



Strategic Imperatives — Security Gets a Business Framework

Terry Sweeney

Security takes on personal and professional hues for Thomas Parenty. He started his own martial arts school in between gigs with the National Security Agency as an encryption expert and starting his own consultancy to advise corporate clientele on smarter security strategies. So he's got the bona fides to talk about protection of all sorts.



Parenty's diverse background underscores that. He served as a member of the National Research Council's Board on Assessment of National Institute of Standards and Technology (NIST) Programs, where he reviewed work on the Advanced Encryption Standard (AES) and wireless security. He's testified before Congress on national security, law enforcement and privacy and has an encryption patent pending. And he worked in the private sector for Sybase.

Parenty's latest book, *Digital Defense: What You Should Know About Protecting Your Company's Assets*, was published in September 2003 by the Harvard Business School Press, just before he relocated to Hong Kong. His book demonstrates the misconception that a firewall (or even lots of firewalls), a new algorithm or even some cool new biometrics technology somehow will protect assets and make the bad guys go away. Instead, Parenty argues that any corporate security process that's going to be effective must be closely tied to the specific business activities and the company's mission.

Executive Circle: You're critical of companies that worry more about protecting computers than information. What's involved in changing the mindset? Is it simply a matter of taking an organization's strategic objectives and mapping security initiatives to each?

Thomas Parenty: The first step is recognizing that an organization's strategic objectives and operational requirements should drive security initiatives. The vast majority of security work is done without any real understanding of what an organization does for a living or how it does it. Because the security work is done in isolation from the organization's real business purpose, you waste money on time and software.

A related problem is that many security technologies are deployed without understanding the threats or effective countermeasures. The result is you don't protect information the way you need to, and you put barriers in the way of people getting their work done.

Executive Circle: Can you give us an example?

Parenty: Many e-commerce websites store consumer financial information, such as credit card numbers, and they encrypt the credit card numbers so they are protected even if a hacker is able to break through the network and operating system protections. So far, so good. Unfortunately, many of these websites still

store the key used to encrypt the credit card numbers in a file on the same computer. If you are concerned about hackers breaking into your computers to steal credit card numbers, you should have the same concern about them stealing the key to decrypt these numbers.

Another example is a multinational chemical company. Several years ago, they went to great lengths to move some of their advanced R&D staff to an off-site facility. They deployed firewalls and a range of other security mechanisms to protect the sensitive formulas stored on the computers there. So far, this is a full credit answer.

Unfortunately, some of the researchers thought that all employees should have access to product formulas, because it might help them in their work. So they bypassed all of the security mechanisms and made the formulas available via the company's internal Web site. This put the company's most important trade secrets at great risk without helping anyone to do their work.

This case is unusual because most companies in the chemical, pharmaceutical, make-up and soft-drink industries have a much better appreciation of the value of their information and who needs access to it to do their jobs.

Computer Security is Not Information Security

Executive Circle: What other methods or processes do you encourage corporate planners to consider to proactively use information security to improve their businesses?

Parenty: One simple method is to look at business operations where existing protection measures, often manual, limit flexibility and growth. The use of information security can eliminate or reduce these limits.

Customer self-service is an increasingly common example. Customer service staff performs many security functions, such as authenticating customers, deciding what information they can receive, what operations they can perform and writing down a record of what has happened for future reference.

Performing all of these security activities is necessary, but expensive when done by staff. Companies improve customer retention while reducing costs by allowing customers to securely access their information without having to go through a voicemail call-tree of 12 choices to talk to a customer service representative.

Increased competitiveness from the ability to perform certain business operations more quickly and efficiently with security can make a huge difference. Business-to-business trade exchanges, with the appropriate security, can make the whole supply chain work much more efficiently.

Executive Circle: You consider computer security as distinct from information security. What's the practical application for IT people?

Parenty: When I say "computer security," I'm talking about perimeter-oriented and generic protections like anti-virus software and firewalls. These technologies protect a company's computers and networks in the same way a fenced parking lot and guard can protect a company's fleet of vehicles. They are necessary measures, but they don't provide any help in protecting the information these computers process.

Even if anti-virus, intrusion detection, firewalls and honeypots worked perfectly so no virus or hacker ever got in, executives still would have no way to answer questions like, were all the checks cut by accounts payable for the price negotiated? Is employee medical information in human resources confidential? Those protections operate at a generic level and so can not answer these business-specific questions.

The pragmatic lesson is that you should do a good job protecting the perimeter, and then get on with life and focus on being able to answer whether all the electronic funds transfers are valid or if a chemical formula is protected from competitors.

Executive Circle: To ensure that enterprise information is safe from fraudulent use, competitors' eyes or other unauthorized use, isn't some focus on technology appropriate?

Parenty: There is a clear need to focus on individual technologies, but there is a danger in focusing on it too early in the security process. One example is the head of a company who approached me to discuss his company's security issues. He started the conversation with, "What firewall would you recommend?" When I asked what the problem was, he said some employees and business partners were taking corporate information from internal computers.

It was then easy to see that a firewall wasn't going to help, but that he needed to control and audit access to information. If you assume you need a particular technology, it's easy to miss the point of what protections you actually need, and you end up with a solution that doesn't solve your problems.

It can be helpful to group security technologies into four areas:

- Confidentiality and privacy of information, which help to create a private online business environment. This includes encryption to protect information while it's transmitted or stored.
- Knowing with whom you are dealing. This means authenticating users and computers using technologies such as smart cards, digital certificates or biometrics.
- Controlling who gets access to what. Access control lists, digital rights management, encryption and authentication come into play.
- Holding people accountable for what they do, and ensuring that the things you see on the Internet are authentic and came from whom you thought they did. Audit trails and digital signatures help.

Not everyone in an organization needs to have the same level of understanding of these technologies. Just like you don't have to be an audio expert to buy a stereo, an executive shouldn't have to know the differences between two different encryption algorithms to make a security purchase decision. IT people should be able to dig down deeply into security technology, as needed. The business problem should drive search for security technology.

Establish the Trust Framework

Executive Circle: You encourage enterprises to think and act around a Trust Framework, which uses information security to provide assurance of safe, proper operation of digital business. Explain how that plays out on a more concrete level.

Parenty: The Trust Framework starts with a given business activity, and identifies the security-related requirements that are necessary for you to feel confident in the success and trustworthiness of this activity. I call these "trust objectives." You shouldn't think about technology at this stage.

Consider a company that wants to expand its office supply business into a business-to-business (B2B) portal for indirect goods. Some of the trust objectives for its current business are authenticating all buyers and sellers, keeping certain pricing information confidential, and maintaining a record of transactions for billing and dispute resolution. These trust objectives still hold true for the B2B portal, but many of the protection mechanisms used to meet these objectives in the physical world disappear in the move online. For example, much of the face-to-face and telephone contact that helped insure the trustworthiness of business transactions is gone.

I look at security technology as part of the "trust evidence" you need to meet your trust objectives in the digital world. For example, authenticating buying and selling organizations within a portal requires an initial registration process that could be in part manual as well as security technologies, such as passwords or digital certificates that will be used on an ongoing basis. Encryption replaces FedEx for protecting sensitive business documents.

By establishing trust objectives, you have a statement of what security means in a specific business context, which is increasingly important for corporate governance. Saying you thought your information was safe is no better a defense than saying you thought the company books were OK. A clear statement of trust objectives and the trust evidence you've used to meet these objectives lets employees, directors, stockholders and regulators decide if that's good enough. Having 25,000 firewalls says nothing about how safe it is to do business with you other than you've made your firewall vendor incredibly happy and rich.

Breaking out of the Mold

Executive Circle: IT sometimes gets stuck in a particular pattern of thinking. How do you encourage enterprises to rise above their own limitations with regard to security implementations or guiding philosophies?

Parenty: A perception among many non-IT business folks is that information security is too complex to understand so it's not worth trying to understand it. That perception is wrong and dangerous, because the people responsible for the success of the business have washed their hands of its decision-making.

Yes, the CIO needs to be more business-like and less technology-minded. But the people who make security technology selections are often much lower down the food chain within the IT department. If they don't have a business focus, the IT department will come up with a technology solution that doesn't fit the organization, because they didn't know better. They will end up spending a whole bunch of money and creating a lot of resentment.

There are two keys to success. The first is for non-IT management to step up to their responsibility to make security decisions. The second is for IT staff to keep in mind the business problem they are trying to solve and not just the security technology they use.

Terry Sweeney is a Los Angeles-based writer and editor who has covered telecommunications, networking and the Internet for more than 20 years.