

## E-Commerce Sentries

# 'White Hat Hackers' Walk the 'Firewalls'

BY MATTHEW DRISKILL

In the virtual world of Internet commerce, trying to keep things secret is time consuming, cash consuming and fraught with peril as developers spend sleepless nights worrying that some teenage hacker, fueled by gallons of Jolt Cola and tacos, is slipping into their intricately constructed website and wreaking havoc.

Banks, e-tailers, online traders, and anyone else performing commerce on the Internet share these concerns and all are doing something about it, although the specifics of what they're doing vary widely. For some e-commerce purveyors, it's a matter of simply keeping your database separate from your online presence. For others, it involves using closed proprietary systems and for others it means using double or triple firewalls.

For all of them however, disclosing their security features is not something they do lightly, if at all, and most of them described the concept as akin to that of the Secret Service disclosing their protection plans for the US president.

What we were able to glean is described below where we give a brief look at what some e-commerce professionals in Hong Kong are doing to ensure security on their sites.

### Online Labs

US-based Online Labs is a firm in the forefront of fighting cyber-crime and the president, Eric Laykin, was recently in the SAR to promote the company's suite of products and services. Online Labs was founded in 1987 and originally specialized in information systems for the legal and professional service communities.

"As e-commerce increased and as Internet users began divulging personal information on the web, Online Labs launched its Security Division," Laykin says. "We focused on security, corporate vulnerability studies, online investigations and systems analysis."

In early 1998, the company also instituted its "FREAKS" division, or Fast Response Electronic Action Knowledge Squad. FREAKS is a team of "stealth" members that resides both

locally and in geographically diverse locations and works to deter Internet-related crime.

"We take a custom approach to the problems being encountered by companies, but we're also working with clients to prevent problems rather than just react to problems," Laykin says. "The way we go about it is we've developed these small teams that will go out to the companies and address these issues. It might be stock fraud where people are putting out false rumors on message boards or a celebrity is being discredited or internal theft of company secrets.

"We try to look for methods that clients can employ to prevent problems."

One of the big revenue generators for the company is litigation support, wherein the company can go in as a forensic firm of sorts and retrieve data thought to be erased. As everyone 'techie' knows, the information is never totally erased and recovering the data from a hard drive to support a company's lawsuit is big business these days.

"Frequently clients don't even know how to organize that data," Laykin adds, "and we prepare that information for litigation support. It takes a huge amount of time and manpower for these kinds of investigations."

In Hong Kong, Online Labs is trying to establish itself as a component of a company's corporate security and Laykin says he's working with about six companies now, although he won't disclose their names. The company also works with such well known investigative firms as Kroll-O'Gara and Burns Security (formerly Borg-Warner). After Asia, the firm plans to work in Europe, although it has no presence there now.

One of the more interesting aspects of Laykin's work is his company's use of so-called "white hat hackers," whom Laykin calls a "valuable commodity."

"You have to spend considerable time on these relationships. Yes, we do hire them and they are and we consider them a valuable



**Eric Laykin, top;  
Charles O'Flaherty,  
above; Fred Litwin,  
left.**

commodity because we don't necessarily look at hackers as a four-letter

word. There are ethical hackers who are interested in the technology and who want to push the limits of the technology and not for bad reasons. So far we've found some terrific talent in that area. We of course do very thorough background checks, but we're happy with the ones we've used."

With the proliferation of online stock trading in the US, stock fraud is probably the growth area in Online Labs' business, says Laykin. Employing the old adage proffered by circus great PT Barnum that "there's a sucker born every minute," Laykin says people relying on message boards for stock information are naive and should be more discriminating about the provenance of their stock information.

"There's a lot more stock fraud today. We've had multiple cases of fraud and attempted price manipulation where people post false rumors on message boards and then short the stock when the price falls. We had a rather large case recently where false rumors were floated that a large manufacturing concern had accounting irregularities that were not true."

### AsiaAlliance

At about a month old, AsiaAlliance is perhaps the newest of the websites to set up business in Hong Kong, although in a sense it's not truly an e-commerce site. The company, founded by American banker Charlie O'Flaherty, uses the web as a tool to connect Internet start-ups with potential inves-

tors around the world.

The young firm, housed in a small office suite in Hong Kong's International Finance Centre, offers Asian-based start-ups a "package deal" via the Web that enables the firms to streamline their ramping up process and matches them with investors looking to get in on the Internet boom in Asia.

"We provide pre-screened business plans from these start-ups to investors and we use the Web to screen those start-ups. If they (the start-ups) pass the first level of screening, then we meet them face-to-face. They have to go through a much more detailed second level of questions as well, one that usually takes anywhere from six to seven hours," says O'Flaherty. "This second stage is really a way to start screening their business plan. The first level has about 140 questions while the second one is much more detailed." The benefit, he adds, is that investors see proposals in the same format instead of a hodgepodge collection of various formats, fonts and languages. This makes it easier on the investor and allows them to make much quicker decisions on potentially funding a deal.

Once a start-up has passed muster and O'Flaherty decides to work with them, then AsiaAlliance starts to bring in investors.

"If we decide to work with them that's when we bring the investors in and then we send them off on their own and they negotiate their own deal."

AsiaAlliance makes its money by charging the start-ups a five percent fee of any capital raised and five percent in equity as well. If the amount raised is above US\$2.5 million, then the deal is "negotiable."

In addition to getting access to funding potential, the start-ups can also avail themselves of other services offered by AsiaAlliance. These include such things as business plan writing assistance, public relations plans, web subhosting assistance, office space, strategic planning and legal assistance. The fees for these items are charged on a consulting basis.

"We think it ends up being a pretty good package," O'Flaherty says. "They can pick the investors and the investors are happy because they don't have 10,000 people calling them and they get to see companies that are pre-screened."

Having all of this information — start-up business plans, company financial information,

names and other information on investors — would certainly be valuable to those prying hacker eyes. So what does AsiaAlliance do to prevent unauthorized access? Surprisingly some very simple things that so far have worked for the company because its site is not designed for money to change hands.

"We don't go for eyeballs on our website so we're really not trying to drive people to it. We don't want the general public on our site because it's not designed that way. We want qualified investors and companies or people with ideas who want to qualify for funding," says O'Flaherty.

The company uses the standard security measures such as Secure Socket Layer and also has double and triple firewall protection.

"It's dangerous to talk about security, but no money changes hands on our site. The ideas though, are worth money. There's a lot of private data that is worth a lot and the investors don't want to be contacted by unsolicited calls. Also, the start-ups don't want their ideas stolen, so what we do is separate our website from our database.

"Right now it's good security, but in two months we'll probably have to upgrade to whatever the latest is that comes out." Another item the company keeps confidential is the actual second stage of questions wherein the applying start-up company fills in significant details about their business plans. Just knowing what kinds of questions are being asked could tip off the competition.

## **Intel**

Singapore-based Fred Litwin, a marketing manager for Intel, says his well-known company is working on hardware solutions to security problems.

"The way people do security, they typically look at firewalls for people coming in from outside the company. People don't usually talk about security inside the company. What we're doing at Intel is launching silicon (chips) so you can encrypt data on the corporate LAN. We have adaptors for servers and clients and hardware as well. We can put the LAN connection right on the motherboard."

Intel's other moves include the recent purchase of US-based Shiva, a networking company, whose products allow users to dial in from a remote location over the public Internet, but instead of actually having your

*Continued on page 8*

*'White Hat Hackers' Walk the 'Firewalls'.*

*Continued from page 6*

data travel on the open road of the Internet, Shiva's products "allow you to set up a tunnel through which your data travels," Litwin says. "Instead of trying to make a long distance call, you dial in a local number to access the network and then set up this closed environment where your data is more secure."

Intel's Litwin says the company is also rolling out new products for Internet Service Providers around the region, to allow them to set up secure virtual private networks for customers who want the convenience of the Internet without the security holes that seem to crop up on a daily basis.

"This is clearly a big channel for us," Litwin adds, "as we can bundle these items into a package that ISPs can sell to their own customers."

### **Computer and Technology Holdings Ltd**

A company that is in the forefront of Internet security is Hong Kong-based Computer and Technology Holdings Ltd, which has the distinction of being named recently as an

Enterprise Security Solution Provider by US-based Internet Security Systems Inc (ISS). C&T, founded in 1991 and with offices around China, delivers security assessment services, intrusion detection, and adaptive security management solutions, according to David Ho, the company's assistant marketing manager.

"We have a long-standing track record in providing innovative systems integration projects with a specific emphasis on the electronic business framework, Internet security, document management and network infrastructure," adds C&T Chairman C S Ng.

ISS's Asia region president, Jo Hong Lin, says "network risk management has never been more vital in today's world of global connectivity and these intrusion systems are a vital component, especially for e-business."

"What we do mainly is use ISS's tools to service the clients," adds David Ho. "The basic component of course is the firewall that resides on the company's server. We build in a system that contains a database of hacking tools that our computers can use to detect suspicious packets of data and then block those packets that contain suspicious hacking signatures."

C&T mainly focuses on large enterprise applications and started to focus on security three years ago.

"Working with ISS gives us access to their security applications and to their teams of experts who work to daily update the system with the newest tools and solutions. Basically, we can go in with a notebook computer, get on the network and scan it and then report back to the company on what we find and propose solutions."

Ho is reluctant to disclose his company's main customers because the companies don't want to disclose to the outside world what tools they're using to foil the hackers.

The use of ethical hackers is another area that C&T is starting to use, but Ho says Hong Kong really doesn't possess a large enough pool of talented, ethical hackers to employ, leading C&T to search Australia and the US for partnerships.

"There's a good opportunity in terms of the security market, but ethical hacking is not an easy thing. The hackers may be good, and their tools may be there, but there aren't enough right now to make a go of it," says Ho.