

Insurance Times: 10 steps for cyber security

October 29, 2002, Vol. XXI No. 22

September 11th gave many corporations the impetus to respond to terrorist threats by scrambling to revamp their crisis management, emergency response and business continuity plans. A cyber loss control expert at the Chubb Group of Insurance Cos., however, warns it was a short-lived response and that companies need to increase their cyber security.

“Cyber-warfare is a real possibility given the skill sets and resources of today’s terrorists and cyber criminals. The threat of cyber-terrorism, push-button warfare and launching online bombs at corporate targets thousands of miles away is very real,” said James Tucker, assistant vice president, Chubb & Son, and loss control computer security specialist, Chubb Commercial Insurance.

“A successful cyber-security breach could result in significant financial loss, loss of market share, loss of reputation and a falling stock price, significantly impacting shareholder value. Taking a proactive approach to information and network security and investing money up-front through a top-to-bottom enterprise-wide cyber-risk assessment is a prudent step that will significantly reduce a company’s future exposures.”

Tucker said companies must remain on guard even after they think they have solved the problem.

“Throwing technology at the cyber-security problem is only part of the solution. Information security is like a snapshot, not a movie,” he said. “The picture is constantly changing. New security vulnerabilities emerge daily.”

To help companies respond to cyber-terrorist threats, Tucker recommends 10 steps for companies to take in designing an information and networking security program:

1. Don’t downplay the risk. Acknowledge that the cyber-terrorist threat exists and prepare for cyber-warfare.
2. Emphasize prevention over repair and invest in an enterprise-wide cyber-security plans.
3. Institute a corporate cyber risk management and information and network security assessment that includes representatives from all disciplines of the company, not just the information technologists.
4. Appoint a senior executive who will be responsible and accountable for the assessment and the security plan.
5. Establish trust within and outside the organization. Include supply chain, Internet service providers, business partners and vendors in the assessment plan and demand confirmation of the sturdiness of security systems.
6. Establish internal information security education, training and awareness.
7. Initiate security auditing, validation and measurement processes. Report all security violations, not just the major ones.
8. Use independent cyber-security expertise to test and validate security systems.
9. Protect critical servers. The Internet may provide easy and unwelcome access from outsiders.
10. Conduct a risk assessment and evaluate the cost-effectiveness of implementing protection. For example, evaluate the trade-off between how well and fast a Web site functions and security issues.