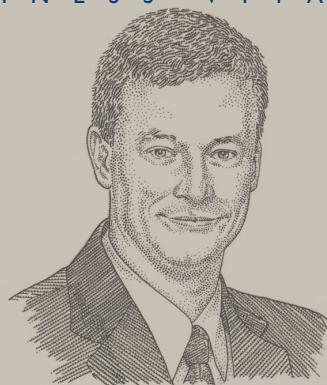


Prying Eyes

Do you have any idea who is reading your email? Organizations are dependent upon email to conduct business, sharing confidential information on an ongoing basis. Dependency has bred complacency and created a major security risk that threatens companies and careers. If not managed properly, email is an open invitation to prying eyes and malicious actions.



Todd Ray is a Business Vitals CIO consultant who helps organizations with issues that threaten information security and business survival.

What is an organization's biggest IT security risk?

Without a doubt, it's email.

Organizations rely on email to share all types of proprietary information such as proposals, contracts, legal documents, salary and hiring information. The question becomes: who is reading the email and how are they using the information? One compromised email can bring down a career or a company.

Why should one assume someone other than the intended recipient is reading email?

Email is so ubiquitous; we have a tendency to take it for granted. A common misperception is that email messages are like letters in sealed envelopes, when in fact they are more like postcards visible to anyone's eyes. This creates opportunities for unintended recipients to read email, a serious security risk. Recently, a CEO of a major company was relieved of his duties because someone other than the intended recipient read his email and used it against him.

Are my own employees a threat?

As much as we'd like to trust the people who work for us, there will always be disgruntled, careless, or bored employees who use access to IT systems to read things they don't need to read. Some are willing to use it for malicious intent.

Why is it so easy to compromise email security?

Many companies choose to manage their own email on an internal server. Right away, there's a security risk because people within

the organization have access and the opportunity to read every email generated. With one click they can share confidential information with co-workers, competitors, the media, you name it.

How real is the threat?

A recent study on security breaches by the Ponemon Institute found that 69 percent of companies reporting serious data leaks attributed it to either malicious employee activities or non-malicious employee error, versus 16 percent of data leaks linked to external forces.

What should an organization do to secure the confidentiality and integrity of their email?

Companies can put a stop to this common security issue by outsourcing the management of their email, enterprise wide or executives only, to a secure third party like Business Vitals. Under our management, which includes our Secure Operations Center and Certified Information Systems Security Professionals, companies are guaranteed that no unauthorized person will see the contents of email. All email is backed up and stored so important correspondence is never lost. Anti-virus and anti-spam protection also is included.



Business
VITALS™

888.287.8483

www.businessvitals.com