



## Securing the supply chain

### Scott Gardner

#### IT Focus

Snuggling up to your supply chain partners has often led to sweaty palms and awkward mornings after, but IT security experts say that hooking up online raises a whole new set of concerns.

Although security specialists sometimes sound uncomfortably like the little boy who cried "Wolf!," in a recent survey of 2,800 Canadian business IT users, one in five reported that their organization had experienced a serious external systems security breach in the last year. Despite this, the study's author, Dr. Peter Carr of Alberta's Athabasca University, also found that most of these same organizations were still planning to increase their technology spending in the coming year.

"There is almost a double problem here in the sense that there is optimism and desire to progress with technology, and for it to become a bigger part of what organizations do, but at the same time that is being threatened quite substantially by the issues around security," said Carr, who is also acting director of Athabasca's Centre for Innovative Management.

"The essence of online collaborative tools is that they link organizations together, but to do that there needs to be openness to the Internet that is potentially going to make organizations more vulnerable to security breaches," Carr said.

"Initially the Web was just being used for publishing static data — 'Here's some information about my company and here's the 1-800 number and e-mail address.' But once you say, 'If I get all my business partners on here I can do my orders online and take a whole step out of the process,' you have to ask yourself if the extra business you are going to get will make up for the increased risk," said Doug MacPherson, a Toronto-based security specialist with IBM Canada's Tivoli division.

MacPherson said that companies should look at their business requirements and those of their partners and try to determine what is the right kind of data to share without giving away the keys to the castle.

#### Keeping the keys to the castle

In the past most supply chain processes were done manually, with someone picking up the telephone or filling out and faxing a form, so a properly secured electronic supply chain is inherently better protected than any manual system, said George Gilka, product marketing manager with the Ottawa-based security and encryption firm Kyberpass Corp. However, he said, since an unauthorized order for 10 million widgets could actually bankrupt some players in the chain, any system has to be built and operated very carefully.

"It depends on your industry, but [supply chain security] primarily boils down to two things, authentication — making sure that the person viewing data or placing an order really is who they say they are — and encrypting the information being sent between the players," Gilka said.

A compelling reason for caution when sharing proprietary information over the Internet is the ever-present, and surprisingly common, possibility of corporate espionage, said Stuart Pothan, Mississauga, Ont.-based manufacturing industry director for Oracle Canada.

"The old way of doing things was having ERP systems within the four walls of your company. Now these information systems stretch out beyond the four walls to customers, suppliers and all your trading partners so you are now sharing more information with more people. The speed of collaboration can be a wonderful advantage, but if you are trying to buy the right product from your supplier, and you need to show design information, obviously that information needs to be secure," Pothan said.

"For example in the automotive sector there are a number of new technologies that are being introduced into cars like global positioning systems and the like. As a supplier of that GPS you don't want to divulge that information over the Internet to organizations in the chain that might also be your competitors."

#### Protecting your information

This is why Gilka recommends the use of the relatively low cost and increasingly user-friendly digital encryption and authentication technologies that are out there.

"In the communication channel where partners are providing details for orders and data like that, these tools can beyond any reasonable doubt confirm the identity of the people doing the transaction. Furthermore, security in the form of (leading Internet protocol) SSL can encrypt the pipe between a browser-based front end and the server receiving the order," he said.

Gilka cited the pharmaceutical industry as a sector that relies on a heavily secured supply chain for their ERP processes. Although he was uncomfortable giving specific details, Gilka knew of at least a few cases where drug companies had landed in very hot water when

sensitive data such as clinical trial results and confidential medical records leaked out to the public Internet. He also said that the pharmaceuticals employ heavy digital security as part of the race to patent new products.

"The reason is that the patent office in the U.S. will not accept an online submission unless it's digitally signed. And from an ROI point of view a pharmaceutical can save money in the vicinity of several hundred thousand dollars per day if they expedite a patent application [electronically], and these are typically tied to some sort of online ERP process," Gilka said.

Oracle's Pothan said that the safest supply chain software should have security built into each level, from the database, to the development tools, to the application level and the end user. He also suggested that buyers try to find built-in digital certificates and data encryption, as well as secure messaging systems.

#### Securing the joins

"Where there really is an opportunity for information to get out of an ERP system, or an Oracle eBusiness Suite is while transmitting messages to a PeopleSoft system or an SAP system. That is, one risk to integrating best of breed applications is that the places where your supply chain, financial or plant maintenance applications join are risky areas — that's the point at which information can get out," Pothan said.

Of course, agreed all the experts, if the links between your internal systems keep you up at night, the links between corporate partners can be the stuff of nightmares.

"If you are one of a group of companies participating in online transactions you want to make sure that you are not exposing your own information because of a lack of proper security implementation by someone else. Security is only as good as the weakest link, and if the weakest link is clearly weak then the whole chain goes to pot," said Kyberpass's Gilka.

"You have to do your due diligence if you want to be a participant in an online supply chain — a company would be crazy not to require proof of security, mutual authentication and database security from its partners," he added.

At a basic level, Pothan said that managers and executives must remember that supply chain technology isn't a magic cure for the same old concerns that have always emerged when companies decide to open up their processes to each other.

"In the old system — without technology — when you would buy something from a supplier, the supplier would come to your office and they would share information with you. In a nickel and dime way you could easily have taken that information and shared it with another supplier, so the risk was definitely present. Business ethics — or the lack of them — are still there, the only thing that changes