this [pandemic planning template](#) from the Centers for Disease Control and Prevention (CDC). You can input this content into the [RSA Archer® Business Continuity & IT Disaster Recovery Planning](#) use case, adapt the plans and activities to your organization's situation, and begin to manage your response and recovery right away.



## STEP 2: EFFECTIVELY MANAGE THE CRISIS EVENT

Crisis response teams are responsible for leading their organizations successfully through business disruptions – quickly making response decisions, enabling the organization to take appropriate action, communicating efficiently and coordinating with business recovery teams. It's vital to keep the organization and extended ecosystem informed and acting in lockstep with each other. Follow these guidelines to help ensure effective crisis management:



Use [technology with a standards-based and best-practices approach](#) to coordinate activities, so crisis teams can focus on actions requiring their expertise and judgment

---



Quickly establish the crisis team and executive leadership as a source of truth and guidance

---



Use communication methods that make information easy to consume (such as mobile devices) and that support real-time back-and-forth messaging between resiliency leaders and response and recovery teams

---



Provide leadership with real-time status updates so they can communicate timely information to the larger community

“For every 10% that a team outscored other teams on virtual communication effectiveness, they also outscored those teams by 13% on overall performance.”

“Five Ways to Improve Communication in Virtual Teams,” MIT Sloan Management Review<sup>1</sup>

# STEP 3: EMPOWER YOUR DYNAMIC WORKFORCE

Disruptions can necessitate that your workforce work remotely, potentially creating stress for employees, contractors and others who are not accustomed to working from home. Remote work can also create security risks if they are using their own devices to log in or using corporate laptops at home where they're not likely to have the security protocols required in the office. As you work to balance [empowering your dynamic workforce](#) to work independently with keeping your online resources secure, there are several things you can do to smooth the transition:



Develop straightforward, concise work-from-home policies and procedures



Ramp up help desk operations and ensure procedures include work-from-home support



Ensure you have adequate [secure access and authentication](#) technologies and controls in place



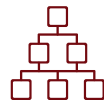
Support mental and emotional well-being with an employee assistance program or wellness program

45% of professionals who handle confidential data at work admitted to using public Wi-Fi and personal email to do so.

Dell End-User Security Survey<sup>2</sup>

# STEP 4: DRIVE RESILIENCY ACROSS YOUR THIRD PARTIES

Third parties are partners, vendors, contractors and supply chains your organization engages to achieve your strategic objectives. Your third parties become an integral extension of your organization and enable you to support customers, innovate, implement technologies and more. However, disruptions that impact your organization may affect your third parties' ability to perform, and vice versa. It's a symbiotic relationship that carries risk, so it's important to build resiliency across your broader business ecosystem. In the midst of a business disruption, it is critical to:



Work with your [third-party risk teams](#) to understand the continuity status of your most critical third parties



Understand supply chain exposures, prioritize them and address gaps as soon as possible



Coordinate your response and recovery plans with those of your most critical third parties



Automate and orchestrate policies across data security tools, and adapt rules and controls based on changing workforce needs and observed behaviors

70% of risk management professionals characterize their organization as moderately to highly dependent on external entities.

“Reestablishing the perimeter: Extending the risk management ecosystem,” DeLoitte<sup>3</sup>

## STEP 5: DON'T FORGET OTHER RISKS



During disruptions, other risks your organization is dealing with don't stop. In fact, they may even escalate as bad actors try to take advantage through cyber attacks or fraud. Regulatory compliance can receive less attention as teams change their focus to current business impacts. Disruptions demand everyone's attention, and if they extend over a long period of time, the risk of not achieving business objectives can create strategic risk.

It is critical to ensure your [risk management program](#) enables you to continue to identify new risks, evaluate and measure critical risks, take appropriate steps to manage the risks within acceptable tolerance levels, and advise executives on decisions they need to make.

### Planning for the Next Time

When the disruption ends – as disruptions always do – that's the ideal time to evaluate your organization's response. This should include:

- Assessment of the effectiveness of response and recovery plans, third-party engagements and contracts and service agreements
- A look at how your workforce responded, using performance measures, employee turnover statistics and other metrics
- Evaluation of overall resiliency capabilities

Consider engaging [experts who have helped many other organizations](#) mature their resiliency capabilities. Now is the time to act, and RSA stands ready to support your organization.

# RSA HELPS YOU COORDINATE BUSINESS RESILIENCY

While other vendors focus on disaster recovery, RSA approaches resiliency for the digital age more strategically by integrating it with your organization's integrated risk management program and by addressing a range of use cases geared toward digital business, with a strong focus on cybersecurity. The RSA solution for business resiliency is designed to help your organization unify disparate teams, understand business impact and coordinate activities to build resiliency.

## HOW WE HELP

### ASSESS BUSINESS RESILIENCY CAPABILITIES

- Engagement
- Assessment
- Risk Quantification
- Governance
- Benchmark Report

**RSA**  
SERVICES

### SECURE, RISK-BASED ACCESS & AUTHENTICATION

- Risk-Based Authentication
- Authentication Anomaly Detection
- Identity, Governance & Lifecycle Management
- Access Policy Violation Detection

**RSA**  
SECURID®  
SUITE

### BUSINESS RESILIENCY

- Business Context
- Criticality & Priority
- Risk Assessment
- Recovery & Testing
- Incident & Crisis

**RSA**  
ARCHER®  
SUITE

### EVOLVED SIEM/ ADVANCED THREAT DETECTION & RESPONSE

- Security Platform
- Logs & Packets
- Endpoint
- UEBA
- Orchestration & Automation

**RSA**  
NETWITNESS®  
PLATFORM

### OMNI-CHANNEL FRAUD PREVENTION

- Omni-Channel Fraud Detection
- Advanced Adaptive Authentication
- Real-Time Risk Assessment
- Fraud Intelligence
- Anti-Phishing Threat Management

**RSA**  
FRAUD & RISK  
INTELLIGENCE SUITE

To see how RSA can help you take action to make your organization more resilient, contact us to [request a demo](#)





## DIGITAL RISK IS EVERYONE'S BUSINESS HELPING YOU MANAGE IT IS OURS

RSA offers business-driven security solutions that provide organizations with a unified approach to managing digital risk that hinges on integrated visibility, automated insights and coordinated actions. RSA solutions are designed to effectively detect and respond to advanced attacks; manage user access control; and reduce business risk, fraud and cybercrime. RSA protects millions of users around the world and helps more than 90 percent of the Fortune 500 companies thrive and continuously adapt to transformational change.

Find out how to thrive in a dynamic, high-risk digital world at [rsa.com](https://rsa.com)

1. N. Sharon Hill and Kathryn M. Bartol, "[Five Ways to Improve Communication in Virtual Teams,](#)" MIT Sloan Management Review, Fall 2018 Issue
2. [End User Security Survey 2017,](#) Dell
3. "[Reestablishing the perimeter: Extending the risk management ecosystem,](#)" Deloitte, October 2018

**RSA**<sup>®</sup>

© 2020 Dell Inc. or its subsidiaries. All Rights Reserved. RSA and the RSA logo are trademarks of Dell Inc. or its subsidiaries in the United States and other countries. All other trademarks are the property of their respective owners. RSA believes the information in this document is accurate. The information is subject to change without notice. Published in the USA, 4/20 eBook H18243 W353671