

“The attitude that digital security is someone else’s problem, or is something to be addressed after the real work gets done, is pervasive in the business world.”

**Thomas J. Parenty
Harvard Business School**

“During the summer of 2001, a tiny computer program known as the Code Red worm burrowed through a security hole in Microsoft’s server software to infect hundreds of thousands of computers around the world. Many companies lost the use of their networks; some had to take their Web sites off-line. The total bill for cleaning up the mess has been estimated at a whopping 2.6 billion.”

**Article by Robert Austin and Christopher Darby
in the Harvard Business Review**

“When it comes to digital security, there’s no such thing as an impenetrable defense. But you can mitigate risks by following sound operating practices.”

**Robert Austin
Christopher Darby
Harvard Business Review**

Information Security

Ten Questions That Need To Be Answered

Courtesy of
Charles H. Le Grand
Institute of Internal Auditors

ACCOUNTABILITY

- ✓ **What management system has been established to assure effective assignment of accountability for the security of your information and supporting technology resources?**

AWARENESS

- ✓ **What has management done to ensure that all parties know, understand and accept the importance of adhering to sound information security?**

ETHICS

- ✓ **What has management done to ensure that your organization is using information assets and administering information security in an ethical manner?**

MULTIDISCIPLINARY CONSIDERATIONS

- ✓ **What has management done to ensure that the perspectives and consideration of all interested and affected parties are considered and balanced in developing your information security policy?**

PROPORTIONALITY

- ✓ **What cost/benefit, risk and due care analyses have been applied to the selection of your information security controls?**

INTEGRATION

- ✓ **How has management coordinated and integrated information security with overall policies and procedures to create and maintain effective security throughout your information systems?**

TIMELINESS

- ✓ **What capabilities do you have to ensure that failures involving information technology or its management will not endanger the organization, its supported business units, its neighbors, or their information assets, and will not impair their ability to operate?**

ASSESSMENT

- ✓ **What capabilities do you have to ensure that risks associated with information and supporting technology resources are effectively assessed on an appropriate periodic basis, or as otherwise required, and managed accordingly?**

EQUITY

- ✓ **How does management ensure that information security measures are fair and legal?**

INFORMATION SHARING

- ✓ **How effectively does management share appropriate information with peer organizations and appropriate governmental entities?**

SUMMARY

The goal isn't to make computer systems completely secure – that's impossible – but to reduce the business risk to an acceptable level.

Business managers should focus on the familiar task of managing risk at an acceptable level.

THANK YOU!!!

H.A. “Red” Boucher & Assoc.
Alaska Information Technologies
redbou@alaska.net