INFORMATICA
INFORMATION SECURITY & RISK MANAGEMENT

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

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* committting 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.