RSA

MAINTAINING RESILIENCY AFTER DISRUPTION

6 Ways to Prepare

After business as usual has been disrupted, the path to stability is a challenging one to negotiate. Countries, organizations and people must all find their way, and each must do it differently. The steps, timing and impacts inevitably will vary. Some will be ready to resume activities quickly, while others will need time to adjust.

Regardless of your organization's state of readiness, it is critical to exercise sound risk management and follow best practices for business resiliency. These include continuously assessing your current and future state, adjusting objectives, taking needed actions and moving forward.

Tomorrow's success truly depends on the steps taken today. Here are six areas on which to focus as you navigate these challenging times.

TOMORROW'S SUCCESS TRULY DEPENDS ON THE STEPS TAKEN TODAY.

CONTINUE RECOVERY AND BUILD RESILIENCY

Trying to rebound from a prolonged disruption can be like trying to hit a moving target. Changing conditions may extend longer than expected, requiring you to adjust business continuity plans to ensure recovery and resiliency strategies are relevant and adaptable. As you consider changes to your recovery priorities and strategies, be sure to:

Focus on the most important elements of your organization to ensure they are recovering and resuming—and remember, people are the highest priority

Adapt your plans so your business recovers and rebounds in the right direction, knowing that direction might change based on new business and recovery objectives

Think of the longer term: Capture what you are learning and adjust recovery and resiliency activities now, but also begin to think about how you can adapt your plans in the future

MANAGE CYBER THREATS

In times of disruption and crisis, change and uncertainty can create the risk of cyber attackers looking to exploit vulnerabilities related to the instability. Factors may include an increasingly remote workforce, rapidly expanding threat landscape that includes the cloud, and growing threat detection and response risk due to altered security operations. Here are three ways security teams can focus their efforts to manage threats that emerge.

Assess endpoint protection capabilities for BYOD when growing numbers of workers are using their own technology to access corporate networks and applications

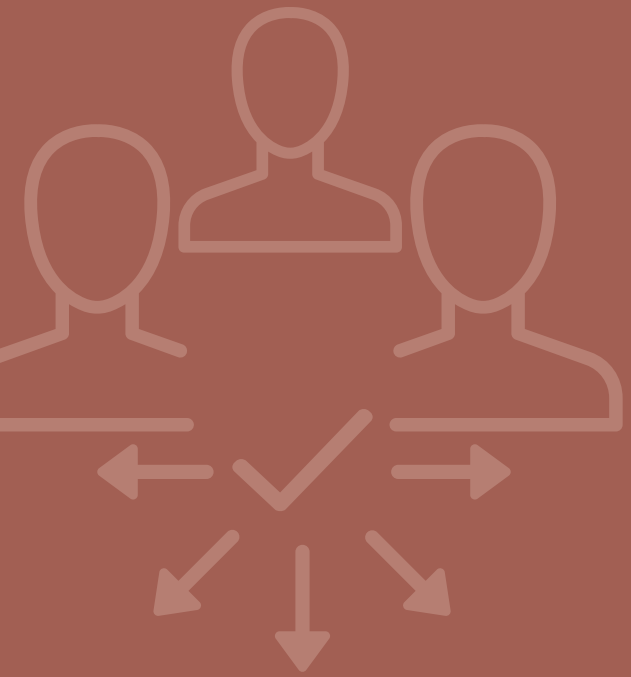
Limit risk in the cloud by identifying and establishing control over unsanctioned applications, as well as reviewing cloud usage policies to ensure their continuing relevance

Stand up or activate a virtualized SOC to ensure broad visibility and case management to identify and investigate threats in a remote world

53% of leaders surveyed at organizations engaged in digital transformation cited managing cyber attack risks among their top priorities.

RSA DIGITAL RISK REPORT, 1ST EDITION[1]

TRANSITION YOUR DYNAMIC WORKFORCE



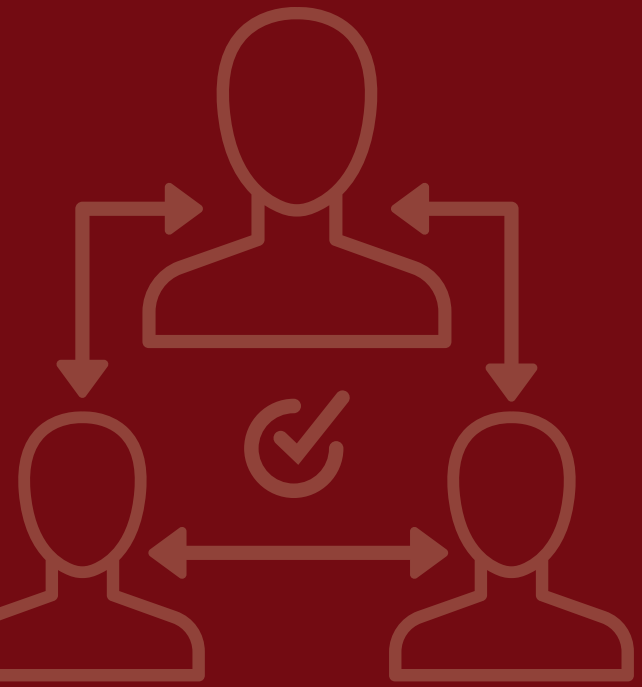
When a crisis results in millions out of work, many working from home and others reinventing themselves to meet changing business needs, organizations must be able to quickly adapt to maintain security and privacy amid the changes. At the same time, they need to determine if, how and when to return to previous workforce practices and policies. Consider these best practices:

Secure remote access with multi-factor authentication, to reduce the risks associated with compromised credentials and identity-based attacks like phishing

Ensure governance can quickly scale to meet the needs of users working remotely, demands for temporary workers and transitions back to physical offices

Modernize authorization and authentication by leveraging identity and access analytics to automatically assess and adapt to unforeseen and unexpected workforce risks

BUILD A RESILIENT THIRD-PARTY ECOSYSTEM



The resiliency of your third parties and your third-party ecosystem is as critical as that of your own organization. It's difficult to build third-party resiliency in the middle of a crisis, but as soon as your operating environment and third parties stabilize, you should begin evaluating ways to make these relationships more resilient. Some examples include:

Address immediate concerns for your most critical vendors, including those who are financially compromised, pose critical compliance or litigation risk, and have fourth-party vendors you may not know enough about

Incorporate measures into the contracting and onboarding phase to review third-party resiliency measures as well as gaps that need to be addressed

Identify and assess resiliency risks across your third-party ecosystem, starting with your most critical third parties, and identify ways to build in resiliency through redundancies and diversification

The resiliency of your third parties and your third-party ecosystem is as critical as that of your own organization.

FOCUS ON COMPLIANCE

Under normal circumstances, accepting the risk of any compliance violation is subject to careful consideration, review and approval by multiple parties. But during a crisis, organizations may not have adequate resources to fulfill their regulatory or internal obligations, or operational processes may be altered in such a way that management has no choice but to commit a violation. During a crisis—and in the process of emerging from one—it's critical to determine what, if any, compliance efforts have eroded, and to respond in these ways:

Identify critical compliance obligations and implement measures, both to avoid violations and to guide actions if a compromise is unavoidable

Engage with management to reaffirm compliance with obligations and the status of preparedness for upcoming regulatory deadlines

Demonstrate good faith by documenting instances of noncompliance (including the exception, rationale and any mitigation), because you may need to show an audit trail to regulators later

Once the crisis is over, be open and proactive with regulators, auditors and others related to any instances of noncompliance, and take proactive steps to correct and get back into compliance.

"Compliance professionals are intimately familiar with the notion that their programs should not be static, but should evolve with changes in the company's business. With this concept of continuous improvement in mind, it is wise to consider how resilient their programs are to crises."

"INSIGHT: CRISIS-PROOFING YOUR COMPLIANCE PROGRAM," BLOOMBERG LAW[2]

PREVENT FRAUD ACROSS DIGITAL CHANNELS

Fraudsters and cybercriminals thrive in times of crisis, using social engineering and other tactics to exploit consumers' emotions and vulnerabilities. This is especially challenging when it happens at the same time that organizations are encouraging more digital interactions and transactions. The key to protecting consumers and revenue is to heighten transaction security while keeping the digital experience frictionless. Follow these guidelines to manage the risk of fraud:

Educate customers about phishing and social engineering scams and how to avoid falling for them, but also be prepared to quickly detect and shut down attacks to reduce their impact

Review fraud prevention efforts across all consumer-facing digital channels, identifying points of weakness, refining fraud prevention strategy accordingly and implementing changes

Build resiliency into fraud investigation teams to ensure case-marking activity remains steady, to keep valuable feedback coming for machine learning by the risk engine

50% monthly decrease in case marking in March 2020 indicates fraud investigation efforts have fallen off steeply, suggesting a lack of resiliency in anti-fraud operation teams.

RSA FRAUD & RISK INTELLIGENCE DATA SCIENCE TEAM, MARCH 2020

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

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 – Maintaining Business Resiliency

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

1 Digital Risk Report, 1st Edition, RSA, September 2019
2 "Insight: Crisis-Proofing Your Compliance Program—Five Key Questions," Bloomberg Law, April 27, 2020

RSA®