Killer apps - and YOU’re the dead meat

G. Mark Hardy, Guardent, Inc.

As our computing model shifts from a well-controlled client-server model to that of the active desktop, a flood of dangerous and malicious code is now coursing through enterprise networks. From Melissa to ILOVEYOU to the next attack, our traditional means of screening out malicious code seem to be letting a lot through. We’ll take a look at the most significant attacks of this past year, see how well (or poorly) the security infrastructure responded, and provide recommendations as to how you can better protect yourself in the future.

Mr. Hardy has worked in the information security industry since 1976, consulting to government, military, and commercial clients. His professional background includes information security planning and policy development, data encryption and authentication (including breaking commercial cryptographic algorithms), software development and strategic planning for electronic commerce, and writing commercial risk assessment software. He was the principal spokesman for both Secure Computing Corporation and AXENT Technologies, Inc., speaking at over 100 conferences, shows, and seminars over the past three years. Mr. Hardy has served on three ANSI security committees (X12, X9F, and X9E9), writing security standards for electronic commerce and the financial industry. He has developed security plans for several U.S. military commands in the United States and Europe, and developed the communications security encryption requirements for a military satellite program. A popular speaker, he also writes about security issues, and is the primary author of the Information Security Handbook for Enterprise Computing and the Client/Server Security Handbook, and was a contributing author to Network Security Secrets. A graduate of Northwestern University, he holds a BS in Computer Science, a BA in Mathematics, and a Masters in Business Administration.