



Trust Matters To Cigna

Benefits provider toes that fine line between providing access to health information and protecting sensitive data.

By Larry Greenemeier, [InformationWeek](#)

Sept. 12, 2006

URL: <http://www.informationweek.com/story/showArticle.jhtml?articleID=192700121>

When it comes to IT security, **Cigna** faces a clash of demands. Its customers--the companies to which Cigna provides employee health benefits services--and their employees want more online access to their benefits information, but that data is some of the most sensitive and heavily regulated information available. Cigna, like many companies in health care, is left searching for ways to provide data while ensuring that it's secure and in line with all privacy and other regulations.

Executive VP Scott Storrer realizes Cigna, which ranks 17th on this year's [InformationWeek 500](#), needs to provide a continuous stream of new services to customers: Cigna's myCigna.com portal lets health care consumers do a side-by-side comparison of the quality and cost of local health care facilities. Last year, it developed a myCigna.com tool that compares the cost of prescription drugs at different pharmacies. But Storrer knows that only secure IT systems can deliver this sensitive information without risk of loss or theft. "We very much want to be seen as a trusted adviser rather than an HMO or gatekeeper," he says. "We can't do this if there are trust issues regarding customer data."



Illustration by Carl Weins

Cigna deals with this conundrum by taking the long view on potential problems. Data theft has been a huge problem this year for many companies, with several highly publicized thefts of laptops containing personal data. These crimes have embarrassed the businesses and government agencies involved and cost them millions of dollars to notify customers, answer questions, and pay for credit monitoring. Cigna is getting ahead of such problems by encrypting all of its portable data and sensitive backup files, an effort that's a lot easier to plan than it is to execute. "It's still an evolving technology," says chief information security officer Craig Shumard, a 25-year veteran of the company. "There's no easy way to roll out encryption."

The health benefits provider uses secure File Transfer Protocol when it exchanges large files with business partners. It also uses secure e-mail and Microsoft Encrypting File System on desktops and laptops. But workers don't rely just on PCs these days to do their work; increased use of removable

media to transfer data challenges encryption efforts. Cigna addresses this in a number of ways, including the use of the WinZip Windows compression tool for CD encryption and technology from Verdasys that encrypts data sent to removable devices. The keys to decrypt data are stored on PCs and laptops into which USB devices plug in. "We don't want people storing data on machines that don't have our security controls," Shumard says.

The Hard Part

Microsoft Encrypting File System hasn't been foolproof. Retrieving decryption keys after a PC has been hit with a virus or is otherwise incapacitated can be difficult. Shumard is looking forward to a time when encryption and decryption are done automatically through logic coded into system hardware, without requiring admins to manage keys. Cigna is interested in the encryption capabilities to be featured in the upcoming Windows Vista operating system; the BitLocker Drive Encryption is supposed to encrypt and protect data on PCs and servers that have been lost or stolen, or whose hard drives weren't properly scrubbed before being decommissioned or resold. But having just finished its Windows XP deployment a year ago, a Vista migration won't make Cigna's to-do list for a few years.

Cigna has been using Zix's e-mail encryption services for four years to protect sensitive data--it processes 70 million benefits claims annually. E-mails that senders designate as "secure messages" in the cc: or bcc: field are sent through an encrypted tunnel to Zix's systems. A message then goes to the intended recipient, who must log on to Zix's system to retrieve the message. It's up to users to determine which e-mails to designate as secure and to follow company policies governing them.

Cigna uses Symantec's Sygate network access-control technology to ensure that any device connecting to its network has the right level of antivirus protection. Cigna also has segmented its network into a number of security zones, each of which requires access privileges to enter. In 2004, IBM Global Services helped Cigna design and develop the architecture, and Cisco last year began implementing it. The zone system limits roaming on the company's network.

Cigna upped its data security capabilities last year, while reducing expenses by 35% and trimming information security staff by 47%. This came largely through centralizing some functions within its Information Protection division and outsourcing others such as logon ID and password management to IBM Global Services.



Among the changes: The Information Protection unit adopted a more centralized model and increased its interaction with the company's business units. Cigna created roles within its business units known as IP (Information Protection) champs and IP coordinators. Champs are senior-level business managers who agree to use their status in the company to bring security matters to the attention of Cigna's top executives. "We talk to senior managers to make sure we're working on the issues that are on their radar screens," Shumard says. "We take their concerns and factor them into our overall risk assessment that's used to create a security road map."

IP coordinators are business and IT managers, such as a claims manager in a branch office, who act as the eyes and ears within their business units to report security problems and concerns.

Cigna hopes this chain-of-command, communication-oriented approach will keep people alert to problems. Such an approach could have helped prevent the theft of a Veterans Affairs Department laptop containing 26.5 million records from an employee's home and the confusion that followed. The

employee whose laptop was stolen and later recovered had been taking sensitive data home for years, but the VA didn't have a clear policy regarding the removal of sensitive data from its offices, so no one did anything about it. In another lapse of communication that a chain-of-command approach might have prevented, VA Secretary James Nicholson says he wasn't told of the theft until weeks after it happened.

Security's In the Details

Shumard's role as Cigna's chief information security officer has changed dramatically since the job was created in 1999. In the late '90s, the main focus was beating back viruses that could bring down computers and disrupt business. "Little thought was given to identity theft, misuse of intellectual property, hackers, or trusted computing," he says.

Combating these threats requires knowing as much as possible about who's using your company's systems and what they're doing while they're logged on. "We're focusing on [creating] trusted users and making sure that the people we've credentialed and given access to continue to use that access appropriately," Shumard says.

Cigna maintains an audit path to track where users go in its systems; admins use Verdasys' Digital Guardian to control application and storage device usage, network communications, clipboard cutting and pasting, and printing. It warns admins about how devices are being used and can block usage if necessary. Digital Guardian is helping the company meet regulatory requirements, such as Sarbanes-Oxley and the Health Insurance Portability and Accountability Act.

Looking ahead, complexity will continue to be the enemy of security at Cigna. IT systems loaded with new features and capabilities are great for employees and customers, but "it really causes a lot of angst" for tech managers, Shumard says.

Cigna is implementing a federated identity management system that will let customers log on to the system and go to their employer's benefits page without having to go through a second logon. This is convenient, but "what goes on behind the scenes to do this is fairly complicated," Shumard says. "We need to make sure that as we establish a circle of trust with your company that we don't do anything to jeopardize the integrity of the data or your privacy."

Cigna's information security progress over the past year indicates the company is up to the challenge. Still, with stolen personal data commanding a premium among criminals, Cigna will need to keep looking over its shoulder.

Data Lockdown

Cigna must offer its 9 million members more online transparency and access to their health and benefits information, while ensuring the privacy and security of that information. Last year, the company developed and implemented an operating model that improved the integration of information protection with business processes. The rollout included:

- Processes for application and desktop logging and monitoring with centralized reporting
- Role-based access for 30,000 users
- Automatic desktop encryption of all files
- Comprehensive incident response
- Tools and processes to protect sensitive external e-mail
- A compliance monitoring program

- Security event monitoring and correlation from multiple sources

Cigna also developed a strategy to facilitate secure offshore business process outsourcing, reduced systems access setup time by 60%, and minimized business disruption using an incident-response process, intrusion detection, and virus and spam controls.



This story was updated Sept. 12, 2006.

[TIFF & PDF Image Viewer](#)

Display, annotate, clean-up, edit, navigate & print images in browser.

www.pegasusimaging.com

[Ribbit for Salesforce](#)

Voice to Text Transcriptions Try our 30 Day FREE Trial Today

www.ribbit.com/salesforce

[Service Catalog Kit](#)

IT Service Catalog best practices. Free Kit with White Papers & More.

www.newScale.com

[IT Infrastructure](#)

Find Out How to Improve Performance of IT Process Whitepaper.

www.Tripwire.com

Ads t

Copyright © 2007 [CMP Media LLC](#)