

# VAQ

Read more articles from the VAQ –  
Value Added Quarterly Business Journal.



## Defending your site

IT security expert says firewalls do not offer complete protection against hackers over the Internet.

**Richard Reiner,**  
Chief Technology  
Officer, and  
**Karen McNeil,**  
Senior Project  
Manager,  
Assurent  
Software, Inc.

**N**ow that your company has established an online presence, the question is: How safe are your applications? That's a question Dr. Richard Reiner wishes more CEOs would consider. Reiner, Chief Technology Officer, Assurent Software Inc., is an internationally recognized authority on information security, application security and privacy. According to Reiner, the diversity of today's Internet-facing applications — including retail banking sites, reservations systems, personalized customer portals, remote access tools, and even marketing web sites — has made the problem of defending business systems against hackers more challenging.

"As the focus has shifted from mainframe to web-based applications, information security risks have intensified," Reiner explains. "Over the past three to four years, hackers have moved away from attacking operating systems, which tend to be well-defended by firewalls, and now strike through the points of entry created by business applications that are accessible over the Internet."

When hackers focus on application level attacks, they do more damage and strike deeper into the core operations of an enterprise. As Internet applications have become progressively more important to businesses, they have correspondingly been integrated with enterprise systems. A customer transaction that is executed via a web-based interface may in turn cascade transactions and data changes throughout the company's information database.

Ensuring that your company's Internet applications have been designed with inherent security features is critical, Reiner asserts, but there are limitations on what can be done to enhance application security at the development stage.

"The current approach to application security is based on building controls into individual applications using source-code level features. Unfortunately, vulnerabilities in the code often survive undetected. The testing process is onerous, expensive and there aren't enough developers who have sufficient training to adequately address security challenges."

While security products have been developed that attempt to recognize existing or "known" application-level attack signatures, hackers often craft specific attacks that would not be recognized by any generic attack signature.

"The Open Web Application Security Project has recorded 135 different ways that Web-based applications can be attacked," Reiner comments. "Often, an attack will not even be noticed until business information is missed, or turns up in the wrong hands."

Reiner adds that too many businesses are operating under a false sense of security when it comes to Internet applications.



# Defending your site

“There is a common fallacy among many business people that installing a firewall will protect against unauthorized use or misuse of Internet applications, when in fact a firewall is really only the first line of defense for the network,” he says. “For more complete protection, you need to consider a two-tiered defense system that includes firewalls as well as positive protection for enterprise applications.”

## ‘Positive’ new technology enhances application security

Just like firewall technology that acts as a front line of protection for networks, new software has been developed to protect applications. One means of protection is ‘positive’ security.

Rather than attempting to recognize every possible attack, positive security is a method of characterizing the acceptable interactions between a user and an application. Any type of access deviating from the model of acceptable use or actions that do not conform to the defined parameters will be recognized as an attack and blocked.

## Risk assessment underlies technology investment

Not surprisingly, Canada’s financial institutions are proactive when it comes to defending their networks and their applications. In fact, online security information and development innovations are shared on a regular basis between IT professionals at all the major banks. This cooperation helps improve the security of the Canadian banking system overall and helps combat fraud.

**Glenn Blair**, Scotiabank’s AGM, Technical Security Services, Information Security and Control, comments:

“We’re at the leading edge when it comes to incorporating new security technologies. Given Scotiabank’s focus on Internet-based cash management solutions, we take our responsibility very seriously – using a cost-effective combination of proactive and detective controls. Our goal from both a development and security perspective is to meet or exceed the business requirements without adding undue risk to the bank.”

Dr. Reiner believes that all companies need to assess the degree of risk to their business in order to determine whether or not to invest in additional application security.

The question of how best to protect the enterprise information system usually boils down to how much of an investment a company needs to make.

“Financial losses such as your annual loss expectancy may be easier to calculate,” says Dr. Reiner. “It’s harder to measure damage to a company’s reputation or cost of failing to protect private information, however, these are the factors that should inform your decisions.”



44 King Street West  
Toronto, Ontario M5H 1H1  
e-mail: [businessproducts@scotiabank.com](mailto:businessproducts@scotiabank.com)  
[www.scotiabank.com/vaq](http://www.scotiabank.com/vaq)