

21st-Century Engineer

Forget about the information superhighway. Instead, picture the Internet as a global railroad

by Sharon Shinn

photos by Robert Houser

Stratten Sclavos is constructing the equivalent of the modern-day railroad. He's laying down virtual tracks through Internet territory as he considers how to carry global commerce through the rest of the 21st century. Maybe even beyond. Sclavos thinks in terms of centuries and lasting legacies.

The chairman and CEO of VeriSign Inc. runs a business not easily defined. The Mountain View, California, company offers "digital trust services"—security and authentication services for online buying and communication, as well as telecom services and domain name services. Recent acquisitions of Signio, which handles payments for online merchants, and Network Solutions, which assigns and tracks Web addresses, have made VeriSign a one-stop supplier of all Internet-based needs for corporations interested in online commerce.

That's all according to plan. Sclavos has said he wants VeriSign to be the Internet's first utility—a pervasive, essential, invisible part of the infrastructure that enables business to get done. He's focused on making Internet transactions as secure and trouble-free as possible, and he's constantly looking toward the future to help him determine what his choices should be now. Even in a field as volatile as technology, such focus has made Sclavos a recognized leader: He received the 2001 Morgan Stanley Leadership Award for Global Commerce and has been named to the *Forbes* list of Top 50 CEOs.

Yet his definition of leadership is one that even an undergraduate business student can understand. "In many ways, it comes down to charting a course—having the ability to articulate for your employees where you're headed and how you're going to get there," he says. "Even more important is choosing people to work with who have that same level of passion, commitment, fear, and competitiveness to drive toward those same goals. A lot of people talk about visionary leaders. I believe that you have to do the heavy lifting every day, make sure you have your best people on your biggest opportunities, and make sure you don't get complacent about where you are at any given point in time."

Sclavos knows where he is right now. Where he takes VeriSign in the coming decades may shape the way the whole world interacts with the Internet.





covered with fast-moving trains. The man in the lead locomotive is VeriSign's **Stratton Slavos**.

I've been trying unsuccessfully to coin a simple explanation of VeriSign. Do you have your own shorthand description of the company's services?

We've been trying to come up with one for nine years! The simplest way to describe us is that we provide intelligent infrastructure services for the Internet and the telecom networks. In essence, we sit above the pipes of the Internet and the traditional voice networks, and we provide services that make those networks more reliable, more secure, and more scalable.

On the Internet side, our domain name services help people find Web sites as well as send e-mail. We handle about 14 billion interactions a day. On the telecom side, we help mobile professionals roam on cellular networks. We handle about 50 percent of all the roaming traffic in North America.

Our services are designed to help people in business find each other, connect, securely communicate, and transact. We think those four things—find, connect, secure, transact—are the equivalent of the dial tone in the phone networks. This will be the infrastructure that services ride on for the digital wave.

Exactly what do you mean when you call VeriSign part of the Internet infrastructure?

Look at the railroads of the mid-1800s. Look at electric power grids and air transportation industries of the 1900s. Today, look at telecom and the Internet. Each time a major economic shift happens, a new intelligent infrastructure has to be put in place. We believe VeriSign is the company to build that intelligent infrastructure for this generation's economic shift.

The wonderful thing about infrastructure businesses is that, once you build them, you really are enabling hundreds or thousands of opportunities to succeed. It may be Internet commerce or it may be Internet telephony, but it's all riding on the same infrastructure, so our investments can be leveraged across them. We don't have to make a live-or-die bet. We sleep better at night knowing that infrastructure is adaptable to many other opportunities.

At the same time, we have to have some courage, because the infrastructure has to be built before the market exists. It really is a "build it and see if they come" phenomenon. The market can't get started until the infrastructure is there, but once it does get started, then the infrastructure better be very scalable and very reliable.

You started at VeriSign in 1995 as one of its first employees. What drew you to the company?

I have an engineering degree, so I'd always been focused on technology; but I really felt that VeriSign would give me a chance to hand-pick a team and build a company that would leave a legacy. Whether that legacy was going to be security or some other version of technology was not as important to me as getting an opportunity to build something from scratch and surround myself with people who had those same goals.

Our first business model, which was written before I got here, was to sell security services to Apple/Mac users and to Lotus Notes users. The Internet came along just about the same time I did, and we had an opportunity to provide services for Netscape's original products and, three months later, for Microsoft.

Over the last nine years, we have learned a lot about how to build an organization. You must understand your core competencies, but you also must adapt to what your customers are telling you are the real opportunities to pursue. Had we chosen the Apple/Mac and Lotus Notes market, we would not have survived as a company.

You reached the CEO's office without having a degree from business school. What do you think you learned on the job that you never could have learned in school?

I think there are two sides to that coin. I had taken my GMAT and intended to go to business school after working for a few years. But I was in Silicon Valley at a time when the best education I could get about high-growth businesses was occurring right in front of me. In that particular era, I would say I probably was better served not going to business school and just living in what was an incredibly dynamic environment. This was a time when the first microprocessors and the first operating systems for Microsoft and Apple came onto the market. It was the most fascinating time in technology to live through.

On the other hand, when I watch business school graduates who work for us, I see that they have a set of skills that I wish I *had* learned earlier. They understand modeling and financial and strategic analysis. Would those tools have helped me in the early years of Silicon Valley? Absolutely. One thing you don't learn in a hypergrowth mode is disciplined thought and analysis.

I think you need a blend of both kinds of learning—the discipline you can get from a business school curriculum as well as on-the-job training that teaches you that business needs to be adaptive every day.

At a time when a lot of other Internet companies were failing so spectacularly, VeriSign was thriving. If students were looking at VeriSign as part of a case study

about successful Internet companies from the 1990s, what would they discover?

We were the last of the old-world venture funding companies instead of the first of the new Internet companies. For us it was about building a company in a bootstrap way—spending as a byproduct of growth, not in anticipation of it, and laying a solid foundation for the company no matter what the markets brought in terms of opportunity and change. I think this notion of building something that will leave a legacy, and doing it in a methodical way, gives a company a strong foundation from day one.

The other thing was that we were willing to adapt our model based on what our customers told us. One of the sayings I'm fond of is, "Our vision is good but our hearing is better." So, very early on, we listened to what Netscape and Microsoft were telling us about the Internet. We listened to what the government and large corporations were telling us about their security needs. Relatively early on, we understood that running intelligent infrastructures would enable electronic commerce and communication; and if we did it right, we'd be a beneficiary. Listening to customers and following the winds of the market gave us a strong ability to adapt quickly to what we saw.

So many technology company founders and business school graduates are taught that they must stick to the strategy and stay focused. That's a very, very important lesson. The corollary is, you've got to listen to your customers if your strategy is wrong. I think you need to keep your options open in terms of business direction and strategy, but you shouldn't stray from your core competencies.

What should business students learn about the reasons technology companies failed during the Internet bubble—and the reasons some of them are so successful now?

I think that the key lesson is that you need to be No. 1 in your market. During the bubble, there was the notion that a rising tide raises all boats. We could have a thousand online booksellers, and they would all thrive. In reality, the No. 1 guy makes at least half the profits of the whole industry. No. 2 may make another 20 to 30 percent, and everybody else fights for the scraps. So the notion of being a me-too player, or that being No. 2 or No. 3 is OK, is really a fallacy. And I think that is just as true in the online world as it was in the offline world.

All the things we used to hear about—the new business models and disruption of the online economy and disintermediation, blah, blah, blah—I don't think that all proved out. I think the reality is, those who got there first with the best

One of the sayings I'm fond of is, "Our vision is good but our hearing is better."



value proposition and proved they could scale are now in a position to drive a disproportionate share of returns to their shareholders and their customers.

VeriSign is successful on a number of fronts, but some of your primary offerings are secure payment options that allow people to buy safely over the Internet. Until such options existed, people were reluctant to make purchases online. What had to happen technologically and psychologically to enable Internet commerce?

Two things had to happen. First, the experience of buying something over the Internet had to be better than the corresponding experience in the physical world. Whether they were on Amazon.com or eBay, customers had to feel like it was a better use of their time and money to buy there. Online buying could only succeed if people could be convinced that the risk was worth the reward. The risk of doing business online with an entity they could not see had to be outweighed by the reward of those benefits.

In the early days, our security technology created an umbrella under which many businesses could promise customers that online buying was not only a better service, but it was as safe as the physical world. If you do a survey of people who still don't buy online, the majority of them will tell you it's because they're afraid of putting in their credit card number. That being said, online commerce through our payment gateway reached \$10 billion for the first time last year.

Another crucial component of your business is providing online security. What sorts of threats do you see to the digital and telecommunications infrastructure, and how can people protect against these threats?

Let me start small and go big. VeriSign networks and data centers probably get attacked more than 500 times a day. Part of that is because of who we are, and part of that is because everything we do is Internet-based. We're just very available for those types of threats. We also manage and monitor the net-

work perimeters for companies like Merrill Lynch and U.S. Bank. On their networks, we are now seeing twice the number of security events on a monthly basis as we did a year ago.

What's really happening? First of all, more and more of every business's assets are being exposed to the network every day. The more we move to a digital infrastructure, the more companies are going to have to open up their corporate assets. So there are richer and bigger targets.

Second, we've moved on from the early stage of security threats that were really acts of mischief perpetrated by unorganized, disassociated groups of teenagers. Now, we're seeing much more organized forms of attack, like phishing and identity theft. With phishing, we have very sophisticated and clever people targeting the e-mail addresses of customers of the largest banks in the world and trying to fool them into giving social security numbers and credit card numbers on Web sites that you and I couldn't tell weren't authentic. The sophistication of the attackers has grown dramatically in the last few years, commensurate with the amount of money that's now being transacted in the online world.

I think we have to step back and say, "Well, isn't it natural that as the economy moves to a digital infrastructure, so do the criminals?" They're always going to be chasing the money. The economy is moving, and so are the threats.

For about three years, you've been a member of the White House National Security Telecommunications Advisory Committee—NSTAC—which deals with national security and emergency preparedness. How has your job there changed recently?

It's really only been in the last 12 to 18 months that we've turned the discussion from copper cables over bridges and under tunnels to network attacks and the potential for serious disruption of our financial, power, and utility systems. While the physical security protections were the most important things to focus on after 9/11, we are now moving into a world where we have to pay equal if not more attention to

I think, as security technology providers, we can create great products and services

the digital threat. What's likely to emerge are blended attacks that will have physical and digital implications.

The real goal of NSTAC is to make sure that the private-sector companies that operate much of the critical infrastructure are both prepared for national security events *and* capable of supporting the first-response initiatives for federal, state, and local governments. We have to make sure we're as resilient against attack as we can be by sharing information—and then, when there is an attack, make sure we can provide a reliable backbone for communications so that emergency responders can do their work.

Extending the issue of security to the university campus, you might know that many business schools now require laptops and offer wireless connectivity. What would be the likeliest threats to such large, multiuser educational wireless networks, and how can schools protect their students and themselves?

I think that in general we are a society, particularly in the U.S., that will always choose ease of use and convenience over better security. That's true in what we do in an airport—it's true when we give our credit card to a waiter—and it's true when we take our laptops and hook up to wireless networks. There's an obligation in the security industry not to force end users to choose security over convenience. That said, we have to begin building services and technologies that are as easy to use or as invisible to the user as they can be. We need to have ubiquitous wireless networks *with* good security.

So what could happen on a campus? The same thing that happens at an enterprise. A user goes home, hooks up to his broadband supplier, is Web surfing on personal time, and unknowingly gets a virus or a worm downloaded onto his computer. He comes back in tomorrow and plugs into the corporate or campus network, then all of a sudden that virus is everywhere. In the new genre of security threats, much of what we're seeing is that the penetration occurs from a friendly device that comes back into the network to contaminate it. That's very different from two or three years ago, when all the threats were coming in the front door.

The new state-of-the-art in security is what's called "vulnerability assessment in management." The idea is, instead of waiting for an attack, why don't we proactively look at all the machines in our network, highlight what the vulnerabilities *could* be, and then begin isolating or patching them? It's somewhat like inoculation against some disease. Vulnerability management offers early warning systems, as opposed to threat detection and response.

I do think there is a longer term issue and opportunity

here. My generation didn't grow up with the Internet. We kind of had it thrust upon us midway through our maturation. My children are growing up with both wireless services and the Internet as a part of life, and they're not as sensitive about security on these networks as they need to be. The next generation is the one that I hope will grow up with an education system that tries to establish a culture of security. Their attitude will be, "It's good to get on the network. It's better to get on the network safely."

I think, as security technology providers, we can create great products and services that will make people secure, but they only work if people use them. The next generation has to grow up using them and taking them for granted.

I want to turn the conversation toward the future. You have a 100-year vision for VeriSign. Can you describe it?

We don't call it the VeriSign Vision. We call it the VeriSign Journey. A hundred years from now, how would we want the history books to describe what we contributed to technology and society in general? We want to build the infrastructures that accelerate the next wave of economic activity—the way the railroads did, the way the electric power company and the air transportation industry did. And that's a lofty goal that our employee base has rallied around.

Backing it up from that hundred-year-out journey, we ask, "What does that mean we have to be 25 years from now? Five years from now? *And* how do we stay on course by achieving certain milestones this year?" If we want to leave a legacy, then we want to be the most influential company of this century—the way that GE or IBM or Microsoft were last century.

We've already got e-mail, e-banking, e-commerce, and wireless data access, and we're heading toward smart appliances. What else is coming?

I have a slide in one of my presentations that shows the proverbial hype curve. It says when a technology is first announced or introduced, the hype is like a rocket ship. But adoption rates are slower than anticipated, so we go into the trough of disillusionment. That lasts for some period of time. And then very quietly, without a lot of fanfare, adoption kicks in.

Much of what you're going to see in the next five to ten years is the adoption of the technology and the infrastructures that were overhyped during the Internet bubble and given up for dead two years ago. Those include using voice-over IP, taking telephony from the traditional networks into IP-backed phones, reducing the costs of technology, and increasing the types of services you can get. Those might be wireless

that will make people secure, but they only work if people use them.



data, games, videos, broadcast TV, ring tones, ringbacks—you name it—five years after they were first touted, these are really starting to take off. Outside of that, we think the notions of RFID tags and electronic product codes really do have the ability to transform the supply chains of the world.

You're talking about radio frequency ID tags, which store information on microchips that can be used to identify both people and products. How do you expect these to radically change commerce?

With RFID, products can be tagged as they pass through the supply chain, out of the manufacturing plant, through the warehouse, to the truck, and eventually onto the shelf. We know where they are. We know whether that product is real or counterfeit. If that product is a pharmaceutical, we know whether it has expired or been recalled. We know if it's been stolen.

When you look at all the inventory that sits in distribution, all of the out-of-stock situations when customers can't find a product on the shelves, all of the theft in the distribution channel and at the point of sale, and add that up for all manufacturers for all industries across all retail distribution centers, you're talking about between \$600 billion to a trillion dollars per year of economic loss. If we can shut down a lot of that leakage, there will be dramatic economic benefits to bread-and-butter industries. That will get translated into lower prices for consumers, better earnings for retailers and packaged good companies, and a reinvestment of some of those savings into new products.

Trust me, RFID will go through its hype curve. Wal-Mart has told its 100 top suppliers they better be on board by January 2005. Everybody's going to be late. In the early years, benefits won't be seen all the way out to the shelf, just in case-and-pallet at the warehouse. So there's going to be some disillusionment in the early days. But I believe this development will be one of the most significant changes our economy will see for several decades.

As for your own future, what would you like to accomplish over the rest of your career, with VeriSign or elsewhere?

I'm absolutely confident this will be the last job I have. I love what we're doing. I think the things we're working on will have an incredible impact on the world over the next five to ten to 20 years. The people we've surrounded ourselves with all have that same kind of energy and passion and commitment to do great things. So I can't think of a place I'd rather be, nor can I think of anybody I'd trade places with in the technology industry.

You know, CEOs often will say that going from zero to \$100 million is the hardest thing. A few years later, if they're still in play, they'll say that going from \$100 million to a billion is the hardest thing. I actually think each new step demands a new level of discipline, a new level of commitment, and a new level of strategic thinking. So as we take VeriSign from \$1 billion to \$2 billion, as we take it from \$2 billion to \$5 billion, I'm excited about the fact that I don't know how to do that job yet. And I'm very confident that I'll learn along the way. I'll take a few missteps here and there, but I'll be able to continue driving forward on this journey.

What advice would you give to today's business school graduates?

I think it is a really interesting time for them. What are the opportunities? Many of them used to go into investment banking and management consulting. My personal opinion is that that's more like being a spectator at the Olympics. All these incredible changes are coming, many of them driven by technology and by telecommunications. They need to get on the field. I'm hopeful that the next generation of business school graduates is really focused on getting into the workforce and helping build something great that leaves a legacy, rather than watching from the sidelines. 