Protection Paramount When It Comes to Email Security

Kentucky Retirement Systems proactive in its approach to email encryption

At a Glance:

- *Kentucky Retirement Systems (KRS), Frankfort, Ky.*

Background:

- *Created in 1956 by the Kentucky General Assembly*
- *More than 300,000 members*
- *1,399 agencies involved*
- *250 employees*

Issue:

- *Needed email encryption to send members' personal information*
- *Wanted to scan both outbound and inbound email for data breaches*

Solution:

- *Zix® Email Encryption*
- *ZixGateway® Inbound*

Benefits:

- *Secure messages sent directly to recipient's email inbox*
- *Strong HIPAA and finance lexicons*
- *Strengthens HIPAA compliance*
- *Easy to use for end-users*
- *Transparent to other Zix customers*

When you offer both health insurance and retirement related financial services to more than 300,000 members, ensuring their personal information is protected is the highest priority.

Kentucky Retirement Systems (KRS) takes this goal very seriously. It has put in place rigorous data protection policies at all levels of operation.

> "We are fully committed to securing every member's personal information."
>
> *– Mike Burnside, Executive Director, Kentucky Retirement Systems*

"We are fully committed to securing every member's personal information," said Mike Burnside, KRS' Executive Director. "We're proactive about protecting this type of data and try to go above and beyond what's expected. It's the right thing to do. Our Board of Trustees is also actively involved in ensuring the protection of our members' information."

KRS is the public pension system for almost all of Kentucky's government and public employees, with close to 1,400 employers paying into the retirement fund. For members who are 65 and older, it's also a self-funded health insurance entity covered by the Health Insurance Portability and Accountability Act (HIPAA).

Early need for encrypted email

"Early on we identified email as an area that needed to be addressed," said Mark McChesney, KRS's Information Security Officer. "People appropriately talk about social networking sites being dangerous in terms of security, but the critical application for us is email because it's simple to use. Email is the way people communicate, and it's an easy way to inadvertently expose data. There's lots of opportunity for bad things to happen with unsecured email. Email is certainly something you should be encrypting."

KRS carefully researched email encryption solutions and chose Zix. "Probably one of the most significant changes and improvements in our infrastructure has been the addition of the secure email solution," McChesney said. "The biggest point of exposure we've had, whether it has

About Zix

Zix is a trusted leader in email data protection. Zix offers industry-leading email encryption, a unique email data loss prevention (DLP) solution, and an innovative bring your own device (BYOD) email solution to meet your company's data protection and compliance needs. Zix is trusted by the nation's most influential institutions in healthcare, finance and government for easy-to-use secure email solutions. For more information, visit www.zixcorp.com

been internal or with our business associates and partners, has been emailrelated. The secure email solution we implemented was the best one for us, because it let us have both manual and automated controls in place."

Inbound email scanned for potential breaches too

While KRS implemented the Zix Email Encryption for automatically scanning and encrypting outbound email sent by its 250 employees, it also scans inbound email from its business partners and associates to check for personal information, such as Social Security Numbers, members' names, birthdates, addresses and account details.

"Like many organizations, we use the system's financial and HIPAA lexicons to pick up any unencrypted sensitive data," said McChesney. "Where we're unique is that we also use it to look for breaches in incoming email. This way we can ensure we're really protecting our members' information."

The security staff receives a daily report from ZixGateway® Inbound which identifies unencrypted inbound email sent by business associates and partners with compromised data. An incident report is opened to document the breach, and the business associate or partner responsible for the violation is notified. A disclosure letter is then sent to affected members.

"With inbound scanning, we've been able to identify potential vulnerabilities from business associates and have been able to proactively notify our members that their data has been exposed," said Burnside. "We've also used it as a tool to work closely with our business partners and employers to educate them on the importance of communicating with us securely. This is significant, because under the new HIPAA regulations, business associates are now held accountable for data breaches."

Business associates now targeted by HIPAA

Stiff punishment is being handed out to healthcare organizations and their business associates not abiding by the strict new HIPAA regulations under the Health Information Technology for Economic and Clinical Health (HITECH) Act, passed as part of American Recovery and Reinvestment Act of 2009. Under the legislation, organizations can be fined $1.5 million — up from $25,000 — for violating patients' privacy. Previously, business associates weren't held accountable.

For KRS, safeguarding email sent by its employees wasn't enough — this organization wants to protect its members from breaches inadvertently made by its business partners too.

"It's really important to look at an encrypted solution for your email that scans both outbound and inbound traffic for potential data breaches," said McChesney. "You owe it to the people you serve."

zix
Phone 866-257-4949
sales@zixcorp.com
www.zixcorp.com