Rainbow/PUSH Coalition
3rd Annual Wall Street Project Conference
"Building Bridges to Expand the Marketplace"
Panel: The Convergence of Telecommunications and Technology

The Security Implications of Getting Online Broadband Access for Your Small or Minority Business

By Eric D. Williams President/CEO, Information Brokers, Inc.

The events of the past four to five years have been phenomenal. Businesses and consumers have engaged a new paradigm in how they relate. This has brought a dramatic and interesting change in the way businesses interact with the consumer and each other. Gone are the days of "*the check is in the mail*" or "*we shipped that last night*". Transactions are instantaneous and perceptions of the authenticity of information - the level of "Trust" has changed.

This is especially evident in business to business relationships. Companies must now modify the way they secure corporate information, the traditional security paradigm has been turned on its head. Businesses can no longer delegate the responsibility of security to a single, paranoid information security officer who wants to deny access to all information.

Consumers, partners, suppliers and resellers must be allowed unhindered access to information concerning the supply chain and availability of inventories. This puts businesses in a very different posture concerning information control. This shift dictate the control of information flow be managed not at the upper levels, the towers of the management hierarchy, but at the edges, closet to the people control that information and those who need to know.

With the introduction of broadband technologies such as Cable modems and Digital Subscriber Line, and others to come businesses must position themselves to accept the responsibility of "Trust" maintenance and responsible uses of the network. The control and administration of the security of computing resources and NOT merely information access, now drives the business security architecture. The reputation of your business may be at risk from bad publicity.

Recently computers have been 'hijacked' by intruders not for the information they contain but to use those compromised systems to disrupt services of other, victim, sites. This is the way intruders see your network - *'its not your data its your resources'*.

continues…

1309 'S' Street S.E.
Washington, DC 20020-6925

Phone: +1 (202) 503-9766
Fax: +1 (202) 315-3511

In this new framework the small business must consider and establish acceptable use standards for those resources and be able to successfully communicate those standards to its users. This includes the levels of confidentiality - and not privacy - to expect. In addition particular attention should be given to the maintenance of the software that enables the e-conomy at all levels. All established ***Service Level Agreements*** (SLA) and ***Acceptable Use Policies*** (AUP) of top-tier services providers should include the ***Best Common Practices*** (BCP) for operations and clearly state the providers accepted liability, especially where secure transaction processes are enabled by that provider.

The top tier providers in the internet industry must work to educate small business in methods to best protect their systems from external intruder compromise. Additionally, these providers should foster the development of a vendor and provider independent ***Public Key Infrastructure (PKI)***. This independent PKI must include the elements of:

Integrity - the enabling of technology to determine that a message received has not been modified in transit.

Confidentiality - the enabling of technology that allows messages to be exchanged between systems or users in a private manner that is not susceptible to eavesdropping.

Authenticity - the enabling of technology that ensures an entity are who they say they are.

Non-Repudiation - the 'Holy Grail' of PKI, is the enabling of technology that stipulates the indicated originator of a message is in fact the originator and that a message can not be repudiated by the indicated originator.

Small Businesses are becoming a significant driver of the marketplace for broadband and the e-conomy. Businesses must:

- Become fully informed of their security posture;
- Assess and plan contingencies;
- Be able to react adequately and quickly, make time for staff education;
- Know the law concerning the retention and privacy of information;
- Examine established policy.

Businesses must be sure that all of management understands the potential impact of a security breach on the company's reputation. These are very real and potential threats.

Cooperation among entities in the Internet community is paramount. Your security may very well depend on someone else's. Support incident response teams, pressure vendors for better security controls in their products.

The intruder community is working hard, there are many tools available to even the unsophisticated intruder. Now is the time to establish a "Cyber-Neighborhood Watch" and use that asset to protect the fledgling new electronic economy from the threat of Cyber-terrorism.

1309 'S' Street S.E.
Washington, DC 20020-6925
Phone: +1 (202) 503-9766
Fax: +1 (202) 315-3511
http://www.**InfoBro**.com/
info@**InfoBro**.com