DataVantage®
Direct Computer Resources, Inc.

Memorandum

CYBER SECURITY

TO: Chief Financial Officers
FROM: Direct Computer Resources, Inc.
RE: Excessive Spending/Unclear ROI on Cyber Security

Do you feel like you spend too much on cyber security? Have you been cornered into funding the latest cyber security widgets and services to prevent the newest Threat du Jour? And still, you're not sure if you can prevent serious cyber consequences. Do you know:

- At what level of exposure information risk might impact financial statements, reputation and brand integrity for the next reporting period?
- Which security lapses might draw attention from regulators, investors, clients or depositors?
- How the President's recent executive orders and other prospective cyber security legislation will protect your shareholders?

No doubt you're overwhelmed by the fearsome rhetoric surrounding cyber security. You may think it's an IT issue and should be handled by your technical team or third-party service provider with all associated costs embedded within their ever-expanding IT budget. You are partially right.

The good news is that most data breaches can be avoided and their impacts mitigated through a program of common sense IT hygiene[1] and prudent financial protections. Your IT service contractor, Cloud provider or in-house team should be taking care of that for you.

But there is also an enterprise risk issue. Since the global financial environment in which we operate has become a complex, interactive system-of-systems, what was once a traditional IT management infrastructure has now become a real-time process control system…. And there may be high-impact[2] systemic risks and exploitable vulnerabilities with significant financial, brand and regulatory consequences.

It's easy to find out and it's not expensive to manage.

If you experience mounting system complexity and change from new systems and additional counterparties or have significant enterprise transition activities which might expose company private or client/depositor sensitive information (e.g. cloud adoption, M&A information system integration or mainframe to distributed environment conversions), you should search proactively for potential enterprise risk impacts. A practical regimen of Enterprise Risk Discovery helps quantify exposure and identify those Information Assets at risk. Post-discovery, you can allocate resources commensurate with exposure to prevent unnecessary costs, unwelcome 10Q commentary, adverse publicity and regulatory overreach.

Also seek answers from professionals who understand your business and stakeholders. Your IT professionals may be the "best of the best," but you still need a business-back perspective through the shareholder lens to gain the proper insight and to maintain a prudent enterprise risk position.

1 Non-Governmental Organizations, Trade Associations and Federal agencies, including the American National Standards Institute (ANSI), the Internet Security Alliance (ISA) and the National Institute of Standards and Technology (NIST) publish sound cyber-care guidelines and best practices.
2 Almost 50% of Global 1,000 companies lost 20% or more in share price in less than a month during the past 10 years - - some never recovered. Most major losses were as a result of a series of high-impact but low-likelihood events…" [Deloitte Report, Disarming the Value Killers — A Risk Management Study]

877.704.0077
www.DataVantage.com
info@DataVantage.com

Version 2.25.2013