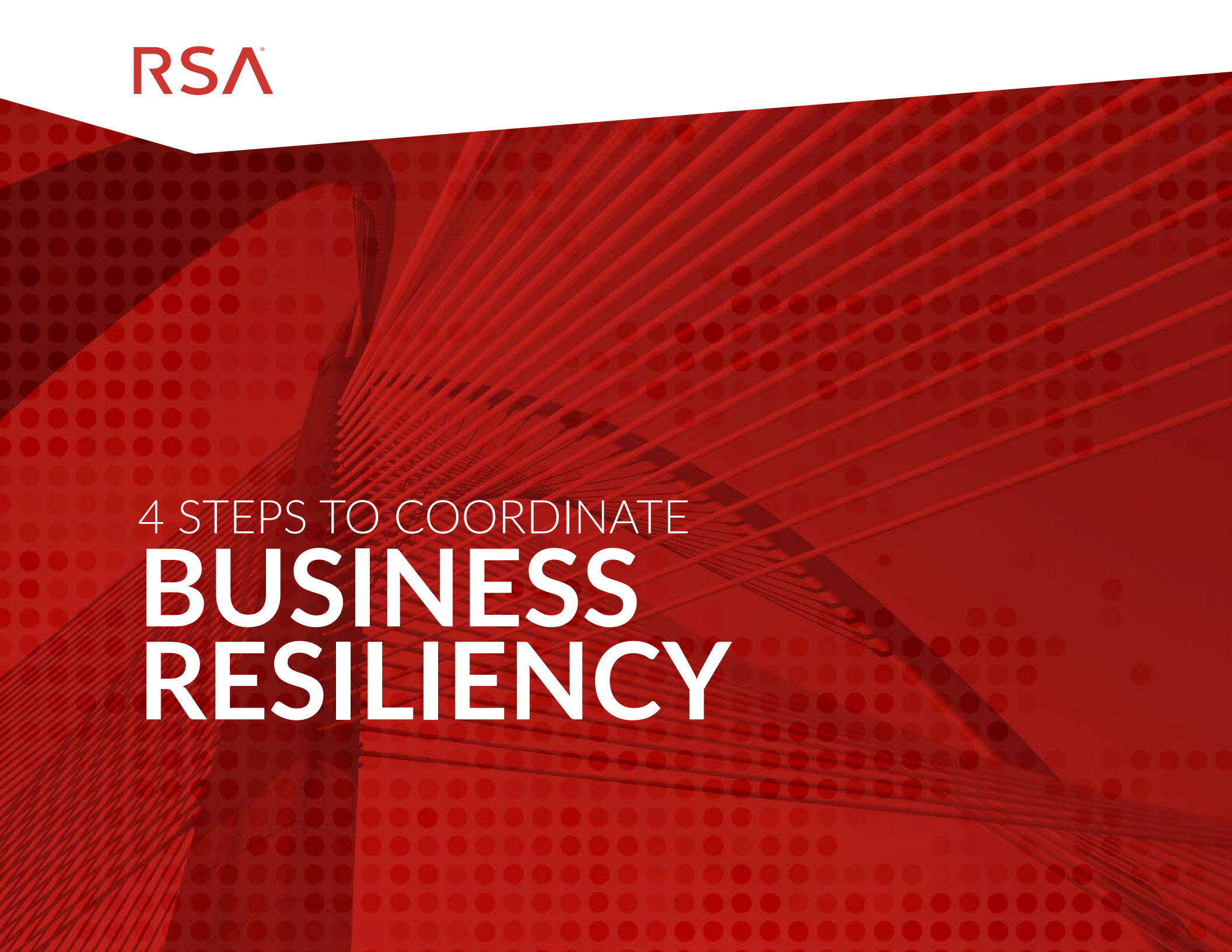
RSA



4 STEPS TO COORDINATE

BUSINESS RESILIENCY

BUSINESS ECOSYSTEMS ARE COMPLEX– DISRUPTIONS WILL OCCUR

Organizations Are Complex and Interrelated

Organizations today represent a complex and continually evolving tapestry of products, services, processes, technologies, employees, third parties and more. Each of these components adds complexity to a business and magnifies its fragility—especially when something goes wrong. If your organization is pursuing digital transformation, there's a very good chance that something will go wrong, whether it's a technology outage, a cyber attack or a wholly unexpected event.

Resources Are Limited

Resiliency and recovery can be expensive, so it's important to prioritize the processes, systems, people and other resources that are most critical to your business. In the event of a disruption, you want to restore these areas as quickly as possible.

Business Recovery Is Not Enough

The more complex your business and the more intricate your extended ecosystem, the harder it is to maintain operations in the face of disruption. Complexity also makes it more difficult to see where resiliency risks lie, where they are emerging, and at what speed they could affect your organization. Business and IT recovery plans can go a long way toward ensuring that critical functions can continue to operate or be recovered, but recovery may not be enough. Proactive resiliency measures should be the goal.

STEP 1: DETERMINE BUSINESS CONTEXT & PRIORITIES

Establishing business context means identifying the most important parts of your business so you can build resilience into them before a disruption occurs.

A business impact analysis (BIA) exercise can help you determine which business processes are most critical. It can also help you identify the upstream and downstream dependencies, systems and processes so that you can make them a priority in your resiliency planning.

STEP 2: COORDINATE BUSINESS CONTINUITY & IT DISASTER RECOVERY PLANNING

Business continuity and IT disaster recovery teams that work independently of each other are unlikely to have full visibility into resiliency risks across an organization. Lack of coordination between these two teams makes it harder for them to develop adequate recovery plans and resiliency procedures.

Managing recovery plans for business processes, systems, people, locations and other interdependencies is complicated enough. Disconnects between business continuity and IT disaster recovery only make it worse.

STEP 3: COORDINATE INCIDENT & CRISIS RESPONSE

A flat tire on a delivery truck. A customer who falls on a slippery floor. A hushed call to a whistle-blower hotline. These kinds of incidents occur often enough inside companies to merit standard procedures for handling them efficiently and effectively.

But what happens when standard incident response procedures aren't enough and an incident develops into a crisis? Does your incident response team know when to engage crisis responders? This handoff is critical, and if it doesn't happen at the right time and in the right way, it can worsen the crisis. That's why coordination between incident and crisis response is absolutely essential to resiliency.

STEP 4: ADAPT YOUR RESILIENCY PROGRAM

Resilient organizations not only implement plans to recover from different types of disruption; they also build resiliency into the fabric of their processes, systems and infrastructure. That means identifying single points of failure—like the one facility that manufactures a key part for your product—and implementing back-up plans so that a failure at that site doesn't grind production to a halt.

Successful business resiliency programs coordinate business priorities, business continuity planning, IT disaster recovery planning, crisis planning and incident response activities, and align these activities with business strategies and objectives.

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 RISK & CYBERSECURITY ADVISORY PRACTICE

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

RSA FRAUD & RISK INTELLIGENCE SUITE

* Interoperability between products

Review other resources that will help you take the next step toward strengthening your business resiliency risk posture. RSA – Coordinate Business Resiliency

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

RSA® Business-Driven Security™ solutions provide organizations with a unified approach to managing digital risk that hinges on integrated visibility, automated insights and coordinated actions. With solutions for rapid detection and response, user access control, consumer fraud protection and integrated risk management, RSA customers can thrive and continuously adapt to transformational change.

Find out how to thrive in a dynamic, high-risk digital world at rsa.com

RSA®