

## **Session E13 – Hacking Evolution: New Trends in Exploits and Vulnerabilities**

*By Brian Christian*

### Topic Summary

Web applications by nature are dynamic and new features are added frequently. A security risk is imposed whenever a Web application is changed. Even the simplest change could pose a major threat to the assets of the company, or just as important, customer information.

To minimize the impact of threats, it is essential to have a plan or a protocol to turn to when virus attacks, denial-of-service, hardware failure, sabotage, or acts of nature affect your business. It has been estimated that three-fourths of today's successful system hacks are perpetrated not via network security flaws, but by entering directly through the "front door" - exploiting vulnerabilities in customer-facing Web applications. By taking advantage of the public access to a company through port 80 and 443 and using it to subvert your applications, hackers can gain easy access into your company's sensitive backend data. Firewalls and intrusion detection systems (IDS) will not stop such attacks because hackers using the Web application layer are not seen as intruders.