zixcorp

News Release **For immediate release**

Zix Corporation Study Reveals Many Healthcare Industry Organizations Unaware of Their Non-compliance with New HIPAA Regulations

Audit of email from 7,500 healthcare organizations shows transmission of protected health information using non-secure email is high in certain segments

DALLAS — June 5, 2003 — Zix Corporation (ZixCorp™), (Nasdaq: ZIXI), a global provider of e-messaging management and protection services, today announced the results of a recent study conducted by its ZixResearch Center, revealing that many leading healthcare organizations are transmitting email messages containing federally protected health information over public networks without using appropriate safeguards, contrary to recently implemented regulations.

The study analyzed a sample of over 4,400,000 email messages sent and received by over 7,500 healthcare organizations, representing the inbound and outbound traffic for approximately seven days for each of the audited organizations, to determine what percentage of such messages contained protected health information. The study found that on average more than 53 percent of the top 100 U.S. healthcare chains and health systems, as well as 35 percent of the top 60 healthcare payors, had transmitted via plain-text email, information that these organizations are required to protect under the Health Insurance Portability and Accountability Act (HIPAA). Overall, 4.4 percent of outbound email that was analyzed contained protected health information, with the organizational totals ranging from 1.9 to 11 percent. The study covered unencrypted email traffic from organizations that had implemented a number of different kinds of solutions, including a variety of technology solutions, a reliance on directives to employees or internal policy-only solutions, and a combination of these measures.

“One implication of these findings is that while some organizations have clearly found an effective way to meet requirements, others may have implemented solutions that are not working as expected,” said Jeffrey Fusile, partner with PricewaterhouseCoopers’ HIPAA Advisory Services Team. “They may be relying on encryption to meet this requirement without developing policies requiring that the encryption solution be used, or they may not be adequately enforcing their policies.”

Another important fact to note is that records of unprotected email are created wherever the email is sent. Each time a healthcare organization sends an email containing protected health information without the appropriate safeguards to another party, a record of the event may

-more-

reside indefinitely on the recipient's email server or in its archives. Once such a record has been created, it may be used as evidence of noncompliance by governmental regulators or by lawyers seeking to use it in civil litigation. "Email has been crucial evidence in a lot of high-profile lawsuits, and many defendants have been surprised when messages they had deleted from their own systems come back to haunt them from other parties' archives," said John R. Christiansen, an attorney at Preston Gates & Ellis LLP.

"What's troubling about these results is the fact that organizations may not be in compliance with HIPAA, and may not realize it," said Daniel S. Nutkis, vice president, strategy and products of Zix Corporation. "While there have been many public statements and industry surveys asserting healthcare organizations are in compliance with HIPAA, studies like this show that organizations may not be aware of their actual email practices. They may not realize that they are sending high volumes of protected health information without protection, or that their employees are not using an appropriate technology solution or following protective email policies. At the same time, it is important to recognize that many organizations have implemented appropriate technologies and policies and are managing their email risks and HIPAA compliance, thus demonstrating that it can be accomplished."

Nutkis noted that a comparison of the results of this study, which provides a snapshot of email usage after the April 14, 2003, HIPAA compliance date with the results of an earlier study done before the HIPAA deadline, indicates that there was a reduction in the percentages of emails containing protected health information sent without encryption. This reduction may reflect that the passing of the compliance deadline has had some effect in developing greater awareness of risks and adoption of appropriate solutions.

The results reported here are based on aggregated statistics derived from information captured during routine customer-commissioned audits by ZixAuditor™, Zix Corporation's email assessment service. The data set analyzed in this study was identified by domain name and categorized in groups of no less than 50 organizations to ensure that any individual organization's compliance could not be ascertained. This method was used to ensure the anonymity of audit participants and their trading partners. ZixAuditor can inspect email messages for specific terms, or in the case of HIPAA, a combination of terms, that would indicate the presence of PHI. It then categorizes the results by type of violations for reporting purposes. Nutkis noted that when ZixAuditor looks at the emails submitted by a participating

-more-

organization, it is reviewing emails generated by the audited organization (i.e., outbound), as well as emails received by that organization from third parties (inbound). The ratio of outbound to inbound messages analyzed is two to one. Information collected at a customer's request for an audit is kept strictly confidential and highly secure during the ZixAuditor analysis and then destroyed in accordance with the ZixAuditor Data Disposition Policy. Only the anonymous statistical data generated by the analyses is then aggregated for the purpose of the overall study.

The study demonstrates how easy it is for an organization's email to be scrutinized by its business partners, once an email is transmitted to them. "Any organization's security strategy and the degree of its effectiveness will be obvious to all of its business partners," said Nutkis.

ZixCorp's audit tool has been in use for more than one year and its accuracy is continuously validated, using a methodology developed by the Hart eCenter at Southern Methodist University. More information on ZixAuditor can be found at www.zixcorp.com/zixauditor.

To assist organizations in better understanding the risks associated with protected health information and email, and for more information on the study, Zix Corporation has produced a white paper on the subject available without charge at www.zixcorp.com/riskstudy.

About Zix Corporation

Zix Corporation (ZixCorp™) is a global provider of e-messaging management and protection services. ZixCorp offers a portfolio of managed on-site and hosted e-messaging solutions to protect organizations from viruses, spam, and electronic attack, while delivering the ability to enforce corporate policies and securely send to anyone. ZixCorp's advisory services and secure e-messaging solutions enable organizations of any size to streamline operations, avoid obsolescence, mitigate risks, and leverage the cost and time efficiencies of e-messaging. For more information, visit www.zixcorp.com.

###

Contacts:
Media Contact: Whitney Gilliam, ZixCorp, (214) 515-7338, wgilliam@zixcorp.com
Investor Contact: Beverly V. Fuortes, ZixCorp, (214) 515-7357, invest@zixcorp.com