

NexTec Group, Inc.

BUSINESS APPLICATION SOLUTIONS FOR YOUR ENTERPRISE

White Paper: Security Concerns for Professional Services Organizations



Security Concerns for Professional Services Organizations

Look for security to be an even bigger concern than usual among clients for at least the next month or two as a book on Internet insecurity is promoted across the country.

IT organizations know how it is when a business executive comes back from a trip with the latest technology ideas from an airline magazine -- this is like that only more so. Anyone working in professional services should be prepared for an even greater concern than usual about security. This is a good time to update staff on some of the issues so they are prepared to answer questions from clients. When users are concerned about security, saying "I'll get back to you on that in a couple of days," is not the best answer.

Richard Clarke, the anti-terrorism chief under Presidents Bill Clinton and George W. Bush has just published *Cyber War*. Written with Robert Knake, a fellow at the Council on Foreign Relations, the book takes a macro view of security and threats from sophisticated hackers, especially those sponsored by governments, such as China. Clarke says that China has stolen billions in intellectual property from companies in the U.S., UK and Japan especially. He has been appearing on talk shows like NPR's *Fresh Air* and his book was prominently reviewed in the [Wall Street Journal](#) and the [New York Times](#).

Clarke and Knake show that Internet security is much weaker than most people appreciate. The breadth and depth of security problems will probably surprise many readers and listeners.

In 2007, the director of MI5 in England wrote to 300 English companies telling them their systems had been penetrated by the Chinese government. Canadian researchers found that the Chinese had hacked into the systems of groups supporting Tibet and arranged to turn on their computers' cameras and microphones in a way that users could not detect. The hack ran undetected for 22 months. Meanwhile U.S. intelligence discovered that the Chinese had set up ways to penetrate the American electric grid so they could pull it down at will. Someone, probably the Chinese, stole terabytes of data about the F-35 fighter, but since they encrypted the data on the way out, no one can even determine what they took.

While American cyber experts boast, privately, about their ability to hack into systems around the world and leave no trace, they appear oblivious to the possibility -- likelihood -- that others are doing the same thing to systems in the U.S.

The publicity from Clarke's book tour will probably elevate security concerns among clients. An annual study of security breaches by Verizon Business Services suggests that PSOs may uncover many security breaches that companies never knew had happened to them. It concluded that 9 out of 10 data breaches were avoidable with good security. Similar to the first study's findings, the latest study found that highly sophisticated attacks account for only 17 percent of

breaches. However, these relatively few cases accounted for 95 percent of the total records breached - proving that motivated hackers know where and what to target. The executive summary [executive summary](#), at the very least, is worth reading.

Finally, a recent book from IT Governance Publishing, "Assessing Information Security", offers a detailed guide to security issues. The three authors liken cyber war to real war, but they go beyond the occasional quote from Sun Tsu's The Art of War to include extended comments from other Chinese strategists, the German strategist Carl von Clausewitz and a more recent thinker, the US Air Force's John Boyd, designer of the F-16 and a big contributor to the Marine Corps' handbooks on strategy and war fighting.

Anyone can quote a few historical military strategists, but the three authors of Security Assessment go beyond that to draw sensible lessons about the dynamic nature of IT security and the potential to move from the defensive to the offensive -- luring in hackers and then taking disciplinary action against them if they are employees, or legal action if they are from outside. A key message is to secure the entire system against physical, social engineering and electronic intrusion and check the defenses constantly.

They offer a sensible methodology. In gap analysis, for example, they suggest that a firm take four steps:

- Business Operation and Politics -- what is critical?
- Threat Profile -- how can it happen?
- Threat Modeling -- how can it happen?
- Attacker profile -- who can and is interested to do it?

Security should always be a concern for PSOs since they often have access to confidential data and have often been the source of data losses -- think laptops with personnel information stolen from cars. Clarke's book and his promotional campaign will elevate awareness; the POSs prepared to discuss security issues intelligently with clients can benefit. The "Assessing Information Security" book is a good guide -- it might even lead to an expanded assignment!