book reviews

Net Attitude: What it is, how to get it, and why your company can't survive without it

By John R. Patrick.
Perseus Publishing 2001,
ISBN 0-7382-0513-3 $26.00.
Reviewed by Eugene Oscapella

John Patrick, Vice President of Internet Technology at IBM Corporation, has written a highly readable and enthusiastic book about the perils and benefits of e-business. As the promotional material for the book asks, "why do so many businesses crash and burn when it comes to launching successful e-business strategies?"

Patrick argues that the inability to harness the full power of the Internet has much less to do with the technology itself than with the cultural and psychological barriers that straitjacket thinking about it.

The book should well be of interest to anyone considering stepping into the world of e-business. The book has a certain evangelical fervour to it (not uncharacteristic, it seems, of enthusiastic Internet "techies") but is highly readable nonetheless.

Of particular interest to PL&B readers is Patrick's chapter dealing with "trust". "Of all the issues that will affect the future of the Internet," he says, "safeguarding personal information is likely to be the most important because it is at the heart of trust. It means that information about an individual needs to be handled in a way that is consistent with the privacy and security expectations of the individual." If not, he says, there will be no trust.

The benefit for the reader of Patrick's chapter on trust lies in its detailed explanation of much of the mind-numbing vernacular dealing with security and privacy on the Internet. Patrick discusses a range of terms, from the ubiquitous Internet "cookies", to P3P, to digital IDs, authentication, authorisation, integrity and non-repudiation. For those who attend privacy, technology and security conferences and walk away with a splitting headache after trying to assimilate these concepts, this chapter alone justifies the book's price.

For those who perceive an increasing depersonalisation brought about by conducting business over the Internet, take hope. Patrick says that "people will have a lot of e-meetings, but I don't think people will give up on meeting in person as a result. There is too much that would be missed."

Further info: www.netattitude.org

E-Business Privacy and Trust

By Paul Shaw. Published by John Wiley & Sons Inc. 2001

Many companies are now looking to e-commerce as an additional channel for increasing revenue. But this potentially lucrative sector has its risks, and businesses who fail to understand and act upon issues of trust, privacy, and security could be leaving themselves open to lawsuits, negative publicity, and most importantly, decreasing revenue through the loss of customers.

E-Business and Trust is set out as a step-by-step handbook aiming to guide companies towards the correct privacy policy for their business. The book addresses many issues, such as consumer expectations, creating and communicating privacy policies, and outlining the legal aspects of maintaining privacy and security.

Written by an expert in computer law, and an author of a number of e-business publications, *E-Business and Trust*, is a relevant guide for both owners of small-scale startups and IT managers in larger companies.

Further info: www.wiley.com

Continued from page 9

As the Staff Paper reveals, the Safe Harbor has inherent flaws that are unlikely to disappear easily. US companies remain reluctant to join Safe Harbor. The implementation deficiencies show that strict compliance is elusive. At the same time, FTC sanctions for non-compliance are doubtful and private dispute settlements are still hypothetical. These fundamental issues will persist while Safe Harbor is used as a substitute for missing legal protections in the US.

In the interim, however, the strategy may to some extent improve US data protection for the treatment of European data by US companies. The Department of Commerce has modified the self-certification form in a way that partially implements FAQ 6 on human resources data. The European Commission's approach also gives US companies a second chance to try to implement the Safe Harbor principles. Companies, however, are at risk if they continue failing to properly implement Safe Harbor. The Staff Report notes specifically that only through "vigilance and enforcement action" can Safe Harbor be "credible and serve its purpose". Companies participating, and those contemplating joining, clearly have much work to do for satisfactory compliance. In addition, the response at the Member State level by the data protection supervisory authorities may not be as forgiving as this preliminary assessment by the European Commission. In any case, the European Commission is still required to make a full re-evaluation of Safe Harbor next year as mandated by Commission Decision 520/2000/EC.