

Security solutions in one place.

INSURANCE & TECHNOLOGY

Message Mania

Nov 01, 2006

URL: <http://www.insurancetech.com/showArticle.jhtml?articleID=193501093>

E-mail and instant messaging (IM) have become ubiquitous business tools and are part of almost everyone's daily routine. For insurers, the technologies provide easy ways to share information with distributors and employees, communicate effectively with customers and agents, and help claims adjusters transfer files to turn around claims -- all in real time.

But hackers, phishers, pharmers, spammers and other criminals all are out to score consumers' private data, and, unfortunately, lacking or substandard security for e-mail and IM leaves many insurance companies vulnerable to leaking clients' Social Security numbers, addresses and medical records, according to Ted DeZabala, principal in the enterprise risk services practice at New York-based [Deloitte](#). "E-mail and IM introduce challenges into the IT environment," he says. "Viruses and worms can be transmitted through them, and when you are dealing with very sensitive data, and the protection and privacy of customer data, security is a big deal."

Adding to the challenge of securing customer data from the bad guys outside their walls, insurers also have to protect the information from internal threats. While internal threats can include employees who steal data for personal gain or expose it for malicious purposes, such as corporate espionage, internal security breaches often are the result of employee errors or oversights. The lack of proper procedures and guidelines for e-mail and IM usage -- or employees' lack of knowledge of such policies -- can expose sensitive data inadvertently. For example, well-intentioned employees may e-mail data to themselves so they can do additional work at home on weekends.

Further, insurers' relationships with outside providers can complicate e-mail and IM security. While a convenient means to communicate with and transmit data to business partners, e-mail and IM may not be secured with the same diligence at every firm. In addition, offshore outsourcing providers may reside in countries with different security standards and regulatory requirements.

Facing Threats

"Companies, in general, wrestle with any electronic means to take information out of the organization," observes Don Garvey, chief information security officer for Warren, N.J.-based [Chubb Group of Insurance Companies](#) (\$48.1 billion in total assets). "Any mechanism that allows information to flow outside of your control is a threat." Often, however, insurance companies have failed to monitor e-mail and IM usage properly.

The brunt of the responsibility for ensuring compliance and acceptable security procedures usually falls on the CIO, something to which Kevin Murray, CIO of New York-based [AXA Financial](#) (\$9.6 billion in annual revenue), can attest. "I have to make sure that our customer data is protected," he says. "We have an obligation to our customers to keep that data safe." Proper e-mail and IM security measures -- including both technology solutions and formalized procedures -- can help protect customer data against theft or loss, protecting carriers from litigation costs and decreased credibility resulting from a data breach, while helping them comply with customer privacy regulations such as the Health Insurance Portability and Accountability Act (HIPAA), Gramm-Leach-Bliley (GLB) and Sarbanes-Oxley (SOX).

To protect their networks, CIOs have created barriers using a variety of security products. Traditional security solutions include firewalls, offered by vendors such as [Cisco](#) (San Jose, Calif.); intrusion-detection applications by companies including [Oracle](#) (Redwood Shores, Calif.); authentication software from vendors such as [CA](#) (Islandia, NY); and biometric devices and electronic tokens provided by vendors such as [RSA Security](#) (Bedford, Mass.) and [Alladin](#) (Chicago). Still, 84 percent of organizations in North America have suffered security incidents in the past year, according to a CA study in which 84 of the 642 respondents were from financial services organizations. The study also discovered that the greatest losses to insurers due to security attacks are productivity, along with loss of trust, damage to reputation, embarrassment, loss of confidential information and loss of business revenue.

But as the cost of security lapses has become more evident, insurers have begun to address vulnerabilities related to the use of e-mail and IM with the addition of encryption software from providers such as [PGP](#) (Palo Alto, Calif.); spam filters from firms such as [CIPHERtrust](#) (Sunnyvale, Calif.); anti-virus software by companies including [IBM](#) (Armonk, N.Y.); and content monitoring applications from companies such as Verdasys (Waltham, Mass.) to the security mix. "We did a study of our own, and 87 percent of the e-mail that comes into our building is spam," relates Charlie Carter, CIO for [Grange Mutual Insurance](#) (\$1.6 billion in total assets) in Columbus, Ohio. "If you consider what it potentially is bringing in [such as viruses and worms], it gets worse. So it is a major concern for our IT [department]."

Balancing the Good With the Bad

For the modern insurance enterprise, then, the challenge becomes balancing the productivity gains offered by e-mail and IM with the security threats they introduce and the costs of mitigating these risks. But carriers' IT departments tasked with increasing security around e-mail and IM typically face limited budgets. "IT security has had limited resources as electronic data became more important, and IT security wasn't given the statutes to keep up with the evolving technology," according to Kevin Kalinich, managing director of professional risk solutions at [Aon](#) (Chicago). "In 2001 and 2002, carriers knew what to do, but they didn't have the resources until 2005 and 2006 -- after carriers, such as AIG, started losing information."

In 2005, according to Ray Wagner, research vice president at [Gartner](#) (Stamford, Conn.), the average IT organization allotted 4 percent to 6 percent of its budget -- or about \$30 million -- to security. "The highest-security organizations are balancing security within their budget," he explains. "Those companies putting more money into security spending are ensuring that they stay out of the headlines."

Chubb uses a balanced approach to security spending within its IT budget, according to the carrier's Garvey. "Quantifying how much to spend on security is hard," he acknowledges. "IT spends more and more every year on tools to meet security needs and compliance, and it isn't always spent by the security department." For instance, customer analytics software may have added security functionality.

In addition, at Chubb, keeping security initiatives a priority also means investing part of its IT security budget on employee security education and creating a corporate culture that fosters employee awareness of the insurer's security standards. "We permit our employees to use e-mail for personal use, and if someone wants to use IM, we don't block it," relates Garvey. "However, we do give our employees guidelines because, for the most part, the bigger risk is not the employees doing a malicious deed; it is the employees who make bad business decisions."

Chubb has developed an educational program for employees on the use of e-mail and IM. If employees are sending information outside of the company for business reasons, it must be encrypted in some way. "If information is not encrypted and it is then forwarded to 10 other people, then there is a problem," says Garvey. "So we focus on purchasing the technology that can really lock that information down."

To limit the amount of confidential information that leaves the organization, Chubb has built its own internal authentication and reporting system, and the carrier uses PGP encryption to protect data leaving the company. Employees who want to take work home can send the files through secured BlackBerry devices from Waterloo, Ontario-based Research in Motion or through laptops that the carrier provides to employees. "It all boils down to recognizing emerging technologies and having an active and robust awareness about our security and the prominence of the information we deal with on a daily basis," says Garvey.

Of course, one way to eliminate security vulnerabilities arising from a technology's use is to ban the technology. To ensure compliance with the SEC's e-mail capture mandate, for example, AXA Financial has chosen to ban IM from being used on all company computers. "There can be advantages and disadvantages to allowing IM, but we've opted not to allow IM," relates AXA's Murray. But, he points out, "We have spent a lot of time, energy and investment to capture every e-mail to be in compliance with SEC legislation."

"Compliance can help quantify risk," says Aon's Kalinich. "If a company can determine its compliance to HIPAA, GLB and SOX, then those are good benchmarks to get entities to a minimum standard" for security protocols.

Deloitte's DeZabala stresses, however, that security efforts must go beyond compliance requirements. "Security needs to be embedded throughout the organization and the infrastructure that supports compliance efforts," he says.

AXA Financial's efforts include a pilot utilizing biometric smart cards to log on to laptops and e-mail. The devices then ask for both a password and a fingerprint scan for user authentication. "You can't get into the system without the biometric smart card, and we also use security tokens for gaining entrance into the network," says Murray.

To further protect customer data, Murray has set up AXA's security system in three levels. "You really need three levels of security," he says. According to Murray, AXA Financial's first level of security includes perimeter security, firewalls and spam protection. The second level is made up of network security programs, antivirus scans and authentication that will "allow gateway to the Internet," he explains.

But it is AXA Financial's third level that ensures the carrier maintains compliance. IT uses software to scan both inbound and outbound e-mails with a rules engine to pick up suspicious e-mails, Murray relates. The rules engines are programmed to flag suspicious keywords and phrases. All company e-mails are captured using [AXS-ONE](#) (Rutherford, N.J.) compliance and surveillance software, which

encrypts and stores e-mails on direct-access storage devices for regulatory purposes. Still, Murray says, "I'm constantly looking for better security because you can't let your guard down."

Monitoring Outsourcers

Keeping your guard up includes monitoring the security practices of business partners. Most insurers outsource both onshore and offshore. While onshore outsourcers are subject to compliance with the same U.S. privacy laws to which insurers are subject, offshore outsourcers may have different requirements, according to Mark Lobel, partner in advisory practice information security at [PricewaterhouseCoopers](#) (PwC; New York). "A survey we conducted showed that controls in India are not at the same level as the U.S.," he contends. "At least half of the respondents we interviewed admitted they were not compliant with information security."

Because offshore outsourcers are not subject to the laws of the U.S., an insurer could potentially be burned if outsourcers do not use the same standards for IM and e-mail security. That is why many insurers include security within outsourcing contracts and even monitor outsourcers' interactions along with all of the e-mail and IM users in the company. "Since companies do not have the same laws in India, outsourcing contracts are tighter now, and many times carriers conduct audits and assessments and even set up their own network at outsourcing firms to monitor" e-mail and IM usage, says Aon's Kalinich.

Philadelphia-based [Cigna](#) (\$44.9 billion in total assets) uses content-monitoring technology to prevent sensitive customer data from being exposed in e-mails and IMs with its offshore providers, according to Craig Shumard, the carrier's chief information security officer. "Data containment is a growing issue," he observes. "We use [content monitoring] extensively with offshore partners to control data. We focus on the trusted user because 70 to 80 percent of the threat is internal."

To protect its intellectual property from leaving the company and ensure regulatory compliance, all outbound e-mail at Cigna is filtered and monitored. According to Shumard, the carrier uses IBM's Sametime, an internal IM system that scans desktops for unauthorized IM programs, as well as antivirus and spam guards from [Symantec](#) (Cupertino, Calif.). Further, Cigna blocks Web-based e-mail to ensure the system does not become vulnerable to viruses or worms. Additionally, the insurer uses [ZixCorp's](#) (Dallas) e-mail encryption software, which allows employees to choose whether each e-mail should be encrypted or not.

Shumard notes that Cigna offshores some application development and, because it has such an extensive security network in place domestically, the carrier made sure that security was part of the contractual agreement. Cigna also purchased Verdasys content monitoring, which does not allow sensitive information to be copied or pasted into e-mail or IM, burned onto CD or put onto any other removable devices. "Because we knew there was a significant risk, we looked at Verdasys as an enabler," says Shumard. "It proved to be very successful to us to be able to monitor what is going on, contain data, utilize encryption and enforce policies around removable media."

IM Security Solutions Emerging

The top security technologies that financial institutions are planning to deploy over the next 18 months are single-sign-on capabilities (29 percent), biometrics devices (21 percent) and instant messaging security applications (19 percent), according to a survey of 150 global financial institutions by New York-based Deloitte. Sixteen percent of the top 50 insurance companies were represented in the study.

While the benefits of single-sign-on solutions and biometrics generally are understood, according to Ted DeZabala, principal in enterprise risk services for Deloitte, IM security is a new challenge for insurers. Many companies do not have the software to protect their networks from IM-borne threats, or to retain and archive IM messages, he asserts.

"IM is a new challenge because most of the [traditional] virus software deals with straight e-mail," says DeZabala. "And although companies are doing archiving for IM, they may not be archiving IM for [regulatory] retention purposes." As such, it is not surprising that organizations plan to invest in IM-specific security solutions. --M.W.



[Copyright © 2004/5 CMP Media, LLC](#) | [Privacy Statement](#)