Insurance Times: Information Risk Management Assumes Higher Priority For Businesses
December 11, 2001, Vol. XX No. 25

by Mark Hollmer
InsuranceTimes

Insurers didn't always consider protecting business information – from interoffice communication to computer files – as important as other kind of risks.
But this is the information age, where the successful dissemination and protection of data over the Web or through a network can make or break a company.
And so the rules have changed, a local security expert says.
"Information security risks are becoming as important as other (kinds) of risks (and) businesses are recognizing this," said Bill Campbell, security director for Storage Networks in Waltham, Mass.
Campbell spoke about the role insurance places in information risk management during the Nov. 8 Industry Day at the Boston Sheraton, an annual meeting held by the Boston Chapter of the CPCU Society.

Risk Management
Insurance coverage of information technology is always written to cover new or missed risks, Campbell said – factors that aren't necessarily accounted for by risk management practices.
But, Campbell cautioned, many technological tools or policies companies use to manage their risks aren't exactly 100 percent effective.
Among his points:
• Firewall computer technology and anti-virus software must be updated regulatory because the programs evolve so frequently, he said.
• Virus protection can especially be "a waste of time and money" because it quickly becomes out of date.
• Companies are also foolish to believe that only certain employees have access to crucial information.
"In my experience," he said, "it's rarely true.
"There are relationships with vendors (and relationships) with customers that inevitably lead to information being shared with other folks."
• Company managers focusing on staff reductions are wrong to also reduce security staff.
Rather than reducing risk by reducing staff, Campbell said, layoffs or staff reductions can actually increase risk by leading to "disgruntled employees."
• Penetration testing — where companies hire a consultant to try and break into their internal network – ultimately falls short. Campbell said the system is flawed because consultants use "automated tools" and software that isn't "very intelligent" and can reveal "false positives."
A human consultant isn't much better here, Campbell said, because the person usually works under constraints and supervision.
"The constraints avoid legal liability so you're never going to see what a hacker sees," Campbell said.
Before seeking insurance coverage, Campbell said, managers should use employees themselves to identify and address vulnerabilities within a company.
Good company information-risk management focuses on even the little details, prioritizes potential risks and helps establish limited access to and control of information systems, he said.
Company managers should also make sure they're up on any software patches and program updates.
Whatever happens, an executive commitment to good risk management is a crucial factor for any company, he said.
"If an executive of the company is not willing to step up to the bar and make things happen," then risk management will be futile, he said.