
Blackberry Blackout

Protective Best Practices Against Disruptions of a
Pervasive Communications Technology Infrastructure
With a Potential Global Economic Impact

An Informatica Research White Paper

By:

Andrew S. Seto, Security Associate, Informatica Corporation

with

Claudiu S. Popa, President & CSO, Informatica Corporation

Table of Contents

Executive Summary	3
1. Introduction	4
2. The Blackberry Wireless Device Infrastructure	4
2.1 Telecom-based Wireless Infrastructure	4
2.2 Blackberry Enterprise Server (BES) Infrastructure	5
3. Impact of Blackberry Unavailability	5
3.1 Managerial Decision Making	5
3.2 Business Operations Processes	6
4. Risks and Best Practices	6
4.1 Blackberry Handheld Device Compromise	7
4.2 Blackberry Enterprise Server (BES) Downtime	7
4.3 Unreliable Corporate Network	7
4.4 Telecommunications Network Service Interruption	8
5. Blackberry Security	8
5.1 Enterprise-Level Security	9
5.2 Device-Level Security	9
6. Conclusion	9
7. References	10

Executive Summary

Blackberry connectivity is a critical requirement for today's professionals who need to stay in touch and make informed decisions in real-time. The impacts of service unavailability range from temporary delays to the disruption of business operations across extended enterprise networks. Designing and implementing an adequate Blackberry infrastructure is a significant challenge, but it will determine the extent of that impact. A telecom-based infrastructure provides the most reliability and stability by relying on the telecommunications provider for Blackberry service. A Blackberry Enterprise Server-based (BES) infrastructure can be less reliable but it compensates by being more appropriate for large- to enterprise-scale companies. Each of these solutions provides distinct advantages and disadvantages depending on the organization and its environment.

Multiple factors in the Blackberry infrastructure can impact availability. These are the Blackberry handheld device itself, the BES servers, the corporate network, and the connectivity provider. Some of these issues can be addressed by implementing system redundancy to ensure that alternative solutions exist, such as prioritizing service restoration over the more time-intensive diagnosis and repair of affected systems.

“Designing and implementing an adequate Blackberry infrastructure is a significant challenge, but it determines the extent of the impact of major outages.”

By implementing the following best practices, organizations can vastly reduce or control the risk of Blackberry service disruption to a manageable level where it provides a reasonable degree of business continuity protection and disaster mitigation:

1. **Quantify the criticality of Blackberry service reliability and uptime before committing resources.** In some cases, a brief service disruption may have a negligible impact on real business processes and extensively redundant safeguards may not be necessary. Time may not always be a critical factor.
2. **Identify alternative methods for secure e-mail retrieval.** When properly implemented, Microsoft Outlook Web Access provides a secure, convenient, and cost-effective option, while a VPN-based option provides the most security (but may be more complex and costly). Educate staff on the use of such alternatives and carry out routine testing to ensure reliable operation when urgently needed.

Note: Wireless networking is nearly ubiquitous, but insecure wireless access points (“hot spots”) are security risks. Always verify that your connection is authenticated and secured using encryption (i.e.SSL/TLS) before using the wireless network. The 802.11 WEP encryption standard is *not* secure, and should be replaced with WPA with “strong” keys or other verifiably secure communication methods.

3. **Ensure that IT personnel actively monitor critical resources,** relevant mail servers and BES systems to detect significant events and prevent disruptions by taking appropriate remedial actions. Ensure that technical staff are trained to implement, use, maintain, support and restore BES systems.
4. **Include Blackberry service disruption in the Business Continuity Plan or Disaster Recovery Plan** to ensure that risks, remediation methods and test results are fully documented and ready for urgent activation. This BCP/DRP must be communicated to the entire organization and routinely tested by professionals.

1 Introduction

Research in Motion's Blackberry handheld has become the most recognized productivity tool in the hands of today's busy professionals. Able to synchronize schedules, navigate the Internet, enable phone calls, and above all else, exchange e-mails anytime and almost anywhere, the Blackberry allows people to get more work done and make informed decisions whether they are in or out of the office.

Blackberry service availability is thus understandably critical for mobile professionals as business continuity should not be restricted by transient availability. Service interruptions can affect the ability to receive information and can impact important decision processes. This paper provides an overview of the Blackberry wireless infrastructure, discusses the impact of disruptions on Blackberry availability and offers suggestions for avoiding or otherwise mitigating the risk of downtime.

2 The Blackberry Wireless Handheld Device Infrastructure

The Blackberry Wireless handheld device can be implemented in two ways. The first is a telecommunications service provider-based infrastructure whereby the user is wholly dependent on the provider for service availability. The second is a Blackberry Enterprise Server-based (BES) infrastructure whereby service dependency is shared between an internal BES server and the external telecommunications provider. Either solution may be more appropriate than the other depending on business requirements, and each comes with a distinct set of advantages and disadvantages.

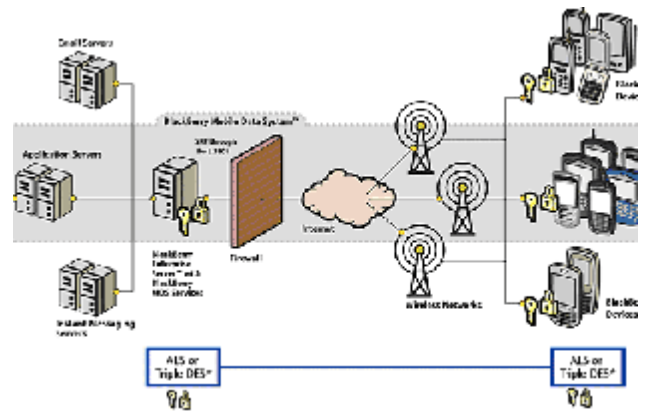
2.1 Telecom-based Wireless Infrastructure

The telecommunications service provider-based wireless infrastructure regards the Blackberry handheld as any other mail-enabled device such as a cellular phone or a PDA. That is, all communications between Blackberry devices are strictly external to the corporate intranet, and communication between a Blackberry device and corporate e-mail account is external until it arrives through a corporate gateway to reach the enterprise mail exchange server. Voice and e-mail data are routed from the device directly to the telecommunications provider (such as Rogers, Bell, or Telus in Canada and Verizon, T-Mobile, or Cingular in the US), through their communications network, and finally arriving at the receiving device. Blackberry devices utilizing this model use telecom-provided devices and carry their individual e-mail accounts and addresses (i.e. *user@telconame.Blackberry.net* is the typical email address format).

This model is the more reliable of the two infrastructure types as service availability is completely dependent on the proven telecommunications infrastructure of the service provider, which often tends to be more reliable or robust.

2.2 Blackberry Enterprise Server (BES) Infrastructure

The Blackberry Enterprise Server (BES) infrastructure communicates with enterprise Microsoft Exchange, IBM Lotus Domino, or Novell Groupwise mail servers to treat the Blackberry handheld as a virtual internal client device. Incoming e-mails are routed to the corporate BES which then encrypts and “pushes” the e-mail to the Internet and to the receiving device. Unlike the telecom-based infrastructure, part of the communications pathway is internal; the key difference is that under the BES-based infrastructure the Blackberry carries a corporate e-mail address and the e-mail itself is stored on internal mail servers rather than an external telecom-provided e-mail account. Among other reasons, the BES-based infrastructure is more appropriate for medium- to enterprise-scale businesses because e-mails and the confidential information they contain are the legal property of the business rather than the telecommunications provider.



Source: http://www.BlackBerry.com/images/technical/bes_41_arch_diagram.gif

This model is the least reliable of the two infrastructure types as service availability is dependent upon both the internal corporate network (the BES especially) as well as the external telecommunications network. A BES failure or internal network availability without adequate redundancy may be sufficient to create a prolonged service disruption.

3 The Impact of Availability

In the business world, Blackberry availability issues impact two main types of users: those who rely on the device to make informed managerial decisions, and those who need to receive messages in order to take operational action. Although both essentially require real-time connectivity, the underlying difference of time sensitivity makes the first model the preferred solution in terms of suitability and reliability.

3.1 Managerial Decision Making

This group of users relies on the Blackberry handheld for important emails but not always urgent ones. These users receive e-mails that are mission-critical and require a significant and knowledgeable decision, but for which business continuity is not dependent on instant service availability. This group is able to compromise timeliness as long as e-mails are received within a reasonable span of time. Furthermore, managers must have the ability to retrieve confidential e-mails which should be securely controlled on internal mail servers rather than stored on third-party (telecom) e-mail systems.

As security and internal management of confidential e-mails are preferred over timeliness and reliability, a BES-based infrastructure is clearly preferred. Since mission-critical e-mails are stored on corporate mail servers and not on telecom-provided e-mail systems, decision-makers still have the ability to retrieve their e-mail and make informed decisions. Business continuity is therefore best protected by this scenario as it is not constrained by the risk of BES failure or even some telecommunications service interruptions.

3.2 Business Operations Processes

This group of users relies more on the Blackberry handheld for time-sensitive e-mails. Such users typically use the device to be notified that a specific event has occurred and a particular action must be taken; for example, an IT department may employ Blackberry devices to notify their personnel that a server has failed and requires immediate action. This group requires that the Blackberry service to be first and foremost reliable, that is, the service must ensure that urgent e-mails are received in a timely manner.

The dependency of business operations on service availability lends preference to the telecom-based infrastructure as the more appropriate model. This is because personnel retain the ability to communicate and take appropriate action in the event of an internal communications failure (i.e. a BES failure or a malicious denial-of-service attack on the corporate intranet) by depending on a robust external telecommunication network.

In the interest of preserving compliance with privacy laws, best practices dictate that e-mails sent to the telecom-provided e-mail (in particular automated messages and alerts) be stripped of as much confidential contextual information as possible but be sufficiently descriptive as to remain actionable by the recipient. Mission-critical and other confidential information should be sent to the internal e-mail address to be stored on a corporate mail server to preserve confidentiality rather than on an external telecom-provided mail server. Verifiable data encryption is always an excellent way to protect data confidentiality and preserve compliance.

4 Risks and Best Practices

Blackberry service interruption may occur at different points of failure depending on the infrastructure selected. In contrast to a telecom-based Blackberry service which is almost entirely dependent upon the reliability of the communications network, a BES-based Blackberry service is dependent on the collective availability of the BES itself, the corporate network, and the telecommunications network.

It is important that companies be sufficiently prepared for a Blackberry service outage by including it within Disaster Recovery Planning (DRP). Blackberry handhelds have in many cases become the preferred communications tool of professionals. Although Blackberry service interruption typically does not threaten business continuity in general, it can severely impair the company's ability to communicate quickly and effectively.

Best practices include:

- Recording device serial numbers and PINs so that compromised devices can be "locked out" of the network to prevent further misuse (and in some cases, even located).
- Recording alternative access numbers (pagers, mobiles) to ensure accessibility for Blackberry-equipped personnel.
- Identifying alternative methods of communication.
- Identifying and implementing alternative methods for e-mail retrieval for off-site employees. For example, Microsoft Outlook Web Access and VPN tunnelling.
- Implementing hardware redundancy of machines most likely to be affected (e.g. The BES itself, network routers, switches, application/mail servers, etc.).
- Ensuring the availability of trained personnel to investigate and restore affected systems, especially complex systems such as the BES.

4.1 Blackberry Handheld Device Compromise

The physical Blackberry device itself is one of the primary weak links for availability. Blackberrys should be safeguarded by the user and securely stored whenever possible. It is important to prevent theft of the device and the information stored therein. Security threats such as trojans, worms, and viruses can also affect device availability (see section 5).

4.2 Blackberry Enterprise Server (BES) Downtime

The BES is a complex software application running on top of an operating system. The BES is responsible for routing incoming e-mails as they reach corporate mail servers or leading application services out to the Internet where they are forwarded to the user Blackberry devices. A BES failure stops handhelds from receiving corporate e-mails, but the devices themselves retain partial functionality (offline functions and Internet access are unaffected). It is worth noting that Blackberry users will not be able to detect BES failures¹, and measures must be taken to ensure that failures are detected and timely remedial action is taken.

BES failures can be the result of hardware or software problems. A software failure may occur as a result of an unstable or erroneous software patch, system error, or a malicious attack on the BES application itself or the underlying operating system. Updates to production software should occur during off-peak hours to minimize impact in the event of a failure. The system needs to be rigorously tested to verify the stability of the change before and after it takes place. Extreme care must be taken during the update process to enable a potential rollback to a stable version in the event of a problem. The priority is to restore availability while the failure can be investigated without affecting business processes.

A hardware failure may present itself as a faulty hard drive, memory module, or a failure in any number of other system components. It is important to have a redundant BES available, either in “hot” standby (failover device that is actively ready) or “cold” standby (device in storage needing to be swapped in), as diagnosis of a hardware problem is often a very lengthy and arduous process. It is critical that a redundant BES be immediately deployed so as to minimize the impact to business processes while the failed system is examined and repaired.

4.3 Unreliable Corporate Network

The corporate network is responsible for the reliable transmission of data throughout the enterprise, and an unreliable infrastructure is very likely to affect business continuity. A corporate network must be sufficiently robust; the use of redundant routing hardware is critical to ensure that alternative data communications pathways exist in the event of failure.

High bandwidth usage, malicious attacks, and typical network device failures are all possible causes for network failure. An ineffective corporate network is unable to properly route e-mail messages from the enterprise mail servers to the Internet, and thus Blackberry device service is negatively affected.

5 Key best practices for building and maintaining a stable network:

- Ensuring that network hardware provides sufficient features, capacity, and speed to meet the enterprise's minimum requirements under normal conditions.

1 In practice, the BlackBerry device can only show a lack of incoming e-mails when the BES fails to route e-mails to the handheld devices (unaware of the failure of the actual server).

- Investing in hardware redundancy to ensure there exists multiple communications pathways to the Internet. The IT department must ensure that the hardware is capable of supporting at least twice the desired data load (such that each device is capable of supporting the entire network load on its own in the event that the primary device fails).
- Retain technical staff with the expertise to monitor, maintain, and remediate network problems.
- Ensuring there are enforced technical and administrative security policies in place to defend against virus, worm, and other malware outbreaks on the corporate network.
- Creating *an effective* DRP to address a prolonged network service interruption.

Conversely, while corporate Blackberry users are affected by network disruptions, this is a situation where a telecom-based Blackberry service is preferable: since the telecom-based Blackberry service is independent of the corporate network, users retain the ability to communicate in the event of a corporate network outage. Critically, in such instances, network engineers are able continue to communicate and coordinate efforts to restore network availability.

An unreliable corporate network affects more than just Blackberry services; it affects business continuity itself. Thankfully, service interruptions on a professionally designed corporate network infrastructure tend to be very rare, brief (typically minutes to a couple hours), and geographically constrained, therefore limiting the overall effect of a network outage on BES-based Blackberry users.

4.4 Telecommunications Network Service Interruption

For a BES-based infrastructure, the telecommunications network is responsible for routing e-mail messages once it leaves the corporate gateway through the Internet to the Blackberry device itself. For a telecom-based Blackberry device, the service provider is entirely (or as dictated by the Service Level Agreement) responsible for the handheld's ability to send and receive e-mails.

Although telecommunications networks tend to be sufficiently robust, immediate remedial action in the event of a service interruption may not be possible. In April 2007, a failed evening-hour software update at RIM's single telecommunications hub in Waterloo, Ontario caused a North America-wide Blackberry service disruption that lasted several hours². Blackberry users were forced to wait without an explanation until service was restored in the late morning of the following day and information was finally communicated regarding the event.

5 Blackberry Security

In order to preserve Blackberry service continuity, security of the device as well as its network must be maintained. Security policies must be implemented at both the enterprise level and at the device level. Fortunately, the BES provides encryption services for outgoing e-mail using the industry standards Triple Data Encryption Standard (3DES) and Advanced Encryption Standard (AES), thus e-mail from the point at which it leaves the corporate network to the time it is received by the device is adequately secure. However, e-mail encryption alone does not provide complete security; a security policy must be in place within the enterprise to ensure

² Despite the relatively minor impact to users as the outage occurred during non-peak hours, the sheer number of affected users caused the incident to garner significant publicity.

that potentially harmful messages are filtered. Additionally, a security policy must be enforced at the device level to ensure that potentially harmful applications cannot be executed.

5.1 Enterprise-Level Security

Because much of the Blackberry infrastructure is dependent upon the internal network, service continuity partly relies on the network's ability to securely and consistently forward incoming e-mail messages from enterprise servers to the Internet. In order to prevent potentially harmful messages from being forwarded to the device, effective e-mail filters must be in place to detect and block anomalous and/or malicious messages. Network devices responsible for forwarding e-mail traffic must be protected against compromise and misuse. The corporate BES must also be securely hardened and updated with critical, timely patches.

An enterprise-level security strategy must also enforce device-level security compliance for all Blackberry handhelds throughout the organization. It must provide for security awareness training to Blackberry users and create incident management procedures to mitigate or prevent the abuse of compromised devices. Any compromised device must be immediately identified and locked out of the corporate network. The compromised Blackberry may also be submitted to RIM (under a confidentiality agreement to protect intellectual property) for a forensic investigation to prevent similar attacks on other devices on the network. A security policy may also only allow the IT group to deploy applications and updates to prevent the compromise of individual devices.

5.2 Device-Level Security

An effective device-level security strategy requires a moderately short device timeout (period of inactivity before automatically "locking" the device and password-prompting the user for reactivation) of 3 to 5 minutes and "strong", quarterly expiring passwords consisting of at least 8 characters with a mix of both upper-case and lower-case letters and numbers. If a device is lost or misplaced, this would essentially render the device unusable to unauthorized users while adequately protecting the confidential information stored within (as long as data encryption is used). In compliance with an enterprise-level security policy, a missing Blackberry must be immediately reported to the IT group for network deactivation/tracking.

A Blackberry device should only allow signed applications to be installed; that is, an application or update to be installed must be accompanied by a valid digital signature validating the authenticity of its source as an authorized party (typically, the organization itself and RIM). This can prevent unauthorized and/or unauthenticated (i.e. possibly malicious) applications and updates from being executed and thus the device is protected against malware infections. Optimally, the ideal solution from a security perspective is to restrict the ability to deploy updates and applications to the IT department only.

6 Conclusion

Blackberry service continuity is critical for working individuals to organize their schedule, coordinate tasks, manage activities and communicate. We have described a variety of availability situations, how they affect business processes and how they can be avoided or mitigated with effective solutions. The nature of the business is a key factor in the planning process. Priorities such as time sensitivity and the need for reliability must be considered before investing in such proactive solutions. Regardless of these considerations, efforts must be made to ensure that brief service interruptions contained and controlled to ensure that they do not adversely affect business continuity.

7 References

McCarthy, Caroline. "Blackberry e-mail is back, but problems remain". CNET News. April 2007
http://news.com.com/2100-1039_3-6177072.html

Reardon, Marguerite. "Blackberry outage: RIM a victim of its own success?". CNET News. April 2007
http://news.com.com/Blackberry+outage+RIM+a+victim+of+its+own+success/2100-1039_3-6177349.html?tag=item

Noguchi, Yuki. "Lost a Blackberry? Data Could Open A Security Breach". Washington Post. July 2005
<http://www.washingtonpost.com/wp-dyn/content/article/2005/07/24/AR2005072401135.html>

Research In Motion. "Blackberry - Blackberry | Wireless Handheld Devices, Software & Services from Research In Motion (RIM): At a Glance: FAQs" Research In Motion. Copyright 2007.
<http://na.Blackberry.com/eng/atag glance/security/faq.jsp>

Image Source: http://www.Blackberry.com/images/technical/bes_41_arch_diagram.gif