The Security Division of EMC

White paper

# Assuring User Identities During a Business Disruption

## Applying a Consistent Strong Authentication Policy to Business Continuity Planning

# The importance of maintaining a two-factor authentication policy during a business disruption

**This white paper examines the importance of maintaining a consistent two-factor authentication policy during a business disruption. In addition, it provides insight into how to develop plans that enable cost-effective, rapid binding of users to their credentials in the event of an emergency – without lowering the security policy, opening the organization up to potential attacks or breaking the IT budget.**

## Introduction

Organizations are continually challenged with how to best support a diverse and geographically distributed community of remote users. This task becomes even more acute during an interruption to the normal cycle of business – such as what might happen during a pandemic or natural disaster when large numbers of users must be deployed to work remotely.

The global nature of business and the need for around the clock access to critical business systems means that organizations must find ways to support remote users, sustain productivity, and maintain a consistent two-factor authentication policy to protect the organization and its assets. Failure to assure the identities of users accessing company resources can expose the organization to fraud and inappropriate account use.

New business models have placed a further burden on the IT/security organization. Applications that were once reserved for only employees operating inside the firewall are now being pushed to the perimeter and extended out to serve a larger base of external users such as customers, partners and suppliers. With such a diverse population of users seeking access to network resources, assuring user identities during a business disruption is not just an option – it is a requirement.

This white paper is about striking the right balance. It examines the importance of maintaining a consistent two-factor authentication policy during a business disruption. In addition, this paper provides insight into how to develop plans that enable cost-effective, rapid binding of users to their credentials in the event of an emergency – without lowering the security policy, opening the organization up to potential attacks, or breaking the IT budget. This paper aims to answer the following questions:

- What is the nature of the threats that are likely to impact my organization?
- What users or entities in the organization require two-factor authentication during a business disruption?
- What are my options for maintaining a strong security policy during a business disruption?
- How can I ensure all users have credentials and can utilize strong authentication during an emergency without breaking the IT budget?
- How can users without hardware or software tokens be accommodated during a business disruption?
- Is there a cost-effective solution for quickly and easily issuing credentials to large groups of new users?

According to an IBM Global CFO Study, 62% of enterprises with over $5 billion in revenue admitted to encountering a major risk event.

## The Challenges of Business Continuity Planning

Organizations face two challenges when designing business continuity plans. The first challenge is keeping employees productive. Business continuity plans often call for employees to temporarily deploy to home offices when there is a disruption. With laptops brought from the office, employees can stay productive by accessing the network using home Internet connections and virtual private networks (VPNs). Employees without laptops can utilize home-based PCs with Internet browsers and stay productive by accessing web mail portals such as Outlook Web Access. Through these methods, employees can effectively work from a home office for days at a time.

The second, but often competing challenge, involves assuring the identities of remote users attempting to gain access to the network. This is a risk/security issue. By not assuring the identities of users attempting to access the network, an organization is put at much greater risk for fraud or unauthorized network access (and the liability and bad publicity that can ensue).

Two-factor authentication has long been the gold standard for protecting organizations with remote access (see sidebar). Two-factor authentication goes beyond simple username and password login to requiring users to enter something they have, like the one-time password on a token, and something they know (a PIN number). So the question is raised: Why not deploy hardware and software authenticators to every employee so regardless of the situation, the network will always be protected by two-factor authentication?

A recent survey by RSA[1] shows that on average, only 20-40% of the typical enterprise workforce is issued hardware or software tokens. The main reason for low deployment rates is the acquisition cost and ongoing management of deploying physical authenticators to every single user. The logic behind this is that only certain segments of employees work outside the firewall so they are the only users that require authenticators. So while a mobile employee may get a hardware token, a user who rarely works outside the office may not receive an authenticator. But with network access being pushed out to more external users and the possibility of a major business disruption, many organizations are starting to re-evaluate their policy for providing two-factor authentication.

### What is Two-factor (Strong) Authentication?

As organizations look to expand their operations globally and employee mobility increases, there is a growing need to provide remote access to enterprise information. More important is protecting access to that information through strong authentication by assuring the identities of all users in order to prevent unauthorized access.

Strong authentication is no longer essential just for remote access, but it is also needed to ensure that users within the enterprise are indeed who they claim to be. Organizations need to protect the identities of desktop users as well as remote workers, which is becoming an even greater challenge as companies permit access to their network to customers, partners and suppliers. And as more and more users continue to rely on the convenience of "anytime anywhere" access, even more issues are presented like what to do in the event of a business disruption that is the result of a fire, natural disaster or pandemic outbreak.

For many companies, multiple authentication options can be selected based on such metrics as the need for portability and the importance of the information a given user group can access. Cost is certainly a consideration, and organizations should evaluate acquisition costs, deployment and help desk costs.

Two-factor authentication offers a host of benefits for securing remote access. First, it is a cost-effective way to operate and allows organizations to evaluate and select from a diverse set of form factors depending on their budget and the needs of users. Second, it is a portable solution that provides users with the "anytime anywhere" access they demand. Finally, and most important, it offers strong security on a much higher level than password authentication alone in order to prevent unauthorized access.

[1] RSA SecurID Customer Survey Q4, 2007

Issuing credentials to every single user in an organization can be time intensive and beyond the range of what most IT budgets can bear. This can lead many organizations to an erroneous conclusion that maintaining a strong authentication policy to accommodate a large influx of users during a shutdown is impractical and therefore, security must be lowered or discarded in order to carry on with business.

Consider a company that has 10,000 global employees, 2,000 of which are mobile employees and use two-factor authentication to access the network on a regular basis. If a disaster occurs and the main headquarters location comes under an indefinite shutdown, there may be hundreds or thousands of employees who will require two-factor authentication in order to gain network access and avoid having productivity impacted. Does your two-factor authentication solution practically support the influx of several hundred or thousands of new users? Is your IT staff prepared to assist these new users with distribution of devices, login support and other issues? How can you maintain information security without straining your IT budget?

### No Longer Just About the Employees

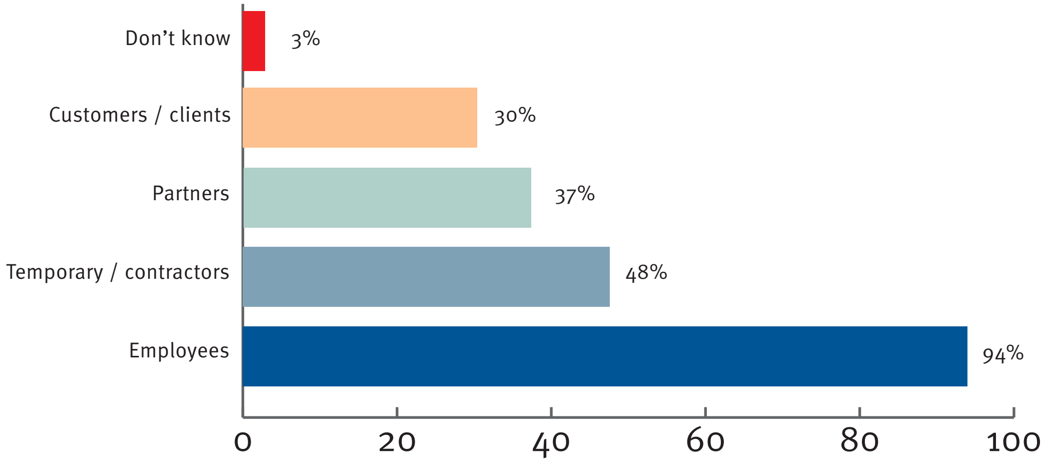
A major consideration to deploying an effective business continuity plan is to evaluate the universe of likely remote users. For example, we know that organizations are now extending critical applications outside the perimeter to new users such as customers, partners, and suppliers as a way to accelerate their business (see graph). In the case of a business disruption, an organization must continue to support these user populations.

## $600K an Hour: Why You Need a Business Continuity Plan

The statistics on business continuity planning are revealing. The IBM Global CFO Study released in October 2007 indicated that at many organizations, formal risk management is still fairly immature. By their own admission, only 52 percent of organizations acknowledge having any sort of formalized risk management program.

While business continuity appears to be an obvious solution for every organization, there are many issues to overcome in building an effective plan, especially internal dynamics. According to an IDG Research Services study,

Which groups within your organization use RSA SecurID authentication?



With such a broad range of network users, organizations need to broaden the definition of who needs to be supported during a business disruption.

when asked to identify the components they find most challenging about business continuity planning, respondents most often cited funding and people (24 percent and 20 percent, respectively), followed by management sponsorship (12 percent), testing (9 percent) and infrastructure/facilities (7 percent).

Despite the challenges, many organizations have taken proactive steps to address the threat of a business disruption and have developed plans. But when it came time to implement the plans, many lacked preparedness. According to the same IBM Global CFO Study, 62% of enterprises with over $5 billion in revenue admitted to encountering a major risk event. Of those organizations, more than 40% of them were not well-prepared to handle the event.

A disaster or crisis could strike at any time. That's why it's important for organizations to have a business continuity plan in place to ensure continuous business processes during and after a disruption in order to minimize the impact on operations. And as most businesses today rely on information to operate effectively, failure to provide access to that information can be costly. A study by Global Switch, a leading provider of high-specification data centers, estimated the cost of IT downtime to European businesses averaged $600,000 per hour.

## Options for Maintaining Two-factor Authentication

There are several issues to consider when determining how to ensure secure access during a business disruption – in particular, maintaining strong two-factor authentication for existing users and new or inexperienced users who will require access during a shutdown.

For existing users, two-factor authentication might be imposed through the use of a hardware authenticator or software token. However, many users do not always carry their hardware authenticator readily on hand or they may have a software toolbar embedded in the browser on their laptop which is locked up in a desk each night. In case of a shutdown, they will have no physical access to their one-time password authenticator and will not be able to securely connect to the network.

### The Pandemic Threat

Of particular interest to many organizations is the threat of some type of pandemic impacting business operations for days, or perhaps weeks, at a time. Companies with a global footprint are especially concerned. The H5N1 bird flu virus is one recent example that has caused major concern and made many organizations evaluate their business continuity plans. For years, various government agencies around the world have been battling to contain the effects of the deadly disease, with limited results. At last count, reports show that cases of the bird flu have been reported in over 45 countries.

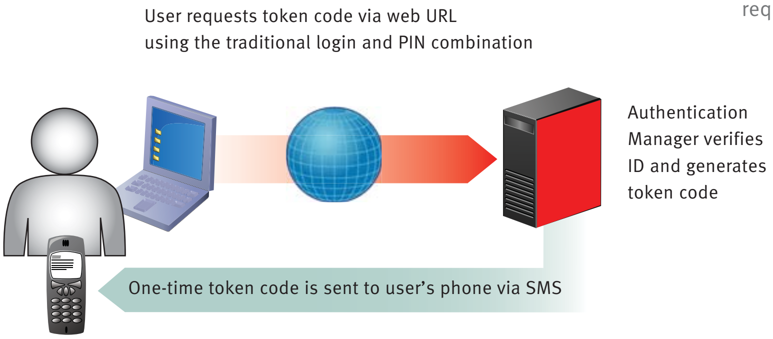
In the event of a pandemic outbreak, organizations could find themselves mandated to work from home. The United States Congressional Budget Office estimates that, should an outbreak occur within a designated area, as much as 40 percent of the entire workforce would be unable to have a physical work presence – maybe for weeks on end. Not having a business continuity plan in place for employees to remotely access critical applications from home and a strong authentication policy to securely protect that information could be very disruptive and costly to a business.

For new or inexperienced users, two-factor authentication may need to be imposed ad hoc. Supplying hundreds or even thousands of users with hardware or software authenticators in the event of a disaster may not be practical. An alternative two-factor authentication solution is needed to accommodate an entire new user population while maintaining a simple user experience.

A business continuity plan should involve more than just providing access to information. A sound plan identifies the risks and threats that could result from a business disruption and provides a means to effectively respond to those risks and threats. So while assuring regular operations is the core purpose of any business continuity plan, maintaining information security, often with a two-factor authentication policy, is just as critical.

Following are the options that most organizations consider today for implementing strong authentication to users in the event of a disruption:

- Issue every user a token. While possible, this option is logistically impractical and can be extremely costly for large numbers of users. The bottom line is that the cost and management of issuing tokens to every user may outweigh the benefits to the organization
- Issue tokens on an "as needed" basis. As in the previous case, even ad-hoc provisioning creates logistical challenges and is typically limited by the constraints of the IT budget.
- Lower your information security policy. This is also known as the "sweat it out" approach. Resorting to a username and password authentication policy might seem like a feasible short-term solution to getting normal business operations underway, but depending on the nature of the threat, a shutdown could last for days or weeks. Also, facing the possibility of a data breach, even if a shutdown endures for just a few hours, is a risk most organizations are not prepared to assume.


User requests token code via web URL
using the traditional login and PIN combination
Authentication
Manager verifies
ID and generates
token code
One-time token code is sent to user's phone via SMS

RSA SecurID On-demand Authentication

Beyond the monetary costs of a breach by unauthorized users, there are irreparable effects such as the loss of customer confidence and brand value and reputation.

## The RSA Solution: On-demand Authentication and the Business Continuity Option*

RSA provides a unique, innovative approach that enables organizations to uphold their two-factor authentication policies during a business disruption, regardless of the number or types of users connecting to the VPN – all without burdening the IT staff or breaking the budget. RSA's solution is comprised of two core components: the RSA SecurID® On-demand Authenticator and the Business Continuity Option license.

### On-demand Authentication

The RSA SecurID On-demand Authenticator enables users to securely access the network without pre-assigned credentials. It is a "tokenless" access method requiring no physical hardware token or software to be installed on the end-point device. On-demand authentication provides flexibility and ease of deployment while maintaining all the security strictures required for two-factor authentication.

The On-demand Authenticator utilizes a self-service web URL where a user logs on to request a one-time password. From an Internet-capable PC, accessing the interface requires traditional login and PIN/password combination. Upon successfully passing this phase, a one-time password is generated by the RSA Authentication Manager server and sent to the user's mobile device (pre-registered in the data store) via Short Message Service (SMS) over the public cellular network. E-mail delivery is also supported.

Once the 8-digit, one-time password is received, the user enters it along with a PIN to the password login of the corporate VPN, web application, Citrix portal or other network resources. On-demand Authenticators can also be used for purposes beyond just business continuity such as deploying them to contractors or partners. This creates a flexible authentication method that is always available and can be used to support two-factor authentication in a number of different use cases.

*The capabilities discussed in this paper are included in RSA Authentication Manager 7.1.

## The Business Continuity Option: Flexible Licensing for On-demand

On-demand Authenticators can be assigned to individual users in the same manner that hardware and software authenticators are assigned. The Business Continuity Option (BCO) license takes this a step further. It offers a true on-the-fly expansion capability for any organization that needs to quickly support a large number of users that might suddenly be deployed to work remotely. The solution is a critical part of any business continuity or pandemic plan.

The Business Continuity Option is like an insurance policy. Purchasing On-demand Authenticators to cover every user in the enterprise, whether or not they actually use it, can still be cost-prohibitive to some organizations. Therefore, RSA has created a special license that can be added to the RSA Authentication Manager license page.

The Business Continuity Option is a licensing feature optionally available with the RSA Authentication Manager 7.1 solution. Once added to the licensing page, an administrator with rights can simply view, select and activate the feature when necessary. The activation "unlocks" the corresponding number of server seats and the On-demand Authenticators which can then be deployed to any remote user needing access.

Users request On-demand Authenticators through the self-service web portal included in Authentication Manager 7.1. The portal provides a convenient 24x7 service for users to manage all aspects of the token lifecycle and submit a request for access. In order to be issued an On-demand Authenticator, a user must login to the self-service portal which then sends the one-time password to a destination that has been pre-determined by the user, such as a mobile phone. The rules of two-factor authentication are again reinforced through this method: something you know (login/password) and something you have (one-time password delivered to the mobile device via SMS or e-mail).

## Best Practices in Business Continuity

Before you deploy a Business Continuity Option from RSA, consider these important steps that could enable you to save time and ease the headache to your IT/security organization.

### 1. Check your VPN license

Make sure your VPN license can support the influx of large numbers of remote users. Many VPN vendors, such as Juniper and Checkpoint, offer flexible licensing options, like the RSA Business Continuity Option, that can expand to meet demand.

### 2. Determine who will require On-demand authentication

Taking the time to sort out the users that will require On-demand authentication during a shutdown can greatly reduce the calls into the help desk. For example, existing token users are not likely to require On-demand authentication.

### 3. Determine on the method of delivery

Both SMS and e-mail delivery are supported. Determine which method meets the needs of your business and your users.

### 4. Establish a relationship with an SMS vendor

If SMS is to be used as a delivery method, establish a relationship with an SMS vendor that delivers global enterprise coverage. RSA has worked with Clickatell, a messaging vendor that works in over 200 countries and on 600 networks worldwide.

### 5. Create policies that facilitate easy on-boarding of users

These include making sure users have been registered and that they have entered their life questions in case they encounter a challenge and additional information is needed.

### 6. Establish a communications plan

Users need to be directed to the self-service console and given instructions on how to access the network using the On-demand Authenticator.

## Summary

There is no advanced warning for when disaster strikes – it just happens. And organizations must have an effective business continuity plan established in order to enable normal business operations to resume as quickly as possible. The longer the network is down and access to information is limited, the more expensive it is for a business.

Failure to implement a strong two-factor authentication policy can be just as costly if your network remains vulnerable to unauthorized users. Beyond just the monetary costs, there are irreparable effects such as the loss of customer confidence and brand value and reputation.

By implementing the On-demand Authentication and the Business Continuity Option solution from RSA, organizations can resume normal operations during a business disruption without compromising security, burdening the IT staff or straining the budget. RSA provides a cost-effective solution to maintain a strong two-factor authentication policy that is easy to deploy and easy for employees to use – even if they have never been required to use two-factor authentication before.

Organizations must have an effective business continuity plan established in order to enable normal business operations to resume as quickly as possible.

The Security Division of EMC

RSA Security Inc.
RSA Security Ireland Limited
www.rsa.com