



## Information Security: Beyond Firewalls

An interview with consultant and author Thomas Parenty



by Thomas Parenty  
December 2003, Issue 22

Protecting your enterprise's information against hackers, viruses, worms, and other Internet nasties is well and good, but you could be using information security to actually improve your company's business. So says Thomas Parenty, president of Parenty Consulting, a firm that helps clients improve their information security and privacy, and a former employee of the National Security Agency. He's also the author of a new book, [Digital Defense: What You Should Know About Protecting Your Company's Assets](#) (Harvard Business School Press, 2003). Parenty recently moved both himself and his practice to Hong Kong, but the day before he left, contributing editor Peter Krass spoke with him from his office in San Francisco.

**Q:** *How does your book differ from others that have been written about information security?*

**A:** My perspective on enterprise security. I've noticed that many IT departments—and this is a reflection of corporations on a whole—tend to focus on protecting computers as opposed to information. They focus on security technology such as anti-virus protection and firewalls that protect enterprise computer systems. But they don't focus on any of the information that's being used to run the business.

Of course, a company should certainly pay attention to the firewall, etc. But even if you do all of that perfectly, and even if you do the Herculean task of installing security patches in a timely manner, you're still not able to answer questions relating to the business operation—for example, "Is my client's financial information, such as credit cards and account numbers, safe from fraud?" or "Are my new product plans protected from being looked at by competitors?" or "Are all those checks that come out of accounts payable really for goods and services that we received at the price negotiated?"

You need to focus on the information that's actually running your business: How does your business operate? What information is necessary for your business and for employees to do what they need to do?

**Q:** *You write about the need for a "trust framework." What is that, and why is it important?*

**A:** One of my main premises is that protecting a company's information, and the thought process that goes into doing that, is fundamentally the same as protecting more tangible assets, which is a task that businesses have had to handle since the beginning of time. It's just requires a small translation process.

The way the trust framework works is that in any business relationship or activity, whether cyber or manual, there are certain protections or security properties that need to hold true in order for a company to feel confident going forward. In the pre-computer world, the initial trust objectives were things like, "If I'm going to have a business relationship with another company, I need to know who that company is; I need to know their background in terms of their ability to pay bills, etc." For example, if I have a bunch of furniture in a storage area, I need to make sure that the physical protection of the furniture is adequate, that it doesn't get stolen.

**Q:** *How does this play out in the computer age?*

**A:** Let's look at banking. In the pre-computer age, if you were going to conduct transactions with a bank, there were certain physical, cultural, and social factors you could use to establish trust. These included personally knowing the banker, physically going into the bank building, seeing signage that gave you confidence. Now, as businesses move into an increasingly automated and computerized business environment, a lot of the physical evidence of a trustworthy relationship disappears. If you're doing electronic banking, you no longer have the banker, the building, and all that other stuff. As a result, the bank should look at computer-security technology from the perspective of how it replaces the kind of physical evidence that businesses have been relying on forever. So instead of merely reacting to, say, a security attack on the network, we should look at information security's role in providing the necessary assurance of the safe and proper operation of a business in the digital world.

**Q:** *You write that implementing trust technology would not only protect the security of the enterprise, but also enhance business. How does that work?*

**A:** Clearly, folks first need to get their house in order. But you can then go a step further in your thinking by asking: How can the operation of my business actually be improved in terms of lowered cost, higher income, better customer or partner satisfaction, or any number of quantifiable metrics?

In much of the marketing literature for various security products, there's a sheet that says you can enhance your business or find new growth opportunities through the security aspects of the product, but it's never clear how you'd do that. So I came up with a way to look at how the proper application of information-security technology can actually enhance business opportunities. Basically, you need to look at how the current deployment of security technology—both manual and computerized—limits the ways your business can operate. Then apply this new perspective of looking at information-security technology as an alternative to trust evidence—those things that make you feel confident in a business transaction. See how a new use of this technology can actually make things better.

**Q:** *Can you give an example?*

**A:** ATM machines illustrate the fundamental point. Before ATM machines, you had to go to a bank branch to do simple financial transactions. Part of the reason for that was security. You needed a teller who would authenticate you as the actual account holder. The teller, in looking through your records, would make access-control decisions about whether to give you money. There were paper audit records and physical protection of money. Because these security activities were done manually, there was a limitation on location; you could have preventions like this only at bank branches during hours when the tellers were there, and the scale of the branch was limited by the expense of building it.

Now, through the application of new technology, or new trust evidence, you can eliminate the limitation on scale. You can have many more ATM machines than branch banks. And there's so much less expense associated with an ATM machine than with a whole branch bank. You eliminate the limitation on time, because you no longer need a human being performing the security-authentication access-control decisions.

There are other inventive ways in which information security can help a business. But based on my experience of more than 20 years, the recipe for making things better is to first look at how security—the way you're currently doing it—imposes limitations. Then determine at how a more judicious use of information-security technology could eliminate those limitations. That's the approach.

**Q:** *What do you think of the relatively recent rise of the chief security officer, or CSO? Good idea, or overkill?*

**A:** While it's good to have a high-level executive with both the awareness and authority to do things, I don't care if it's a CSO, CIO, or an executive VP. The particular title doesn't matter. What matters is that whoever has that responsibility must be able to get something done, whether through the specific organizational position or, even more important, with the support of other executives. I've seen organizations where the chief information security person reports into building maintenance. I say, wonderful, have a CSO, but that's unimportant compared with the need for an individual who has the responsibility, the force of will, and the necessary support to do the job.

**Q:** *What should companies do to ensure that the top IT security chief, whatever the person's title, has that kind of authority?*

**A:** There needs to be a much closer identification and understanding between a company's core business activities and the information-security technology procedures necessary to support them. Right now, in most places, there's a huge gulf between them. On one hand, each company has a core set of business objectives. On the other, there's a set of security technologies that have some relationship in supporting those goals. But that relationship is often very poorly defined and understood. As long as this lack of understanding persists, nothing good will happen.

One of the primary responsibilities of CIOs and other IT managers is to make sure they know which security technologies are supporting every business activity. Without that, no organization is going to effectively move forward. One reason is that nobody on the business side will be willing to pay the money. Another reason is that while the folks on the IT side may be well-intentioned, they won't be doing the things that are necessary. They may not even know what's necessary.

**Q:** *How can a CIO show an ROI for IT security projects? It seems difficult. Yet increasingly, CFOs and other senior executives demand ROI figures before agreeing to make new investments.*

**A:** It's understandable, but not effective. A math professor I know once said, "If you torture the numbers long enough, they'll confess." Well, I've seen many different approaches to quantitative risk assessment. There has been lots of torturing going on, and many numbers have confessed. I don't see that kind of calculation as effective, in some cases, because we don't have the actuarial history that you do in other forms of insurance. There isn't a sufficient amount of data.

One reason ROI has been so popular is that anything quantitative is appealing; you can have measured results. Another is that in a world where the business objectives are so vastly removed from the security technologies, you're grasping at straws to come up with any way to justify your expense.

My experience is that what motivates companies to spend money on information security is the desire to eliminate or avoid pain. Only when you have well-defined pain will companies do anything, regardless of any ROI numbers you come up with.

One kind of pain that I've found to be incredibly motivating is government regulation, such as the Sarbanes-Oxley Act of 2002. Another form of pain is the loss of a customer or a potential customer. One company hired me because a potential customer, one of the largest banks in the world, was stalling at doing business with it. The bank had done an analysis of my client's security and realized it wouldn't have any way of protecting its PIN [personal ID number] information when the data resided on a partner's computers. So, to avoid the pain of losing both the sale and a foothold in the financial industry, the company hired me to help get its security house in order and avoid that lost-revenue pain.

Some companies, such as financial institutions, place a particularly high value on reputation, trust, reliability, and stability. Other companies have a well-developed sense of the value of their intellectual property, recognizing that the pain of losing that information is a sufficient motivation to spend dollars on security.

But if you say, "If we spend  $x$  amount of dollars on security, we'll get  $x + 5$  back," I would be very suspicious of those numbers. It's just not a compelling argument.